PROTEÇÃO DE DADOS PESSOAIS NO SISTEMA DE JUSTIÇA: O MODELO EUROPEU INTEGRADO E PROPOSTAS INOVADORAS PARA GOVERNANÇA DE INTELIGÊNCIA ARTIFICIAL (IA) NO MINISTÉRIO PÚBLICO BRASILEIRO

PERSONAL DATA PROTECTION WITHIN THE JUSTICE SYSTEM: THE EUROPEAN INTEGRATED MODEL AND INNOVATIVE PROPOSALS FOR ARTIFICIAL INTELIGENCE (AI) GOVERNANCE IN PUBLIC PROSECUTOR'S OFFICE

Andrea C. Name Willemin
Diretora de Desenvolvimento Tecnológico e Segurança da Informação do "Centro de Seguridad (CESEG) - Universidad de Santiago de Compostela (USC).
Colaboradora Externa da Unidade Especial de Proteção de Dados Pessoais (UEPDAP) Do Conselho Nacional do Ministério Público (CNMP).
E-mail: andrea.willemin@usc.es

Rui Carlos Kolb Schiefler
Procurador de Justiça no Ministério Publico do Estado de Santa Catarina.
Coordenador da Unidade Especial de Proteção de Dados Pessoais (UEPDAP) do Conselho Nacional do Ministério Público (CNMP).
E-mail: rschiefler@mpsc.mp.br

RESUMO

A União Europeia consolidou o ecossistema jurídico mais avançado do mundo em proteção de dados pessoais no sistema de justiça. Este artigo analisa como o *General Data Protection Regulation* **(**GDPR) - Regulamento Geral de Proteção de Dados Europeu -, a Diretiva 680/2016 (*Law Enforcement Directive - LED*), o *AI Act* e a NIS 2 operam de forma integrada, criando um modelo normativo que equilibra a independência judicial e a proteção de dados na era digital. A pesquisa também demonstra que a Resolução nº 281/2023 do Conselho Nacional do Ministério Público (CNMP) brasileiro estabelece fundamentos técnicos surpreendentemente convergentes com os padrões europeus, abrindo caminho para a incorporação de tecnologias emergentes de forma segura e constitucionalmente orientada. A partir dessa análise comparada, propõem-se duas inovações institucionais: (1) o desenvolvimento, pela Unidade Especial de Proteção de Dados Pessoais (UEPDAP), de competências especializadas em supervisão e auditoria de sistemas de inteligência artificial; e (2) a criação de um Observatório de Inteligência Artificial e Proteção de Dados para o Ministério Público brasileiro. Essas propostas contribuem para a consolidação de uma governança digital robusta e replicável, fundamentada

em boas práticas internacionais e na integração entre Direito, tecnologia e *accountability* pública.

Palavras-chave: proteção de dados pessoais; inteligência artificial; Ministério Público; GDPR; AI Act; governança algorítmica; governança de dados; sistema de justiça; NIS 2; Resolução CNMP 281/2023.

ABSTRACT

The European Union has developed the world's most advanced legal ecosystem for personal data protection within the justice system. This article examines how the GDPR, Directive 680/2016 (Law Enforcement Directive), the AI Act, and NIS 2 operate in an integrated manner, establishing a normative framework that balances judicial independence with data protection in the digital age. The research highlights that Brazil's National Council of the Public Prosecutor's Office (CNMP) Resolution No. 281/2023 introduced technical foundations strikingly aligned with European standards, enabling the safe and constitutionally grounded integration of emerging technologies. Based on this comparative analysis, two institutional innovations are proposed: (1) empowering the Brazilian Special Unit for Personal Data Protection (UEPDAP) to develop AI oversight and audit capabilities; and (2) establishing an Observatory on Artificial Intelligence and Data Protection within the Public Prosecutor's Office. These proposals offer practical contributions toward a robust, replicable model of digital governance grounded in international best practices and the alignment of law, technology, and public accountability.

Keywords: personal data protection; artificial intelligence; Public Prosecutor's Office; GDPR; AI Act; algorithmic governance; data governance; justice system; NIS 2; CNMP Resolution 281/2023.

INTRODUÇÃO

A transformação digital do sistema de justiça configura um dos fenômenos mais relevantes da contemporaneidade jurídica, demandando profunda reconfiguração dos paradigmas de proteção de dados e governança institucional. A União Europeia respondeu a esse desafio desenvolvendo, na última década, o sistema normativo mais avançado mundialmente para proteção de dados em órgãos judiciais - um modelo que transcende regulamentação setorial para criar arquitetura sistêmica de proteção de direitos fundamentais.[1]

Esse sistema emerge não de norma isolada, mas da interação entre quatro pilares: o GDPR estabelece princípios basilares; a Diretiva 680/2016 (LED) cria regime especializado

[1] KUNER, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2013.

para aplicação da lei; o AI Act introduz a primeira governança abrangente de IA; e a NIS 2 estabelece fundamentos de segurança cibernética. [2]

Essa arquitetura normativa representa uma verdadeira evolução paradigmática. Reconhece que a proteção efetiva de dados no contexto judicial contemporâneo exige mais que regras sobre tratamento de dados, pois requer governança sofisticada de algoritmos, segurança cibernética robusta e mecanismos especializados de supervisão que respeitem a independência funcional dos órgãos judiciais.[3] Nas palavras de Kuner, Bygrave e Docksey[4], a integração sistêmica destes instrumentos representa maturação de uma abordagem holística à governança digital que serve de referência internacional.

O modelo europeu vai além de sua aplicação regional, estabelecendo padrões técnicos e metodológicos que influenciam desenvolvimentos regulatórios em diversas jurisdições. A sofisticação técnica dos institutos europeus, combinada à capacidade de integração sistêmica, oferece laboratório privilegiado para compreender como instrumentos normativos distintos podem operar harmoniosamente.[5]

Destaca-se especialmente a capacidade desse modelo em conseguir equilibrar valores aparentemente conflitantes: (a) rigor na proteção de dados pessoais versus preservação da independência judicial; (b) inovação tecnológica versus proteção de direitos fundamentais; e (c) eficiência operacional versus transparência democrática. Esse balanceamento não decorre de compromissos pontuais, mas de arquitetura técnica cuidadosamente desenhada permitindo coexistência harmoniosa de diferentes valores através de mecanismos institucionais especializados.[6]

No contexto nacional, a Resolução n. 281/2023 do CNMP representa um marco significativo, estabelecendo fundamentos técnicos notavelmente alinhados aos padrões

---

[2] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119, 4 maio 2016. UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. Jornal Oficial da União Europeia, L 119, 4 maio 2016. UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União*. Jornal Oficial da União Europeia, L 333, 27 dez. 2022. UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. Jornal Oficial da União Europeia, L 1689, 12 jul. 2024.

[3] LYNSKEY, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015.

[4] KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. *The EU General Data Protection Regulation: A Commentary*. Oxford: Oxford University Press, 2020.

[5] HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*. Cham: Springer, 2016.

[6] GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer, 2014.

europeus.[7] Esta resolução criou, por exemplo, uma estrutura de governança de dados que, embora inicialmente focada na implementação da Lei Geral de Proteção de Dados Pessoais (LGPD), possui flexibilidade técnica e visão estratégica necessárias para incorporar avanços normativos representados pelo AI Act e NIS 2.

A análise comparativa revela oportunidades únicas de integração e aprendizado mútuo. O Brasil demonstrou, através da Resolução n. 281/23, capacidade de inovação institucional que pode contribuir para o desenvolvimento de melhores práticas globais, enquanto o modelo europeu oferece soluções técnicas testadas e validadas orientando evolução futura do sistema brasileiro.[8]

Esta investigação analisa mecanismos técnicos de funcionamento e integração sistêmica dos institutos europeus de proteção de dados aplicáveis aos órgãos judiciais, formulando propostas inovadoras que contribuam tanto para o aperfeiçoamento do modelo europeu quanto para a evolução do sistema brasileiro.

Baseando-nos nessa análise, propomos duas inovações fundamentais. Primeira: modelo técnico para que a UEPDAP, prevista na Resolução n. 281/23, desenvolva competências especializadas em supervisão de sistemas de IA e tecnologias emergentes. Segunda: criação de um Observatório de Inteligência Artificial e Proteção de Dados para o Ministério Público brasileiro, estruturado segundo padrões do AI Act, viabilizando implementação segura e ética de sistemas de IA no âmbito da Resolução n. 281/23.[9]

Adotamos metodologia de análise técnica comparativa, fundamentada no exame detalhado dos textos normativos europeus, documentos técnicos das autoridades de supervisão, relatórios de implementação e literatura especializada. A análise concentra-se em aspectos técnicos e operacionais, evitando debates jurídicos controversos para focar em soluções práticas implementáveis.

A base documental deste estudo é constituída por textos normativos oficiais da União Europeia, como o Regulamento Geral de Proteção de Dados (RGPD ou GDPR), a Diretiva 680/2016/UE, o AI Act e a Diretiva NIS 2, bem como as decisões e comunicações da Comissão Europeia, do Conselho Europeu de Proteção de Dados (EDPB) e da Agência da União Europeia para a Cibersegurança (ENISA). Estes documentos oferecem evidência direta e serviram de fio

---

[7] BRASIL. Conselho Nacional do Ministério Público. *Resolução nº 281, de 14 de dezembro de 2023. Estabelece diretrizes para a proteção de dados pessoais no âmbito do Ministério Público*. Brasília: CNMP, 2023.
[8] PASQUALE, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press, 2015.
[9] RUSSELL, Stuart; NORVIG, Peter. *Artificial Intelligence: A Modern Approach*. 4. ed. Boston: Pearson, 2020.

condutor à análise. A pesquisa também recorreu a pareceres e relatórios de autoridades nacionais europeias de supervisão, além de literatura científica publicada em revistas com revisão por pares e livros de editoras acadêmicas; tais obras foram escolhidas pela relevância e pelo reconhecimento dos seus autores na área de proteção de dados, garantindo a fiabilidade interpretativa. Por fim, relatórios de organismos internacionais de reconhecida competência técnica foram utilizados para complementar a compreensão comparativa do tema. As leis nacionais e outros materiais foram examinados apenas por meio dessas fontes secundárias especializadas, à semelhança do procedimento adoptado em estudos comparados de âmbito europeu.

A metodologia comparativa baseia-se no modelo de análise funcional desenvolvido por Zweigert e Kötz[10], adaptado para governança digital. Essa abordagem permite identificar soluções funcionalmente equivalentes em diferentes sistemas, focando resultados práticos alcançados.

Seguimos quatro etapas: mapeamento estrutural dos institutos europeus; análise funcional de operação prática de cada instituto; identificação de interfaces entre institutos; e avaliação de aplicabilidade das soluções europeias ao contexto brasileiro.

Reconhecemos limitações inerentes à análise comparativa de sistemas em evolução. A temporalidade constitui limitação significativa, pois alguns instrumentos como o AI Act são recentes e carecem de dados empíricos extensivos sobre implementação. A especificidade cultural dos sistemas jurídicos pode limitar transferibilidade direta de soluções.

A complexidade técnica de sistemas de IA e cibersegurança requer conhecimentos especializados que transcendem o âmbito jurídico tradicional. Mitigamos essas limitações focando aspectos técnicos e operacionais, evitando generalizações excessivas.

O estudo estrutura-se em oito seções. Após esta introdução, seções 2 a 5 examinam cada pilar normativo europeu. A Seção 6 analisa a operação sinérgica para criar modelo integrado. A Seção 7 apresenta propostas inovadoras para a UEPDAP e o Observatório. A Seção 8 formula recomendações técnicas.

