

DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS

MESTRADO EM RELAÇÕES INTERNACIONAIS

UNIVERSIDADE AUTÓNOMA DE LISBOA

“LUÍS DE CAMÕES”

**SOBERANIA DIGITAL PARTILHADA NO CONTEXTO EUROPEU: O
CASO DE PORTUGAL**

Dissertação para a obtenção do grau de Mestre em Relações Internacionais

Autor: Bruno Jorge Madeira Grácio

Orientador: Professor Daniel Cardoso

Número do Candidato: 30005297

Abril de 2026

Lisboa

Agradecimentos

A concretização desta dissertação representa o culminar de um longo percurso académico e pessoal, que não teria sido possível sem o apoio, a orientação e o incentivo de várias pessoas e instituições que me acompanharam ao longo deste processo.

Em primeiro lugar, manifesto o meu mais profundo agradecimento ao Professor Doutor Daniel Cardoso, meu orientador, pela disponibilidade constante, pela orientação rigorosa e pela confiança depositada neste trabalho. A sua exigência intelectual, o seu espírito crítico e a sua capacidade de motivar foram determinantes para o desenvolvimento desta dissertação e para o meu crescimento académico.

Estendo igualmente o meu reconhecimento a todos os professores e membros do corpo docente que, ao longo do curso, contribuíram para a minha formação, transmitindo conhecimentos, perspectivas e metodologias que se revelaram essenciais para a construção deste projeto.

Aos meus pais, deixo um agradecimento sentido e profundo. O amor, a paciência e o apoio incondicional que sempre me deram foram o alicerce de todo o meu percurso. A eles devo a determinação e os valores que me orientam, bem como a força para alcançar cada etapa deste caminho.

À minha namorada, pelo carinho, paciência e incentivo constante, mesmo nos momentos de maior exigência, deixo o meu sincero agradecimento. Agradeço também à sua família, pela generosidade e apoio contínuo, que foram fundamentais para manter o equilíbrio e a motivação ao longo deste percurso.

Aos meus padrinhos, que sempre acreditaram em mim e acompanharam cada etapa com orgulho e encorajamento, deixo igualmente uma palavra de gratidão.

Aos meus amigos, que estiveram presentes nos momentos de pausa e descontração, oferecendo apoio, compreensão e boas doses de humor quando mais precisei, o meu muito obrigado.

Aos meus colegas de trabalho, e em particular aos da Agência da Baixa da Banheira, agradeço a compreensão, o incentivo e a camaradagem demonstrada ao longo deste processo. A vossa disponibilidade e espírito de equipa tornaram possível conciliar as responsabilidades profissionais com as exigências desta investigação.

Por fim, agradeço a todos aqueles que, de forma direta ou indireta, contribuíram para a realização deste trabalho. Cada palavra de incentivo, cada gesto de apoio e cada demonstração de confiança tiveram um papel importante na concretização deste objetivo que agora se cumpre.

Resumo

Esta dissertação analisa o conceito de soberania digital e a sua materialização na União Europeia (UE), com particular incidência sobre o caso português. Num contexto em que o digital se tornou uma dimensão estruturante do poder político e social, o estudo procura compreender como as noções clássicas de soberania são reconfiguradas perante a crescente interdependência tecnológica. A investigação assenta numa metodologia qualitativa baseada na análise documental, legislativa e estratégica.

Os resultados demonstram que o digital constitui hoje um domínio de soberania partilhada, exercida de forma multinível. A UE emerge como principal agente de regulação através de instrumentos como o RGPD, o DSA, o DMA e a Diretiva NIS2, que estabelecem normas comuns para a proteção de dados, segurança das redes e regulação das plataformas. Portugal ilustra bem esta dinâmica: com limitações estruturais como a dependência de plataformas estrangeiras e reduzida capacidade de inovação endógena, encontra na integração europeia um mecanismo de reforço de poder e resiliência digital.