Para facilitar a compreensão da complexa arquitetura normativa europeia, apresentamos uma síntese executiva demonstrando visualmente como os quatro pilares se integram, criando um sistema coeso de governança digital no sistema de justiça.

[10] ZWEIGERT, Konrad; KÖTZ, Hein. *Introduction to Comparative Law*. 3. ed. Oxford: Oxford University Press, 1998.

Tabela 1; Matriz de Integração dos Institutos Europeus

	GDPR	LED (Diretiva 680/2016)	AI Act	NIS 2
Âmbito de Aplicação	Tratamento de dados pessoais em geral	Tratamento de dados no setor de aplicação da lei	Sistemas de IA eom impacto sobre direitos fundamentais	Segurança cibernética e resiliência de redes è sistemas
Principios Fundamentais	Licitude, lealda-de, minimização, etc.	Licitude, lealda-de, minimização, etc.	Gestão de risco, transparência, etc.	Gestão de risco, transparência, etc.
Mecanismos de Supervisão	Autoridades de proteção de dados	Autoridades de proteção de dados	Autoridades de supervisão de IA	Autoridades nacionais competentes
Direitos dos Titulares	Acesso, retificação, apagamento, etc.	Direitos semelha-tes ao GDPR em contexto policial	Semelhantes aos do GDPR	Semelhantes aos do GDPR
Integração Sistêmica	Padrões elevados de proteção de dados	Avaliação de risco, segurança, etc.	Gestão do ciclo de vida, segurança, et.	Gestão do ciclo de vida, segurança, et.

Tabela I - Matriz de Integração dos Institutos Europeus de Proteção de Dados
Fonte: Elaboração própria baseada na análise dos instrumentos normativos europeus.

Figura 1: Modelo de Integração Sistémica dos Institutos Europeus

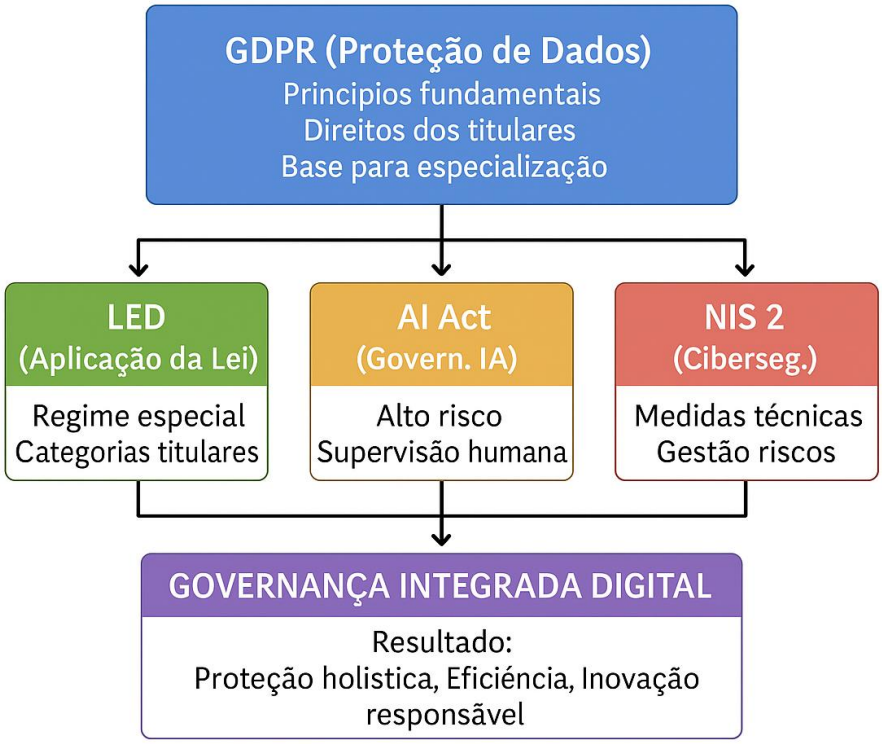

Figura I - Modelo de Integração Sistêmica dos Institutos Europeus
Fonte: Elaboração própria baseada na análise comparativa dos institutos normativos.

Esta representação demonstra como os quatro pilares operam integrados e sinergicamente. O GDPR fornece princípios fundamentais especializados e complementados pelos demais: a Diretiva (UE) 2016/680 (LED) adapta esses princípios ao contexto específico da aplicação da lei penal; o AI Act estabelece governança específica para IA; e a NIS 2 fornece infraestrutura de cibersegurança. O resultado é uma governança coesa, equilibrando proteção de direitos fundamentais, eficiência operacional e inovação responsável.

A integração baseia-se em cinco princípios transversais permeando todos os institutos: proporcionalidade (obrigações graduadas conforme risco); responsabilização (*accountability* - demonstração ativa de conformidade); transparência adaptada (informação adequada ao contexto); supervisão humana (controle humano sobre automação); e proteção por conceção (*privacy by design* - salvaguardas desde desenvolvimento). Esta abordagem produz benefícios sinérgicos transcendendo a aplicação isolada de cada instituto: eficiência operacional, proteção abrangente, inovação responsável e fortalecimento da confiança institucional.

1 O REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS: ARQUITETURA TÉCNICA

O Regulamento (UE) 2016/679 - GDPR - constitui o alicerce do sistema europeu de proteção de dados, estabelecendo arquitetura normativa sofisticada baseada em princípios operacionais, direitos procedimentais e mecanismos de *accountability* transcendendo regulamentação setorial.[11] Sua estrutura foi concebida como sistema aberto e modular, integrando-se harmoniosamente com regulamentações específicas sem perder coerência normativa.[12]

1.1 Princípios operacionais: da teoria à implementação técnica

O GDPR estabelece sete princípios fundamentais, funcionando não apenas como diretrizes éticas, mas como parâmetros técnicos mensuráveis para avaliação de conformidade.

[11] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119, 4 maio 2016.
[12] LYNSKEY, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015.

Codificados no artigo 5º, constituem critérios operacionais traduzíveis em indicadores técnicos específicos.[13] Neste contexto cinco deles se destacam:

Os princípios da licitude, lealdade e transparência (art. 5(1)(a)) operacionaliza-se através de sistema técnico de bases jurídicas (art. 6º) e obrigações estruturadas de informação (arts. 13º-14º). Para órgãos judiciais, a base predominante reside no exercício de funções de interesse público (art. 6(1)(e)), requerendo demonstração técnica de necessidade e proporcionalidade.[14]

O princípio da limitação das finalidades (art. 5(1)(b)) estabelece que dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas. No contexto judicial, permite flexibilidade para tratamentos posteriores compatíveis, incluindo atividades investigativas e procedimentos judiciais relacionados.[15]

O princípio da minimização (art. 5(1)(c)) exige que dados sejam adequados, pertinentes e limitados ao necessário. Para órgãos judiciais, requer avaliação contínua de necessidade e proporcionalidade, especialmente em investigações complexas envolvendo grandes volumes informacionais.

1.2 Bases legais específicas para órgãos judiciais

A arquitetura do GDPR reconhece especificidades dos órgãos judiciais através de bases legais específicas e exceções adaptadas. O artigo 6(1)(e) estabelece que o tratamento é lícito quando necessário ao exercício de funções de interesse público ou autoridade pública investida no responsável - base particularmente relevante para tribunais e MP, que exercem funções constitucionalmente definidas.[16]

Para categorias especiais de dados (art. 9º), o GDPR estabelece exceções no art. 9(2)(f), permitindo tratamento quando necessário ao exercício de funções jurisdicionais, funções específicas do MP ou proteção de direitos e liberdades de terceiros. Esta exceção reconhece que

---

[13] VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer, 2017.
[14] EUROPEAN DATA PROTECTION BOARD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Brussels: EDPB, 2019.
[15] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119, 4 maio 2016.
[16] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119, 4 maio 2016.

a eficácia da justiça pode requerer processamento de dados sensíveis, exigindo, porém, proporcionalidade.

O considerando 45 esclarece especificamente que tratamento de dados pelos tribunais no exercício da função jurisdicional está abrangido pelo regulamento, mas que a independência judicial deve ser respeitada[17] - disposição estabelecendo equilíbrio fundamental entre proteção de dados e independência judicial caracterizando todo modelo europeu.

1.3 Direitos dos titulares: adaptações ao contexto judicial

O GDPR estabelece um conjunto abrangente de direitos dos titulares (Cap. III), mas reconhece que o contexto judicial pode requerer limitações específicas. O artigo 23º permite Estados-Membros adotarem medidas legislativas restritivas quando necessário e proporcionais para salvaguardar objetivos de interesse público, incluindo exercício da função jurisdicional.

O direito de acesso (art. 15º) pode ser limitado quando possa comprometer investigações em curso ou independência judicial. Porém, essas limitações devem ser temporárias e proporcionais, sendo revistas regularmente.[18]

O direito ao apagamento (art. 17º) encontra limitações no art. 17(3)(e), estabelecendo não aplicação quando o tratamento for necessário ao exercício da liberdade de expressão ou cumprimento de obrigação legal - exceção fundamental para preservar a integridade dos registos judiciais e assegurar transparência do sistema.

1.4 Supervisão e independência judicial

Uma característica distintiva do GDPR no contexto judicial é o tratamento da supervisão, equilibrando proteção de dados com independência judicial. O artigo 55(3)

[17] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119, 4 maio 2016.
[18] EUROPEAN DATA PROTECTION BOARD. *Guidelines 10/2020 on restrictions under Article 23 GDPR*. Brussels: EDPB, 2020.

estabelece que autoridades de proteção de dados não têm competência para supervisionar operações pelos tribunais no exercício da função jurisdicional.[19]

Esta exceção visa a preservar a independência judicial, mas cria desafios para assegurar conformidade. A solução europeia envolve desenvolvimento de mecanismos de supervisão interna e formação especializada dos magistrados.[20] Vários Estados-Membros estabeleceram estruturas especializadas dentro do sistema judicial para questões de proteção de dados, combinando expertise técnica com compreensão das especificidades judiciais.

O *European Data Protection Board* - EDPB desenvolveu orientações sobre a aplicação do GDPR no contexto judicial, reconhecendo que proteção efetiva requer abordagens adaptadas respeitando a independência judicial[21], enfatizando a importância de formação contínua, políticas internas e medidas técnicas e organizacionais adequadas.

2 A DIRETIVA 680/2016: PROTEÇÃO DE DADOS NA APLICAÇÃO DA LEI

A Diretiva (UE) 2016/680 - LED - estabelece regime especializado de proteção de dados para atividades de prevenção, investigação, detecção ou repressão de infrações penais, reconhecendo características únicas a justificar tratamento normativo diferenciado.[22] A LED não substitui o GDPR. Complementa-o, criando sistema dual, permitindo proteção adequada em diferentes contextos operacionais.[23]

---

[19] UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119, 4 maio 2016.
[20] KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. *The EU General Data Protection Regulation: A Commentary*. Oxford: Oxford University Press, 2020.
[21] KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. *The EU General Data Protection Regulation: A Commentary*. Oxford: Oxford University Press, 2020.
[22] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.
[23] BOEHM, Franziska. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*. Berlin: Springer, 2012.

2.1 Âmbito de aplicação e interface com o GDPR

A LED aplica-se especificamente ao tratamento de dados por autoridades competentes para fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções, incluindo proteção contra ameaças à segurança pública (art. 1(1)). Esta delimitação funcional cria interface clara com o GDPR, evitando sobreposições.[24]

Para o Ministério Público, frequentemente atuando em funções investigativas e processuais, a LED aplica-se às atividades de investigação criminal, enquanto o GDPR pode aplicar-se a outras funções. Essa dualidade requer sistemas de governança sofisticados operando sob diferentes regimes, conforme contexto específico.[25]

O artigo 2(1) define "autoridade competente" como qualquer autoridade pública competente para prevenção, investigação, detecção ou repressão de infrações ou execução de sanções, incluindo proteção contra ameaças à segurança. Definição abrangente, incluindo não apenas polícias, mas também MP e outras autoridades com competências investigativas.[26]

2.2 Princípios adaptados ao contexto da aplicação da lei

A LED adapta princípios fundamentais às especificidades das atividades de aplicação da lei, mantendo coerência conceitual com o GDPR, mas permitindo flexibilidade operacional necessária.[27] O artigo 4º estabelece princípios espelhando os do GDPR, com adaptações específicas.

O princípio da licitude (art. 4(1)(a)) requer que o tratamento seja baseado no direito da União ou Estado-Membro, mas reconhece que atividades de aplicação da lei podem requerer

---

[24] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.

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

[26] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.

[27] DE HERT, Paul; PAPAKONSTANTINOU, Vagelis. *The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review*, v. 32, n. 2, p. 179-194, 2016.

coleta sem conhecimento do titular - adaptação fundamental para preservar a eficácia investigativa.[28]

O princípio da limitação das finalidades (art. 4(1)(b)) permite que dados coletados para aplicação da lei sejam tratados posteriormente para finalidades compatíveis, incluindo outras investigações ou procedimentos. Flexibilidade reconhecendo que investigações podem evoluir e requerer análises adicionais.

O princípio da minimização (art. 4(1)(c)) exige dados adequados, pertinentes e não excessivos, mas reconhece que investigações podem requerer coleta ampla para identificar padrões e conexões.[29]

2.3 Categorização de dados e salvaguardas específicas

A LED estabelece sistema sofisticado de categorização reconhecendo diferentes riscos. O artigo 6º exige que Estados-Membros assegurem distinção clara entre categorias de titulares.[30]

Categorias incluem: suspeitos (pessoas sobre as quais existem motivos ou suspeitas razoáveis de infração); vítimas (pessoas que sofreram danos); testemunhas (pessoas com informações relevantes); e outras pessoas (incluindo contatos de suspeitos).

Esta categorização orienta medidas de segurança e prazos de conservação. Dados de suspeitos podem ser conservados por períodos mais longos, com medidas menos restritivas que dados de vítimas ou testemunhas.[31]

---

[28] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.

[29] HIJMANS, Hielke; KRANENBORG, Herke. *Data Protection Anno 2014: How to Restore Trust?* Cambridge: Intersentia, 2014.

[30] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.

[31] GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer, 2014.

Para categorias especiais (art. 10º), a LED estabelece salvaguardas específicas, exigindo que o tratamento seja estritamente necessário, sujeito a salvaguardas adequadas, e autorizado por direito da União ou Estado-Membro.[32]

2.4 Direitos dos titulares: equilíbrio entre proteção e eficácia investigativa

A LED estabelece direitos dos titulares (Cap. III) equilibrando proteção com necessidades operacionais das autoridades. Estes direitos podem ser mais limitados que os do GDPR, mas devem ser exercidos sem comprometer investigações ou segurança.

O direito de informação (arts. 13º-14º) pode ser diferido quando informação imediata comprometa investigações. Porém, deve ser fornecida assim que não comprometa mais a investigação.[33]

O direito de acesso (art. 15º) pode ser restringido quando possa comprometer investigações, mas deve ser concedido quando não apresente riscos. Autoridades devem manter registos das restrições, revendo-as regularmente.

Direitos de retificação (art. 16º) e apagamento (art. 17º) podem ser limitados quando necessário para preservar a integridade investigativa ou quando dados forem necessários para procedimentos futuros.

2.5 Transferências internacionais e cooperação judiciária

A LED estabelece regime específico para transferências internacionais no contexto de aplicação da lei (Cap. V), reconhecendo que cooperação internacional é essencial para combater

[32] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.

[33] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.

crime transnacional.[34] Este regime é mais flexível que o do GDPR, mantendo, porém, salvaguardas fundamentais.

Transferências podem basear-se em decisões de adequação da Comissão (art. 36º), salvaguardas adequadas incluindo acordos internacionais (art. 37º), ou derrogações para situações particulares (art. 38º).

O artigo 38º estabelece derrogações permitindo transferências quando necessárias para proteger interesses vitais, prevenir ameaças imediatas à segurança ou para cooperação judiciária internacional.

A LED reconhece a importância dos instrumentos de cooperação judiciária existentes, incluindo mandado de detenção europeu, estabelecendo que transferências baseadas nestes instrumentos são consideradas como tendo salvaguardas adequadas.

3 O REGULAMENTO DA INTELIGÊNCIA ARTIFICIAL: GOVERNANÇA DE SISTEMAS DE IA

O Regulamento (UE) 2024/1689 - AI Act - representa uma primeira tentativa abrangente de regulamentação da IA a nível supranacional, estabelecendo marco pioneiro baseado em abordagem de risco reconhecendo especificidades dos diferentes contextos.[35] Para o sistema de justiça, introduz salvaguardas assegurando que a utilização de IA preserve princípios fundamentais do Estado de Direito.[36]

3.1 Arquitetura técnica baseada em risco

O AI Act estrutura-se em classificação de risco em quatro níveis, cada um com obrigações específicas proporcionais ao risco. Esta abordagem reconhece que nem todos os

[34] UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.
[35] UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. *Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024.
[36] ALBRECHT, Jan Philipp. *How the GDPR Will Change the World*. *European Data Protection Law Review*, v. 2, n. 3, p. 287-289, 2016.

sistemas apresentam os mesmos riscos, permitindo regulamentação diferenciada, evitando sobrecarregar aplicações de baixo risco enquanto estabelece salvaguardas rigorosas para aplicações críticas.[37]

Figura 4 - Classificação de Riscos de IA baseada no AI Act
Fonte: Elaboração própria baseada no Regulamento (UE) 2024/1689.

Sistemas proibidos (art. 5º) incluem aqueles que usam técnicas subliminares, explorando vulnerabilidades de grupos, implementando pontuação social por autoridades, ou realizando identificação biométrica remota em tempo real em espaços públicos (com exceções limitadas para aplicação da lei). Proibições refletem o reconhecimento de riscos inaceitáveis, independentemente das salvaguardas.

Sistemas de alto risco (art. 6º e Anexo III) incluem especificamente sistemas na administração da justiça e processos democráticos. Esta classificação sujeita sistemas a obrigações rigorosas ao longo do ciclo de vida: gestão de risco, governança de dados, documentação técnica, transparência, supervisão humana e robustez.[38]

Sistemas de risco limitado (art. 50º) estão sujeitos a obrigações de transparência, exigindo que utilizadores sejam informados da interação com IA.

Sistemas de risco mínimo não têm obrigações específicas, podendo aderir voluntariamente a códigos de conduta.

[37] UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. *Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024.
[38] UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. *Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024.

3.2 Sistemas de IA na administração da justiça: requisitos específicos

O AI Act classifica explicitamente sistemas destinados a avaliar credibilidade de provas em investigações ou procedimentos como alto risco (Anexo III, ponto 8(a)), reconhecendo impacto potencial nos direitos fundamentais e equidade dos procedimentos.[39]

Os requisitos para alto risco (Cap. 2 do Tít. III) estabelecem obrigações assegurando segurança, transparência e conformidade com Estado de Direito:

A gestão de risco (art. 9º) identifica, analisa, avalia e mitiga riscos. No contexto judicial, inclui riscos de viés, discriminação, erro e impacto nos direitos fundamentais.[40]

A governança e qualidade dos dados (art. 10º) assegura que conjuntos de treino, validação e teste sejam suficientemente representativos, precisos e completos. Para sistemas judiciais, significa assegurar que dados de treino não contenham vieses resultando em discriminação.[41]

A documentação técnica (art. 11º) fornece informações claras sobre o sistema, incluindo capacidades, limitações, desempenho e riscos. A documentação deve permitir que autoridades avaliem a conformidade.[42]

A manutenção de registos (art. 12º) permite a rastreabilidade das operações. No contexto judicial, isso é fundamental para auditabilidade de decisões apoiadas por IA.[43]

A transparência e as informações aos utilizadores (art. 13º) asseguram que sistemas sejam suficientemente transparentes para permitir interpretação e uso adequado dos resultados. Para magistrados, significa compreender como o sistema chegou às conclusões.

A supervisão humana (art. 14º) assegura que sistemas sejam concebidos permitindo supervisão eficaz. No contexto judicial, magistrados devem manter controle total sobre decisões, usando IA como ferramenta de apoio.[44]

---

[39] UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. *Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024.

[40] EDWARDS, Lilian; VEALE, Michael. *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*. *Duke Law & Technology Review*, v. 16, n. 1, p. 18-84, 2017.

[41] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. *International Data Privacy Law*, v. 7, n. 2, p. 76-99, 2017.

[42] SELBST, Andrew D.; POWLES, Julia. *Meaningful information and the right to explanation*. *International Data Privacy Law*, v. 7, n. 4, p. 233-242, 2017.

[43] KAMINSKI, Margot E. *The Right to Explanation, Explained*. *Berkeley Technology Law Journal*, v. 34, n. 1, p. 189-218, 2019.

[44] UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. *Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024.

3.3 Avaliação de conformidade e supervisão

O AI Act estabelece procedimentos de avaliação de conformidade para alto risco (arts. 43º-46º), realizados antes da colocação no mercado ou entrada em serviço. Para sistemas de autoridades públicas, incluindo órgãos judiciais, a avaliação pode ser realizada internamente se houver competências técnicas adequadas.[45]

A supervisão é realizada por autoridades nacionais competentes designadas pelos Estados-Membros (art. 59º), com poderes de investigação incluindo acesso a dados, documentação e instalações, podendo impor medidas corretivas.[46]

Para sistemas no contexto judicial, a supervisão deve equilibrar conformidade com respeito à independência judicial. O AI Act reconhece essa tensão, permitindo que Estados-Membros estabeleçam modalidades específicas, respeitando especificidades constitucionais.

3.4 Integração com a proteção de dados

O AI Act estabelece que disposições são sem prejuízo das obrigações do GDPR e LED (art. 2(7)), criando relação de complementaridade onde cada instrumento contribui para a proteção de direitos em sua área específica.[47]

A integração se manifesta em várias dimensões. Requisitos de governança de dados do AI Act complementam princípios do GDPR, criando salvaguardas específicas para dados em sistemas de IA. Requisitos de transparência do AI Act facilitam o cumprimento de obrigações de informação do GDPR. Requisitos de supervisão humana reforçam *accountability* do GDPR.

Esta integração requer que organizações desenvolvam abordagens coordenadas, atendendo simultaneamente aos requisitos de ambos os instrumentos. Para órgãos judiciais, significa implementar governança, assegurando tanto proteção de dados pessoais quanto governança adequada de IA.

---

[45] UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. *Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024.

[46] HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. *The European Union general data protection regulation: what it is and what it means*. *Information & Communications Technology Law*, v. 28, n. 1, p. 65-98, 2019.

[47] UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*. *Jornal Oficial da União Europeia*, L 1689, 12 jul. 2024.

4 A DIRETIVA NIS 2: CIBERSEGURANÇA E PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

A Diretiva (UE) 2022/2555 - NIS 2 - estabelece medidas para elevado nível comum de cibersegurança na União Europeia, expandindo significativamente o âmbito da regulamentação original e introduzindo requisitos mais rigorosos para infraestruturas críticas.[48] Para o sistema de justiça, reconhece que órgãos judiciais constituem infraestruturas críticas, requerendo proteção especial contra ameaças cibernéticas.[49]

4.1 Âmbito de aplicação e entidades abrangidas

A NIS 2 aplica-se a entidades essenciais e importantes em setores críticos, incluindo explicitamente a administração pública (art. 2(1) e Anexo I). Órgãos judiciais, incluindo tribunais e MP, enquadram-se como entidades essenciais devido ao papel fundamental no funcionamento do Estado de Direito.[50]

O artigo 3(1) define entidade essencial como aquela que presta serviço ou exerce atividade em um setor essencial, cuja perturbação teria impacto significativo em serviços essenciais, atividade econômica, saúde pública, segurança ou bem-estar social. Órgãos judiciais enquadram-se claramente devido ao seu papel na manutenção da ordem jurídica e social.

A NIS 2 estabelece que entidades essenciais estão sujeitas à supervisão *ex ante*, incluindo auditorias e inspeções regulares, enquanto entidades importantes estão sujeitas principalmente a supervisão *ex post*. A diferenciação reconhece que entidades essenciais, incluindo órgãos judiciais, requerem monitorização mais intensiva devido ao papel crítico.[51]

---

[48] UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União*. *Jornal Oficial da União Europeia*, L 333, 27 dez. 2022.

[49] VEALE, Michael; BINNS, Reuben; EDWARDS, Lilian. *Algorithms that remember: model inversion attacks and data protection law*. *Philosophical Transactions of the Royal Society A*, v. 376, n. 2133, 2018.

[50] UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União*. *Jornal Oficial da União Europeia*, L 333, 27 dez. 2022.

[51] BINNS, Reuben. *Fairness in Machine Learning: Lessons from Political Philosophy*. *Proceedings of Machine Learning Research*, v. 81, p. 149-159, 2018.

4.2 Requisitos de gestão de risco de cibersegurança

A NIS 2 estabelece requisitos específicos de gestão de risco que entidades abrangidas devem implementar (art. 21º), particularmente relevantes para órgãos judiciais, processando informações sensíveis e operando sistemas críticos.[52]

Os requisitos técnicos e organizacionais incluem políticas de análise e gestão de risco, tratamento de incidentes, continuidade de negócio e gestão de crises, segurança da cadeia de fornecimento, segurança na aquisição, desenvolvimento e manutenção de sistemas e procedimentos para avaliar eficácia das medidas.[53]

Para órgãos judiciais, tais requisitos devem ser implementados respeitando a independência judicial e confidencialidade dos procedimentos. A NIS 2 reconhece essa especificidade permitindo que Estados-Membros adaptem requisitos às características dos diferentes setores.[54]

A gestão de risco deve ser proporcional ao tamanho da entidade e ao risco, mas deve abranger todos os elementos da infraestrutura de TI: sistemas de gestão processual, bases de dados judiciais, sistemas de comunicação e infraestruturas de rede.[55]

4.3 Notificação de incidentes e resposta a crises

A NIS 2 estabelece obrigações de notificação visando a facilitar resposta coordenada a ameaças e permitir a partilha de informações sobre ameaças emergentes (art. 23º). Para órgãos judiciais, essas obrigações devem equilibrar transparência com necessidade de proteger informações sensíveis.[56]

---

[52] UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União*. *Jornal Oficial da União Europeia*, L 333, 27 dez. 2022.

[53] MITTELSTADT, Brent. *Principles alone cannot guarantee ethical AI*. *Nature Machine Intelligence*, v. 1, n. 11, p. 501-507, 2019.

[54] FLORIDI, Luciano et al. *AI4People—An Ethical Framework for a Good AI Society*. *Minds and Machines*, v. 28, n. 4, p. 689-707, 2018.

[55] JOBIN, Anna; IENCA, Marcello; VAYENA, Effy. *The global landscape of AI ethics guidelines*. *Nature Machine Intelligence*, v. 1, n. 9, p. 389-399, 2019.

[56] UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União*. *Jornal Oficial da União Europeia*, L 333, 27 dez. 2022.

Incidentes significativos devem ser notificados às autoridades no prazo de 24 horas após tomada de conhecimento, com informações adicionais em 72 horas. A notificação deve inclui a natureza do incidente, medidas tomadas para mitigar o impacto e a avaliação preliminar.[57]

Para órgãos judiciais, a notificação deve considerar o impacto nos procedimentos judiciais: atrasos em julgamentos, comprometimento de dados processuais ou interrupção de serviços essenciais. A NIS 2 permite que informações sensíveis sejam protegidas através de canais seguros com autoridades.

A resposta deve incluir medidas para restaurar a continuidade, preservar evidências para investigação e para comunicação com as partes interessadas adequadamente. Para tribunais, pode incluir procedimentos para manter julgamentos, proteger dados processuais e informar advogados e partes sobre impactos.[58]

4.4 Integração com proteção de dados e governança de IA

A NIS 2 reconhece explicitamente a importância da integração com outros instrumentos, incluindo GDPR e AI Act, fundamental para criar um sistema coeso de governança digital abordando simultaneamente cibersegurança, proteção de dados e governança de IA.[59]

A segurança dos dados pessoais constitui ponto de convergência natural entre cibersegurança e proteção de dados. As medidas exigidas pela NIS 2 contribuem diretamente para o cumprimento de obrigações de segurança do GDPR (art. 32º), criando sinergias e beneficiando ambos os objetivos.[60]

A notificação de violações representa a área onde regimes se sobrepõem, exigindo coordenação cuidadosa. Incidentes de cibersegurança resultando em violações de dados devem ser notificados tanto às autoridades de cibersegurança (NIS 2) quanto às de proteção de dados (GDPR).[61]

---

[57] WINFIELD, Alan F. T.; JIROTKA, Marina. *Ethical governance is essential to building trust in robotics and artificial intelligence systems*. *Philosophical Transactions of the Royal Society A*, v. 376, n. 2133, 2018.
[58] HAGENDORFF, Thilo. *The Ethics of AI Ethics: An Evaluation of Guidelines*. *Minds and Machines*, v. 30, n. 1, p. 99-120, 2020, p. 105.
[59] UNIÃO EUROPEIA. Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União. *Jornal Oficial da União Europeia*, L 333, 27 dez. 2022.
[60] MORLEY, Jessica et al. The ethics of AI in health care: A mapping review. *Social Science & Medicine*, v. 260, 113172, 2020.
[61] BAROCAS, Solon; HARDT, Moritz; NARAYANAN, Arvind. *Fairness and Machine Learning: Limitations and Opportunities*. Cambridge: MIT Press, 2023.

Para sistemas de IA, a NIS 2 fornece infraestrutura de segurança necessária, assegurando operação segura e resiliente. A integração entre cibersegurança e governança de IA é particularmente importante para sistemas de alto risco no contexto judicial, onde falhas podem ter impactos significativos nos direitos fundamentais.[62]

4.5 Supervisão e coordenação nacional

A NIS 2 estabelece estruturas de supervisão incluindo autoridades competentes, pontos de contacto únicos, e o "*Computer Security Incident Response Teams"* (CSIRTs), devendo coordenar-se com outras autoridades, incluindo as de proteção de dados e supervisão de IA.[63]

Para o setor judicial, a supervisão deve respeitar a independência e pode requerer estruturas especializadas, compreendendo as especificidades dos órgãos judiciais. Vários Estados-Membros estabeleceram unidades especializadas dentro dos conselhos superiores da magistratura para coordenar questões de cibersegurança no sistema judicial.[64]

A coordenação europeia é facilitada através da ENISA e do Grupo de Cooperação estabelecido pela Diretiva, permitindo a partilha de informações sobre ameaças, desenvolvimento de melhores práticas e resposta coordenada a incidentes transfronteiriços.[65]

5 INTEGRAÇÃO SISTÊMICA DOS INSTITUTOS EUROPEUS

A verdadeira inovação do modelo europeu não reside na excelência individual de cada instrumento, mas na capacidade de integração sistêmica, criando um ecossistema coeso de governança digital transcendendo a soma das partes.[66] Esta integração não resulta de plano pré-

---

[62] BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press, 2019.
[63] UNIÃO EUROPEIA. Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União. *Jornal Oficial da União Europeia*, L 333, 27 dez. 2022.
[64] NOBLE, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press, 2018.
[65] EUBANKS, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press, 2018.
[66] ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

concebido, mas emerge da aplicação consistente de princípios fundamentais comuns e da coordenação cuidadosa entre diferentes iniciativas legislativas.[67]

5.1 Mecanismos de coordenação normativa

A coordenação entre os instrumentos se opera através de múltiplos mecanismos, assegurando coerência conceitual, procedimental e substantiva, desenvolvidos ao longo do tempo através da experiência de implementação e da necessidade de evitar conflitos.[68]

Referências cruzadas explícitas constituem o primeiro nível de coordenação. O AI Act estabelece que as disposições são "sem prejuízo" das obrigações do GDPR e LED (art. 2(7)), criando hierarquia onde a proteção de dados mantém primazia. Similarmente, NIS 2 reconhece a importância da proteção de dados, estabelecendo que medidas de cibersegurança devem respeitar seus princípios.[69]

Definições harmonizadas facilitam uma interpretação coordenada. "Dados pessoais" mantém consistência entre GDPR, LED e referências no AI Act, permitindo aplicação coerente. O "Tratamento" é igualmente harmonizado, facilitando a compreensão de quando diferentes instrumentos se aplicam.[70]

Os princípios transversais permeiam todos os instrumentos, criando uma linguagem comum. A proporcionalidade orienta tanto obrigações de proteção de dados quanto requisitos de cibersegurança e salvaguardas de IA. A a*ccountability* manifesta-se em todos através de obrigações de documentação, avaliação de impacto e demonstração de conformidade.[71]

---

[67] VÉLIZ, Carissa. *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. London: Bantam, 2020.
[68] HINTZ, Arne; DENCIK, Lina; WAHL-JORGENSEN, Karin. *Digital Citizenship in a Datafied Society*. Cambridge: Polity Press, 2019.
[69] VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press, 2018.
[70] SRNICEK, Nick. *Platform Capitalism*. Cambridge: Polity Press, 2017.
[71] GILLESPIE, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press, 2018.

5.2 Coordenação institucional e procedimental

A coordenação institucional entre diferentes autoridades de supervisão constitui elemento crucial para a eficácia do modelo integrado. O EDPB se coordena com outras autoridades europeias para assegurar uma interpretação consistente dos requisitos, especialmente quando se intersectam com outros domínios regulatórios.[72]

Os procedimentos harmonizados para avaliação e supervisão facilitam implementação coordenada. *"Data Protection Impact Assessment*", (DPIAs) podem ser integradas com avaliações de risco de IA e cibersegurança, criando abordagem holística para gestão de riscos digitais - integração reduzindo custos administrativos e melhorando a qualidade das avaliações.[73]

Orientações conjuntas e documentos de trabalho esclarecem como os instrumentos devem ser aplicados coordenadamente. O EDPB desenvolveu orientações sobre intersecção entre proteção de dados e IA, enquanto a ENISA produziu documentos sobre integração entre cibersegurança e proteção de dados.[74]

Mecanismos de consulta entre autoridades asseguram que decisões em um domínio considerem impactos em outros. Autoridades de proteção de dados consultam as de cibersegurança ao avaliar medidas de segurança, enquanto autoridades de IA consideram implicações de proteção de dados ao avaliar sistemas de alto risco.[75]

5.3 Sinergias operacionais e benefícios integrados

A integração sistêmica produz sinergias operacionais, beneficiando tanto organizações que devem cumprir requisitos quanto cidadãos protegidos. Sinergias manifestam-se em múltiplas dimensões, criando valor adicional e justificando complexidade do sistema integrado.[76]

---

[72] EUROPEAN DATA PROTECTION BOARD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Brussels: EDPB, 2019.
[73] ROBERTS, Sarah T. *Behind the Screen: Content Moderation in the Shadows of Social Media*. New Haven: Yale University Press, 2019.
[74] TUFEKCI, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press, 2017.
[75] MOROZOV, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs, 2013.
[76] WINNER, Langdon. Do Artifacts Have Politics? *Daedalus*, v. 109, n. 1, p. 121-136, 1980.

A eficiência operacional resulta da eliminação de duplicações e conflitos. Organizações podem desenvolver estratégias unificadas, atendendo simultaneamente a requisitos de proteção de dados, governança de IA e cibersegurança. As medidas implementadas para um objetivo frequentemente contribuem para outros, reduzindo custos totais.[77]

A proteção abrangente assegura cobertura holística de todos os aspectos da governança digital. A combinação de proteção de dados, governança de IA e cibersegurança cria um sistema multinível abordando diferentes tipos de riscos coordenadamente. Lacunas que poderiam existir em abordagens setoriais são eliminadas através da integração.[78]

Inovação responsável é facilitada através de um quadro regulatório oferecendo segurança jurídica para desenvolvimento tecnológico. As organizações podem inovar com confiança, sabendo que o cumprimento dos requisitos integrados assegura conformidade com todos os aspectos relevantes. A segurança jurídica facilita investimentos em tecnologias emergentes.[79]

A confiança institucional é fortalecida através de proteção coordenada, demonstrando compromisso institucional com direitos fundamentais. Cidadãos podem confiar em que interações com órgãos públicos são protegidas por um sistema robusto e abrangente de salvaguardas digitais.[80]

5.4 Ciclo integrado de governança digital

Figura V - Ciclo Integrado de Governança Digital
Fonte: Elaboração própria baseada na análise dos institutos europeus.

[77] LESSIG, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006.
[78] NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2009.
[79] SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.
[80] BENNETT, Colin J.; RAAB, Charles D. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: MIT Press, 2006.

O ciclo integrado representa materialização prática da integração sistêmica, estabelecendo processo contínuo de avaliação, implementação, monitorização e melhoria. Assegura, assim, conformidade dinâmica com múltiplos requisitos. Reconhece que a governança digital não é um estado estático, mas um processo evolutivo, adaptando-se continuamente às mudanças tecnológicas e regulatórias.[81]

A fase de avaliação constitui o ponto de partida, envolvendo a análise sistemática dos riscos digitais e dos requisitos regulatórios aplicáveis. Deve considerar simultaneamente riscos de proteção de dados (DPIA), riscos de IA (avaliações de conformidade), riscos de cibersegurança (análises de risco) e requisitos específicos do setor judicial. A integração dessas dimensões permite uma visão holística, facilitando o desenvolvimento de estratégias de mitigação coordenadas.[82]

A fase de implementação materializa estratégias através de medidas técnicas e organizacionais coordenadas. Deve considerar interdependências entre medidas e assegurar que soluções atendam simultaneamente a múltiplos requisitos. Exemplo: sistemas de gestão de identidade podem contribuir para a proteção de dados (controlo de acesso), governança de IA (supervisão humana) e cibersegurança (autenticação robusta).[83]

A fase de monitorização estabelece mecanismos contínuos de supervisão, permitindo detectar desvios e identificar oportunidades de melhoria. Deve abranger todas as dimensões da governança digital usando indicadores, capturando tanto conformidade formal quanto eficácia substantiva. As tecnologias de monitorização automatizada podem facilitar, mas devem ser complementadas por avaliações humanas regulares.[84]

A fase de melhoria fecha o ciclo através da análise dos resultados e implementação de ajustes necessários. Deve considerar não apenas os resultados internos, mas também a evolução do panorama regulatório e tecnológico. A melhoria contínua assegura que a governança permaneça eficaz e atualizada face às mudanças constantes no ambiente digital.

---

[81] REGAN, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.
[82] REGAN, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.
[83] SCHWARTZ, Paul M. *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*. *Harvard Law Review*, v. 126, n. 7, p. 1966-2009, 2013.
[84] BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020.

6 PROPOSTAS INOVADORAS PARA O MINISTÉRIO PÚBLICO BRASILEIRO

Uma análise comparativa do modelo europeu integrado revela oportunidades significativas para o aperfeiçoamento da governança digital no MP brasileiro, particularmente através da evolução e especialização das estruturas estabelecidas pela Resolução CNMP n. 281/2023. As propostas baseiam-se na experiência europeia, mas adaptadas às especificidades do contexto jurídico e institucional brasileiro, visando a criar soluções inovadoras posicionando o MP na vanguarda da governança digital no sistema de justiça.[85]

6.1 Especialização da UEPDAP em inteligência artificial e tecnologias emergentes

A Unidade Especial de Proteção de Dados Pessoais do Conselho Nacional do Ministério Público (UEPDAP/CNMP), estabelecida pela Resolução n. 281/23, representa uma inovação institucional significativa, podendo ser expandida para abordar desafios emergentes relacionados à IA e outras tecnologias disruptivas. A expansão não requer alteração fundamental da estrutura existente, mas o desenvolvimento de competências especializadas e adaptação de procedimentos para abranger novas dimensões da governança digital.[86]

6.1.1 Modelo técnico de especialização

A especialização proposta baseia-se no modelo de competências integradas do AI Act europeu, adaptado às especificidades do MP brasileiro. Reconhece que a proteção de dados e governança de IA não são apenas dimensões complementares requerendo abordagens coordenadas, mas também competências técnicas específicas.[87]

As competências em avaliação de risco de IA constituem o núcleo da especialização. A UEPDAP deve desenvolver capacidade para avaliar sistemas utilizados ou propostos,

[85] BRASIL. Conselho Nacional do Ministério Público. *Resolução nº 281, de 14 de dezembro de 2023*. Estabelece diretrizes para a proteção de dados pessoais no âmbito do Ministério Público. Brasília: CNMP, 2023.
[86] YOUNG, Alasdair R. *The European Union as a global regulator? Context and comparison*. *Journal of European Public Policy*, v. 22, n. 9, p. 1233-1252, 2015.

[87] LAVENEX, Sandra. *A governance perspective on the European neighbourhood policy: integration beyond conditionality? Journal of European Public Policy*, v. 15, n. 6, p. 938-955, 2008.

considerando não apenas a proteção de dados, mas também a equidade, a transparência, a robustez e a supervisão humana. A avaliação deve seguir metodologias baseadas no AI Act, adaptadas ao contexto brasileiro.[88]

As competências em transparência e explicabilidade são essenciais para assegurar que os sistemas sejam compreensíveis e auditáveis. A UEPDAP deve avaliar se os sistemas fornecem explicações adequadas para decisões e se são compreensíveis para utilizadores. Isto é particularmente importante no contexto judicial, onde decisões devem ser justificadas e transparentes.[89]

As competências em supervisão humana asseguram que os sistemas sejam usados como ferramentas de apoio, não substitutos do julgamento humano. A UEPDAP deve avaliar se os sistemas permitem supervisão eficaz e se os utilizadores têm formação adequada. A manutenção do controle humano é fundamental para preservar a responsabilidade institucional e a independência funcional do MP.[90]

6.1.2 Estrutura Técnica Proposta

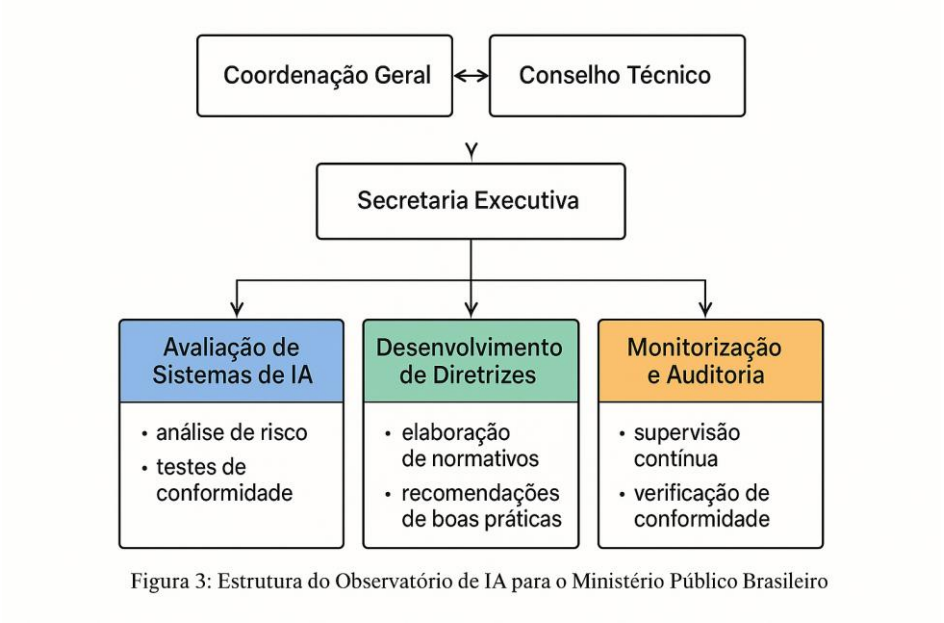

Figura 3: Estrutura do Observatório de IA para o Ministério Público Brasileiro

Figura III - Estrutura Técnica Proposta para a UEPDAP Especializada
Fonte: Elaboração própria baseada na análise do modelo europeu e da Resolução n. 281/2023.

[88] BÖRZEL, Tanja A.; RISSE, Thomas. *From Europeanisation to diffusion: introduction*. *West European Politics*, v. 35, n. 1, p. 1-19, 2012.
[89] SCHIMMELFENNIG, Frank; SEDELMEIER, Ulrich. *Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe*. *Journal of European Public Policy*, v. 11, n. 4, p. 661-679, 2004.
[90] RADAELLI, Claudio M. *The Europeanization of public policy*. In: FEATHERSTONE, Kevin; RADAELLI, Claudio M. (Eds.). *The Politics of Europeanization*. Oxford: Oxford University Press, 2003. p. 27-56.

A estrutura técnica proposta baseia-se na criação de divisões especializadas abordando diferentes aspectos da governança digital integrada. Deve ser flexível e adaptável, permitindo ajustes conforme a evolução das necessidades e da tecnologia.[91]

A Divisão de Avaliação de Sistemas de IA seria responsável pela análise técnica dos sistemas utilizados ou propostos. Conduziria avaliações de risco, análises de impacto e auditorias técnicas, assegurando que os sistemas atendam aos padrões. Manteria também registro de sistemas aprovados e características técnicas, facilitando gestão e supervisão contínua.[92]

A Divisão de Políticas e Normas desenvolveria diretrizes internas para utilização de IA, baseadas em melhores práticas internacionais adaptadas às especificidades do MP. Seria responsável pela elaboração de políticas, procedimentos e protocolos orientando implementação responsável de IA. Ela se coordenaria com outras instituições para harmonizar abordagens e partilhar experiências.[93]

A Divisão de Formação e Capacitação desenvolveria programas de formação especializada em IA para membros e funcionários. Seria responsável pela criação de currículos, materiais didáticos e programas de certificação, assegurando competências adequadas para utilização responsável. A formação deve ser contínua e adaptada aos diferentes perfis profissionais.[94]

A Divisão de Monitorização e Auditoria estabeleceria mecanismos contínuos de supervisão dos sistemas em operação. Seria responsável pela monitorização de desempenho, detecção de anomalias e condução de auditorias periódicas. Manteria sistema de alertas para identificar potenciais problemas e assegurar resposta rápida a incidentes.[95]

---

[91] COWLES, Maria Green; CAPORASO, James; RISSE, Thomas (Eds.). *Transforming Europe: Europeanization and Domestic Change*. Ithaca: Cornell University Press, 2001.
[92] HÉRITIER, Adrienne et al. *Differential Europe: The European Union Impact on National Policymaking*. Lanham: Rowman & Littlefield, 2001.

[93] KNILL, Christoph; LEHMKUHL, Dirk. *The national impact of European Union regulatory policy: Three Europeanization mechanisms*. *European Journal of Political Research*, v. 41, n. 2, p. 255-280, 2002.
[94] BULMER, Simon; RADAELLI, Claudio M. *The Europeanisation of national policy? Queen's Papers on Europeanisation*, n. 1, 2004.
[95] VINK, Maarten P.; GRAZIANO, Paolo (Eds.). *Europeanization: New Research Agendas*. Basingstoke: Palgrave Macmillan, 2007.

6.2 Observatório de inteligência artificial e proteção de dados

A criação de um Observatório de IA e Proteção de Dados para o MP brasileiro representa uma proposta inovadora visando a posicionar a instituição na vanguarda da governança digital. Funcionaria como um centro de excelência, combinando funções de pesquisa, desenvolvimento, monitoramento e disseminação de conhecimento.[96]

6.2.1 Missão e objetivos estratégicos

A missão do Observatório consiste em promover a utilização responsável e eficaz da IA no MP brasileiro, assegurando que a tecnologia sirva aos objetivos institucionais, respeitando direitos fundamentais dos cidadãos. Reflete o equilíbrio necessário entre inovação tecnológica e proteção de direitos, caracterizando o modelo europeu.[97]

Os objetivos de pesquisa e desenvolvimento visam a estabelecer o Observatório como centro de referência em IA aplicada ao sistema de justiça. Inclui a condução de pesquisas sobre aplicações no contexto ministerial, desenvolvimento de soluções tecnológicas inovadoras e colaboração com instituições acadêmicas. As pesquisas devem orientar-se para problemas práticos enfrentados pelo MP e contribuir para o avanço do conhecimento global.[98]

Os objetivos de monitorização e avaliação estabelecem o Observatório como responsável pela supervisão contínua da utilização de IA no MP. Inclui monitorização de desempenho dos sistemas, avaliação de impactos e identificação de tendências emergentes. Deve basear-se em indicadores objetivos e metodologias rigorosas, permitindo avaliação científica dos resultados.[99]

Os objetivos de capacitação e disseminação visam a assegurar que o conhecimento desenvolvido seja eficazmente transferido para a prática institucional. Inclui formação de membros e funcionários, elaboração de publicações técnicas e organização de eventos de

---

[96] GRAZIANO, Paolo; VINK, Maarten P. *Europeanization: New Research Agendas*. Basingstoke: Palgrave Macmillan, 2008.

[97] EXADAKTYLOS, Theofanis; RADAELLI, Claudio M. (Eds.). *Research Design in European Studies: Establishing Causality in Europeanization*. Basingstoke: Palgrave Macmillan, 2012.

[98] FALKNER, Gerda et al. *Complying with Europe: EU Harmonisation and Soft Law in the Member States*. Cambridge: Cambridge University Press, 2005.

[99] TREIB, Oliver. *Implementing and complying with EU governance outputs*. *Living Reviews in European Governance*, v. 1, n. 1, 2006.

disseminação. A capacitação deve adaptar-se às diferentes necessidades e perfis profissionais.[100]

Os objetivos de cooperação institucional estabelecem o Observatório como ponto focal para colaboração com outras instituições nacionais e internacionais. Inclui participação em redes de cooperação, intercâmbio de experiências e desenvolvimento de projetos conjuntos. A cooperação deve facilitar aprendizagem mútua e harmonização de abordagens entre jurisdições.[101]

6.2.2 Estrutura organizacional

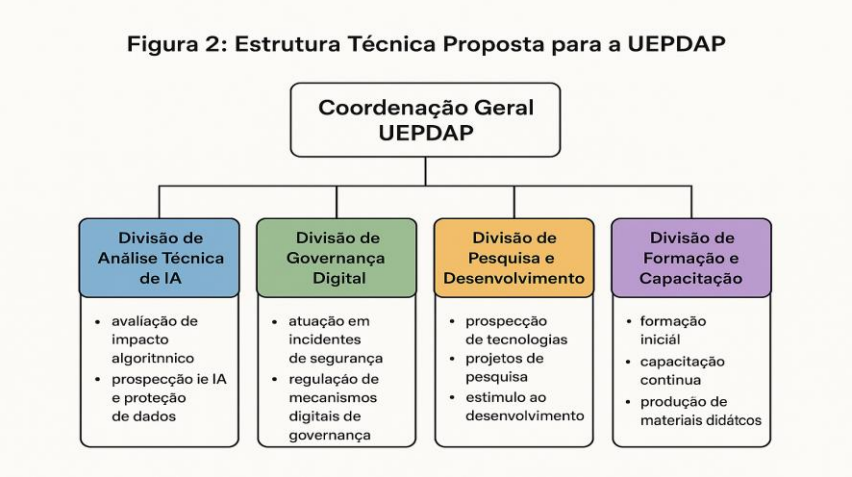

Figura 2 - Estrutura Organizacional do Observatório de IA e Proteção de Dados
Fonte: Elaboração própria baseada nas melhores práticas internacionais.

A estrutura organizacional proposta baseia-se em modelo matricial, combinando especialização técnica com flexibilidade operacional. Deve ser suficientemente robusta para assegurar continuidade institucional, mas flexível para adaptar-se às mudanças tecnológicas e organizacionais.[102]

A Coordenação Geral seria responsável pela liderança estratégica do Observatório, incluindo desenvolvimento de políticas, coordenação com outras unidades do MP e

[100] THOMSON, Robert. *The Council Presidency in the European Union: Responsibility with Power*. Basingstoke: Palgrave Macmillan, 2006.
[101] TALLBERG, Jonas. *Leadership and Negotiation in the European Union*. Cambridge: Cambridge University Press, 2006.

[102] BEACH, Derek. *The Dynamics of European Integration: Why and When EU Institutions Matter*. Basingstoke: Palgrave Macmillan, 2005.

representação externa. O Coordenador seria escolhido entre membros do MP com experiência em tecnologia e gestão, assegurando legitimidade institucional e competência técnica.[103]

O Conselho Técnico seria composto por especialistas internos e externos, incluindo membros do MP, acadêmicos, especialistas em tecnologia e representantes da sociedade civil. Seria responsável pela orientação técnica, incluindo aprovação de projetos e avaliação de resultados. A diversidade de perspectivas asseguraria abordagem equilibrada e credibilidade científica.[104]

A Secretaria Executiva seria responsável pela gestão operacional, incluindo administração de projetos, gestão de recursos e apoio às atividades de pesquisa. Composta por funcionários especializados em gestão de projetos tecnológicos, asseguraria coordenação eficaz entre áreas.[105]

A Área de Pesquisa e Desenvolvimento conduziria projetos de investigação sobre aplicações de IA no contexto ministerial. Composta por pesquisadores com formação em ciência da computação, direito e áreas relacionadas, manteria colaborações com universidades e centros de pesquisa, ampliando capacidade investigativa.[106]

A Área de Avaliação e Monitorização seria responsável pela supervisão contínua dos sistemas utilizados pelo MP. Desenvolveria metodologias de avaliação, conduziria auditorias técnicas e manteria sistemas de monitorização automatizada. Seria composta por especialistas em auditoria de sistemas e análise de dados.[107]

A Área de Capacitação e Disseminação desenvolveria programas de formação e materiais educativos sobre IA. Seria responsável pela organização de cursos, seminários e conferências, bem como elaboração de publicações técnicas. Manteria também plataformas digitais para disseminação de conhecimento e facilitação de colaboração.[108]

---

[103] RITTBERGER, Berthold. *Building Europe's Parliament: Democratic Representation Beyond the Nation State*. Oxford: Oxford University Press, 2005.
[104] HIX, Simon; HØYLAND, Bjørn. *The Political System of the European Union*. 3. ed. Basingstoke: Palgrave Macmillan, 2011.

[105] NUGENT, Neill. *The Government and Politics of the European Union*. 8. ed. Basingstoke: Palgrave Macmillan, 2017.
[106] WALLACE, Helen; POLLACK, Mark A.; YOUNG, Alasdair R. (Eds.). *Policy-Making in the European Union*. 7. ed. Oxford: Oxford University Press, 2015.
[107] PETERSON, John; SHACKLETON, Michael (Eds.). *The Institutions of the European Union*. 4. ed. Oxford: Oxford University Press, 2017.
[108] CINI, Michelle; PÉREZ-SOLÓRZANO BORRAGÁN, Nieves (Eds.). *European Union Politics*. 6. ed. Oxford: Oxford University Press, 2019.

7 CONCLUSÕES E RECOMENDAÇÕES

A análise comparativa do modelo europeu integrado de proteção de dados no sistema de justiça revela a emergência de paradigma sofisticado de governança digital, equilibrando eficácia institucional, inovação tecnológica e proteção de direitos fundamentais. Este modelo, construído através da articulação harmoniosa entre GDPR, LED, AI Act e NIS 2, oferece lições valiosas para outras jurisdições que estejam enfrentando desafios similares na modernização de seus sistemas de justiça.[109]

7.1 Síntese dos principais achados

A investigação revela que o sucesso do modelo europeu se baseia em cinco elementos fundamentais, reforçando-se mutuamente. Primeiro: a abordagem baseada em princípios permite flexibilidade na implementação, mantendo coerência conceitual. Princípios de proporcionalidade, responsabilização, transparência, supervisão humana e proteção por conceção permeiam todos os instrumentos, criando linguagem comum de governança digital.[110]

Segundo: a especialização normativa reconhece que diferentes contextos requerem diferentes abordagens regulatórias. A existência de instrumentos específicos para âmbito penal (LED), para IA (AI Act) e para cibersegurança (NIS 2) permite adaptação às especificidades sem comprometer a coerência sistêmica.[111]

Terceiro: a coordenação institucional assegura que diferentes autoridades trabalhem harmoniosamente, evitando conflitos de competência e duplicações desnecessárias. Os mecanismos de cooperação entre autoridades de proteção de dados, cibersegurança e outras entidades facilitam a implementação coordenada e a resposta eficaz a desafios emergentes.[112]

Quarto: a supervisão adaptada reconhece especificidades do contexto judicial, particularmente a importância da independência. A exclusão dos tribunais da supervisão direta

[109] DINAN, Desmond. *Ever Closer Union: An Introduction to European Integration*. 4. ed. Basingstoke: Palgrave Macmillan, 2010.
[110] ROSAMOND, Ben. *Theories of European Integration*. Basingstoke: Palgrave Macmillan, 2000.
[111] WIENER, Antje; DIEZ, Thomas (Eds.). *European Integration Theory*. 2. ed. Oxford: Oxford University Press, 2009.
[112] HAAS, Ernst B. *The Uniting of Europe: Political, Social, and Economic Forces 1950-1957*. Stanford: Stanford University Press, 1958.

das autoridades de proteção de dados é compensada por mecanismos de supervisão interna e formação especializada, preservando tanto independência quanto proteção de dados.[113]

Quinto: a evolução contínua permite que o modelo se adapte às mudanças tecnológicas e sociais. A capacidade de atualizar e refinar instrumentos assegura que eles permaneçam relevantes e eficazes face às transformações constantes do ambiente digital.[114]

7.2 Implicações para o Ministério Público brasileiro

As implicações da análise para o MP brasileiro são múltiplas e significativas. A instituição encontra-se em posição única para liderar a transformação digital do sistema de justiça nacional, aproveitando sua autonomia funcional e administrativa para implementar soluções inovadoras baseadas em melhores práticas internacionais.[115]

A especialização da UEPDAP em IA representa oportunidade de posicionar o MP na vanguarda da governança de IA no sistema de justiça. Essa especialização deve ser implementada gradualmente, começando com a capacitação das equipes existentes e evoluindo para a criação de competências técnicas avançadas, permitindo supervisão eficaz de sistemas de IA.[116]

A criação do Observatório oferece plataforma para desenvolvimento de conhecimento especializado e disseminação de boas práticas. Pode servir como modelo para outras instituições do sistema de justiça, facilitando a harmonização de abordagens e o desenvolvimento de padrões nacionais de excelência.[117]

A integração entre proteção de dados, governança de IA e cibersegurança deve ser prioridade estratégica, reconhecendo que essas dimensões são complementares e se reforçam mutuamente. A abordagem integrada reduz custos, melhora a eficácia e facilita conformidade com múltiplos requisitos regulatórios.[118]

---

[113] MITRANY, David. *A Working Peace System*. Chicago: Quadrangle Books, 1966.
[114] MORAVCSIK, Andrew. *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*. Ithaca: Cornell University Press, 1998.
[115] ANDHOLTZ, Wayne; STONE SWEET, Alec (Eds.). *European Integration and Supranational Governance*. Oxford: Oxford University Press, 1998.
[116] PIERSON, Paul. *The Path to European Integration: A Historical Institutionalist Analysis*. Comparative Political Studies, v. 29, n. 2, p. 123-163, 1996.
[117] POLLACK, Mark A. *The Engines of European Integration: Delegation, Agency, and Agenda Setting in the EU*. Oxford: Oxford University Press, 2003.
[118] STONE SWEET, Alec; SANDHOLTZ, Wayne; FLIGSTEIN, Neil (Eds.). *The Institutionalization of Europe*. Oxford: Oxford University Press, 2001.

A cooperação internacional deve ser intensificada, aproveitando redes existentes para aprender com experiências internacionais e contribuir para o desenvolvimento global da governança digital. O MP brasileiro pode desempenhar papel de liderança regional, compartilhando inovações e aprendendo com outras jurisdições.[119]

7.3 Recomendações estratégicas

Com base na análise, apresentam-se recomendações estratégicas para o aperfeiçoamento da proteção de dados no MP brasileiro:

Primeira Recomendação: Implementar gradualmente a especialização da UEPDAP em IA, iniciando com capacitação técnica das equipes existentes e evoluindo para a criação de divisões especializadas. A implementação deve ser acompanhada de investimento em formação contínua e desenvolvimento de competências específicas em avaliação de risco de IA, transparência algorítmica e supervisão humana.[120]

Segunda Recomendação: Criar o Observatório de IA como estrutura complementar à UEPDAP, dotado de autonomia técnica para conduzir pesquisas e desenvolver recomendações. Deve ser estabelecido através de ato normativo específico, definindo missão, objetivos e estrutura, assegurando recursos adequados e legitimidade institucional.[121]

Terceira Recomendação: Desenvolver políticas integradas de governança digital, abordando simultaneamente proteção de dados, governança de IA e cibersegurança. As políticas devem basear-se em avaliações de risco abrangentes e ser regularmente atualizadas para refletir mudanças tecnológicas e regulatórias.[122]

Quarta Recomendação: Estabelecer parcerias estratégicas com universidades, centros de pesquisa e organizações internacionais, facilitando o desenvolvimento de conhecimento especializado. Parcerias devem incluir programas de intercâmbio, projetos conjuntos e iniciativas de capacitação ampliando competências técnicas da instituição.[123]

---

[119] CHECKEL, Jeffrey T. *International Institutions and Socialization in Europe*. Cambridge: Cambridge University Press, 2007.
[120] CHRISTIANSEN, Thomas; JØRGENSEN, Knud Erik; WIENER, Antje (Eds.). *The Social Construction of Europe*. London: SAGE Publications, 2001.
[121] RISSE, Thomas. *A Community of Europeans? Transnational Identities and Public Spheres*. Ithaca: Cornell University Press, 2010.
[122] DELLA PORTA, Donatella; CAIANI, Manuela. *Social Movements and Europeanization*. Oxford: Oxford University Press, 2009.
[123] IMIG, Doug; TARROW, Sidney (Eds.). *Contentious Europeans: Protest and Politics in an Emerging Polity*. Lanham: Rowman & Littlefield, 2001.

Quinta Recomendação: Criar mecanismos de monitorização contínua, permitindo avaliar a eficácia das medidas implementadas e identificar oportunidades de melhoria. Os mecanismos devem incluir indicadores quantitativos e qualitativos, capturando tanto a conformidade formal quanto a eficácia substantiva das políticas de governança digital.[124]

7.4 Perspectivas futuras

As perspectivas futuras para a proteção de dados no sistema de justiça são moldadas por tendências tecnológicas emergentes e evolução do panorama regulatório. A IA continuará transformando as práticas judiciais, criando novas oportunidades, mas também novos desafios, requerendo adaptação contínua dos marcos de governança.[125]

O desenvolvimento de tecnologias de *privacy-by-design* oferece oportunidades para integrar a proteção de dados diretamente nos sistemas tecnológicos, reduzindo a dependência de medidas organizacionais. Essas tecnologias podem facilitar a conformidade e melhorar a proteção efetiva, mas requerem investimento em pesquisa e desenvolvimento.[126]

A crescente importância da cibersegurança exigirá investimentos contínuos em medidas técnicas e organizacionais. A integração entre proteção de dados e cibersegurança tornar-se-á ainda mais importante conforme os sistemas se tornem mais interconectados e as ameaças mais sofisticadas.[127]

A cooperação internacional em matéria de proteção de dados e a governança digital intensificar-se-á, criando oportunidades para a harmonização de abordagens e a partilha de melhores práticas. O Brasil pode desempenhar papel de liderança neste processo, aproveitando a experiência com LGPD e inovações do MP.[128]

A formação e capacitação contínuas tornar-se-ão ainda mais importantes conforme a tecnologia evolui. O desenvolvimento de competências especializadas em proteção de dados,

---

[124] MARKS, Gary; HOOGHE, Liesbet; BLANK, Kermit. *European Integration from the 1980s: State-Centric v. Multi-level Governance*. Journal of Common Market Studies, v. 34, n. 3, p. 341-378, 1996.
[125] HOOGHE, Liesbet; MARKS, Gary. *Multi-Level Governance and European Integration*. Lanham: Rowman & Littlefield, 2001.
[126] BACHE, Ian; FLINDERS, Matthew (Eds.). *Multi-level Governance*. Oxford: Oxford University Press, 2004.
[127] KOHLER-KOCH, Beate; RITTBERGER, Berthold (Eds.). *Debating the Democratic Legitimacy of the European Union*. Lanham: Rowman & Littlefield, 2007.
[128] FOLLESDAL, Andreas; HIX, Simon. *Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik*. *Journal of Common Market Studies*, v. 44, n. 3, p. 533-562, 2006.

IA e cibersegurança será essencial para manter a eficácia das medidas de proteção e assegurar que instituições possam adaptar-se às mudanças tecnológicas.[129]

7.5 Considerações finais

Esta investigação demonstra que a proteção de dados no sistema de justiça é um desafio complexo, requerendo abordagens sofisticadas e integradas. O modelo europeu oferece lições valiosas, mas a sua aplicação em outros contextos requer adaptação cuidadosa às especificidades locais e características institucionais específicas.[130]

O MP brasileiro encontra-se em posição privilegiada para liderar esta transformação, aproveitando a sua autonomia institucional e a excelente base normativa estabelecida pela Resolução CNMP n. 281/2023. Propostas apresentadas nesta investigação oferecem um importante caminho para posicionar a instituição na vanguarda da governança digital, contribuindo tanto para o avanço nacional quanto para o desenvolvimento global de melhores práticas.[131]

O sucesso desta transformação dependerá do compromisso institucional com inovação responsável, investimento em capacitação técnica e desenvolvimento de cultura organizacional orientada à proteção de direitos fundamentais. Proteção de dados não é apenas uma obrigação legal, mas um imperativo ético que reflete o compromisso do MP com os valores democráticos e o Estado de Direito.[132]

A jornada para a excelência em governança digital é contínua e requer adaptação constante às mudanças tecnológicas e sociais. As propostas apresentadas nesse ensaio representam um ponto de partida, não um destino final. O aperfeiçoamento contínuo - baseado em evidências e orientado por princípios - será essencial para manter a relevância e a eficácia das medidas implementadas.

Finalmente, esta investigação contribui para o diálogo global sobre governança digital no sistema de justiça, oferecendo perspectivas que podem enriquecer o debate internacional. A

---

[129] MAJONE, Giandomenico. *Europe's 'Democratic Deficit': The Question of Standards*. *European Law Journal*, v. 4, n. 1, p. 5-28, 1998.
[130] MORAVCSIK, Andrew. *In Defence of the 'Democratic Deficit': Reassessing Legitimacy in the European Union*. *Journal of Common Market Studies*, v. 40, n. 4, p. 603-624, 2002.
[131] SCHARPF, Fritz W. *Governing in Europe: Effective and Democratic?* Oxford: Oxford University Press, 1999.
[132] BRASIL. Conselho Nacional do Ministério Público. *Resolução nº 281, de 14 de dezembro de 2023. Estabelece diretrizes para a proteção de dados pessoais no âmbito do Ministério Público*. Brasília: CNMP, 2023.

experiência brasileira, informada por melhores práticas europeias, mas adaptada às especificidades nacionais, pode inspirar reformas similares em outras jurisdições e contribuir para o desenvolvimento de padrões globais de excelência em proteção de dados no sistema de justiça.

REFERÊNCIAS

ALBRECHT, Jan Philipp. How the GDPR Will Change the World. *European Data Protection Law Review*, v. 2, n. 3, p. 287-289, 2016.

BACHE, Ian; FLINDERS, Matthew (Eds.). *Multi-level Governance*. Oxford: Oxford University Press, 2004.

BAROCAS, Solon; HARDT, Moritz; NARAYANAN, Arvind. *Fairness and Machine Learning: Limitations and Opportunities*. Cambridge: MIT Press, 2023.
BEACH, Derek. *The Dynamics of European Integration: Why and When EU Institutions Matter*. Basingstoke: Palgrave Macmillan, 2005.

BENJAMIN, Ruha. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity Press, 2019.

BENNETT, Colin J.; RAAB, Charles D. *The Governance of Privacy: Policy Instruments in Global Perspective*. Cambridge: MIT Press, 2006.

BINNS, Reuben. Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of Machine Learning Research*, v. 81, p. 149-159, 2018.

BOEHM, Franziska. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*. Berlin: Springer, 2012.

BÖRZEL, Tanja A.; RISSE, Thomas. From Europeanisation to diffusion: introduction. *West European Politics*, v. 35, n. 1, p. 1-19, 2012.

BRADFORD, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018.

BRASIL. Conselho Nacional do Ministério Público. Resolução nº 281, de 14 de dezembro de 2023. Estabelece diretrizes para a proteção de dados pessoais no âmbito do Ministério Público. Brasília: CNMP, 2023.

BULMER, Simon; RADAELLI, Claudio M. The Europeanisation of national policy? *Queen's Papers on Europeanisation*, n. 1, 2004.

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

CHECKEL, Jeffrey T. *International Institutions and Socialization in Europe*. Cambridge: Cambridge University Press, 2007.

CHRISTIANSEN, Thomas; JØRGENSEN, Knud Erik; WIENER, Antje (Eds.). *The Social Construction of Europe*. London: SAGE Publications, 2001.

CINI, Michelle; PÉREZ-SOLÓRZANO BORRAGÁN, Nieves (Eds.). *European Union Politics*. 6. ed. Oxford: Oxford University Press, 2019.

COWLES, Maria Green; CAPORASO, James; RISSE, Thomas (Eds.). *Transforming Europe: Europeanization and Domestic Change*. Ithaca: Cornell University Press, 2001.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, v. 32, n. 2, p. 179-194, 2016.

DELLA PORTA, Donatella; CAIANI, Manuela. *Social Movements and Europeanization*. Oxford: Oxford University Press, 2009.

DINAN, Desmond. *Ever Closer Union: An Introduction to European Integration*. 4. ed. Basingstoke: Palgrave Macmillan, 2010.

EDWARDS, Lilian; VEALE, Michael. Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review*, v. 16, n. 1, p. 18-84, 2017.

EUBANKS, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press, 2018.
EUROPEAN DATA PROTECTION BOARD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*. Brussels: EDPB, 2019.

EUROPEAN DATA PROTECTION BOARD. *Guidelines 10/2020 on restrictions under Article 23 GDPR*. Brussels: EDPB, 2020.

EXADAKTYLOS, Theofanis; RADAELLI, Claudio M. (Eds.). *Research Design in European Studies: Establishing Causality in Europeanization*. Basingstoke: Palgrave Macmillan, 2012.

FALKNER, Gerda et al. *Complying with Europe: EU Harmonisation and Soft Law in the Member States*. Cambridge: Cambridge University Press, 2005.

FLORIDI, Luciano et al. AI4People—An Ethical Framework for a Good AI Society. *Minds and Machines*, v. 28, n. 4, p. 689-707, 2018.

FOLLESDAL, Andreas; HIX, Simon. Why There is a Democratic Deficit in the EU: A Response to Majone and Moravcsik. *Journal of Common Market Studies*, v. 44, n. 3, p. 533-562, 2006.

GILLESPIE, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press, 2018.

GONZÁLEZ FUSTER, Gloria. *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Cham: Springer, 2014.

GRAZIANO, Paolo; VINK, Maarten P. *Europeanization: New Research Agendas*. Basingstoke: Palgrave Macmillan, 2008.

HAAS, Ernst B. *The Uniting of Europe: Political, Social, and Economic Forces 1950-1957*. Stanford: Stanford University Press, 1958.

HAGENDORFF, Thilo. The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds and Machines*, v. 30, n. 1, p. 99-120, 2020.

HÉRITIER, Adrienne et al. *Differential Europe: The European Union Impact on National Policymaking*. Lanham: Rowman & Littlefield, 2001.

HIJMANS, Hielke. *The European Union as Guardian of Internet Privacy*. Cham: Springer, 2016.

HIJMANS, Hielke; KRANENBORG, Herke. *Data Protection Anno 2014: How to Restore Trust?* Cambridge: Intersentia, 2014.

HINTZ, Arne; DENCIK, Lina; WAHL-JORGENSEN, Karin. *Digital Citizenship in a Datafied Society*. Cambridge: Polity Press, 2019.

HIX, Simon; HØYLAND, Bjørn. *The Political System of the European Union*. 3. ed. Basingstoke: Palgrave Macmillan, 2011.

HOOFNAGLE, Chris Jay; VAN DER SLOOT, Bart; BORGESIUS, Frederik Zuiderveen. The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, v. 28, n. 1, p. 65-98, 2019.

HOOGHE, Liesbet; MARKS, Gary. *Multi-Level Governance and European Integration*. Lanham: Rowman & Littlefield, 2001.

IMIG, Doug; TARROW, Sidney (Eds.). *Contentious Europeans: Protest and Politics in an Emerging Polity*. Lanham: Rowman & Littlefield, 2001.

JOBIN, Anna; IENCA, Marcello; VAYENA, Effy. The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, v. 1, n. 9, p. 389-399, 2019.

KAMINSKI, Margot E. The Right to Explanation, Explained. *Berkeley Technology Law Journal*, v. 34, n. 1, p. 189-218, 2019.

KNILL, Christoph; LEHMKUHL, Dirk. The national impact of European Union regulatory policy: Three Europeanization mechanisms. *European Journal of Political Research*, v. 41, n. 2, p. 255-280, 2002.

KOHLER-KOCH, Beate; RITTBERGER, Berthold (Eds.). *Debating the Democratic Legitimacy of the European Union*. Lanham: Rowman & Littlefield, 2007.

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

KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher. *The EU General Data Protection Regulation: A Commentary*. Oxford: Oxford University Press, 2020.

LAVENEX, Sandra. A governance perspective on the European neighbourhood policy: integration beyond conditionality? *Journal of European Public Policy*, v. 15, n. 6, p. 938-955, 2008.

LESSIG, Lawrence. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books, 2006.

LYNSKEY, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015.

MAJONE, Giandomenico. Europe's 'Democratic Deficit': The Question of Standards. *European Law Journal*, v. 4, n. 1, p. 5-28, 1998.

MARKS, Gary; HOOGHE, Liesbet; BLANK, Kermit. European Integration from the 1980s: State-Centric v. Multi-level Governance. *Journal of Common Market Studies*, v. 34, n. 3, p. 341-378, 1996.

MITTELSTADT, Brent. Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, v. 1, n. 11, p. 501-507, 2019.

MITRANY, David. *A Working Peace System*. Chicago: Quadrangle Books, 1966.

MORAVCSIK, Andrew. *The Choice for Europe: Social Purpose and State Power from Messina to Maastricht*. Ithaca: Cornell University Press, 1998.

MORAVCSIK, Andrew. In Defence of the 'Democratic Deficit': Reassessing Legitimacy in the European Union. *Journal of Common Market Studies*, v. 40, n. 4, p. 603-624, 2002.

MORLEY, Jessica et al. The ethics of AI in health care: A mapping review. *Social Science & Medicine*, v. 260, 113172, 2020.

MOROZOV, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs, 2013.

NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford University Press, 2009.

NOBLE, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press, 2018.

NUGENT, Neill. *The Government and Politics of the European Union*. 8. ed. Basingstoke: Palgrave Macmillan, 2017.

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

PETERSON, John; SHACKLETON, Michael (Eds.). *The Institutions of the European Union*. 4. ed. Oxford: Oxford University Press, 2017.

PIERSON, Paul. The Path to European Integration: A Historical Institutionalist Analysis. *Comparative Political Studies*, v. 29, n. 2, p. 123-163, 1996.

POLLACK, Mark A. *The Engines of European Integration: Delegation, Agency, and Agenda Setting in the EU*. Oxford: Oxford University Press, 2003.

RADAELLI, Claudio M. *The Europeanization of public policy*. In: FEATHERSTONE, Kevin;

RADAELLI, Claudio M. (Eds.). *The Politics of Europeanization*. Oxford: Oxford University Press, 2003. p. 27-56.

REGAN, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.

RISSE, Thomas. *A Community of Europeans? Transnational Identities and Public Spheres*. Ithaca: Cornell University Press, 2010.

RITTBERGER, Berthold. *Building Europe's Parliament: Democratic Representation Beyond the Nation State*. Oxford: Oxford University Press, 2005.

ROBERTS, Sarah T. *Behind the Screen: Content Moderation in the Shadows of Social Media*. New Haven: Yale University Press, 2019.

ROSAMOND, Ben. *Theories of European Integration*. Basingstoke: Palgrave Macmillan, 2000.

RUSSELL, Stuart; NORVIG, Peter. *Artificial Intelligence: A Modern Approach*. 4. ed. Boston: Pearson, 2020.

RYAN, Mark; STAHL, Bernd Carsten. Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications. *Journal of Information, Communication and Ethics in Society*, v. 19, n. 1, p. 61-86, 2021.

SANDHOLTZ, Wayne; STONE SWEET, Alec (Eds.). *European Integration and Supranational Governance*. Oxford: Oxford University Press, 1998.

SCHARPF, Fritz W. *Governing in Europe: Effective and Democratic?* Oxford: Oxford University Press, 1999.

SCHIMMELFENNIG, Frank; SEDELMEIER, Ulrich. Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe. *Journal of European Public Policy*, v. 11, n. 4, p. 661-679, 2004.

SCHWARTZ, Paul M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. *Harvard Law Review*, v. 126, n. 7, p. 1966-2009, 2013.

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. *International Data Privacy Law*, v. 7, n. 4, p. 233-242, 2017.

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

SRNICEK, Nick. *Platform Capitalism*. Cambridge: Polity Press, 2017.

STONE SWEET, Alec; SANDHOLTZ, Wayne; FLIGSTEIN, Neil (Eds.). *The Institutionalization of Europe*. Oxford: Oxford University Press, 2001.

TALLBERG, Jonas. *Leadership and Negotiation in the European Union*. Cambridge: Cambridge University Press, 2006.

THOMSON, Robert. *The Council Presidency in the European Union: Responsibility with Power*. Basingstoke: Palgrave Macmillan, 2006.

TREIB, Oliver. Implementing and complying with EU governance outputs. *Living Reviews in European Governance*, v. 1, n. 1, 2006.

TUFEKCI, Zeynep. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. New Haven: Yale University Press, 2017.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119, 4 maio 2016a.

UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que se refere ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais*. Jornal Oficial da União Europeia, L 119, 4 maio 2016b.

UNIÃO EUROPEIA. *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União*. Jornal Oficial da União Europeia, L 333, 27 dez. 2022.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial*.

Jornal Oficial da União Europeia, L 1689, 12 jul. 2024.

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press, 2018.

VEALE, Michael; BINNS, Reuben; EDWARDS, Lilian. Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A*, v. 376, n. 2133, 2018.

VÉLIZ, Carissa. *Privacy Is Power: Why and How You Should Take Back Control of Your Data*. London: Bantam, 2020.

VINK, Maarten P.; GRAZIANO, Paolo (Eds.). *Europeanization: New Research Agendas*. Basingstoke: Palgrave Macmillan, 2007.

VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer, 2017.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, v. 7, n. 2, p. 76-99, 2017.

WALLACE, Helen; POLLACK, Mark A.; YOUNG, Alasdair R. (Eds.). *Policy-Making in the European Union*. 7. ed. Oxford: Oxford University Press, 2015.

WHITMAN, James Q. The Two Western Cultures of Privacy: Dignity Versus Liberty. *Yale Law Journal*, v. 113, n. 6, p. 1151-1221, 2004.

WIENER, Antje; DIEZ, Thomas (Eds.). *European Integration Theory*. 2. ed. Oxford: Oxford University Press, 2009.

WINFIELD, Alan F. T.; JIROTKA, Marina. Ethical governance is essential to building trust in robotics and artificial intelligence systems. *Philosophical Transactions of the Royal Society A*, v. 376, n. 2133, 2018.

WINNER, Langdon. Do Artifacts Have Politics? *Daedalus*, v. 109, n. 1, p. 121-136, 1980.

YOUNG, Alasdair R. The European Union as a global regulator? Context and comparison. *Journal of European Public Policy*, v. 22, n. 9, p. 1233-1252, 2015.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

ZWEIGERT, Konrad; KÖTZ, Hein. *Introduction to Comparative Law*. 3. ed. Oxford: Oxford University Press, 1998.