O conceito central da dissertação — a soberania digital partilhada — descreve a soberania como uma capacidade relacional e cooperativa, exercida por meio de mecanismos regulatórios e infraestruturas interligadas. Não nega o papel do Estado, mas redefine-o: a autoridade preserva-se através da coordenação com entidades supranacionais e atores privados com poder tecnológico.

A dissertação conclui que a soberania digital europeia não representa uma perda de autonomia nacional, mas a sua transformação. Portugal exemplifica esta transição: a soberania digital deixa de ser um ideal de controlo total e passa a ser um processo de cooperação e adaptação às novas condições tecnológicas globais, emergindo como resposta pragmática aos desafios do século XXI.

Palavras-chave: Soberania digital; Portugal; Políticas digitais; Integração europeia.

Abstract

This dissertation examines the concept of digital sovereignty and its materialization within the European Union (EU), with a particular focus on the Portuguese case. In a global environment where the digital sphere has become central to political, economic, and social power, the study investigates how classical notions of sovereignty are being reconfigured amid increasing technological interdependence. The research adopts a qualitative methodology based on documentary, legislative, and strategic analysis.

The findings indicate that the digital domain has evolved into a shared sphere of sovereignty, governed through multi-level and techno-political structures. The EU has emerged as a central regulatory actor through instruments such as the GDPR, DSA, DMA, and the NIS2 Directive, establishing common standards for data protection, network security, and platform regulation. Portugal illustrates this dynamic clearly: constrained by structural limitations — dependence on foreign platforms and limited endogenous innovation — the country leverages European integration as a power-enhancing mechanism, strengthening its digital resilience through institutional coordination.

The dissertation's central contribution is the concept of shared digital sovereignty, which defines sovereignty as a relational and cooperative capacity exercised through regulatory mechanisms and interconnected infrastructures. It does not negate the role of the State but redefines it: authority is preserved through coordination with supranational entities and private actors holding technological power.

The dissertation concludes that European digital sovereignty does not entail the loss of national autonomy but its transformation. Portugal embodies this transition, where digital sovereignty evolves from an abstract ideal of absolute control into a practical process of cooperation and adaptation — a pragmatic response to the challenges of the twenty-first century.

Keywords: Digital sovereignty; Portugal; Digital policies; European integration.

Índice

Introdução.....	10
1. Enquadramento teórico.....	15
1.1. Conceito de Soberania Digital: Definição e Evolução	17
1.2. Supranacionalização e Intergovernamentalismo na União Europeia.....	20
2. Contexto Europeu: O Regulamento Geral de Proteção de Dados (RGPD) e as Implicações para os Estados-Membros.....	30
2.1 - Schrems II.....	33
2.2 - CSA - Regulation to Prevent and Combat Child Sexual Abuse	34
2.3. Diretiva NIS e a Segurança das Redes e Sistemas de Informação	39
3. O Caso de Portugal: Soberania Digital e Integração Europeia	47
3.1. Infraestruturas Digitais em Portugal: Dependência de Plataformas Externas	50
3.3. Parcerias com Empresas Estrangeiras no Setor Tecnológico.....	61
3.4. O Papel de Portugal nas Políticas Digitais da União Europeia.....	66
3.5 O Papel de Portugal ao nível interno	70
Conclusão.....	75
Referências Bibliográficas.....	80

Acrónimos

AMA – Agência para a Modernização Administrativa

CNCS – Centro Nacional de Cibersegurança

CSA – Regulation to Prevent and Combat Child Sexual Abuse

CSIRT – Computer Security Incident Response Team

CFR – Council on Foreign Relations

DSA – Digital Services Act

DMA – Digital Markets Act

ECA – European Chips Act

EDIH – European Digital Innovation Hub

EDN – Estratégia Digital Nacional

ENISA – Agência da União Europeia para a Cibersegurança

GAIA-X – European Federated Data Infrastructure Project

GEE – Gabinete de Estratégia e Estudos

IA – Inteligência Artificial

ICT / TIC – Information and Communication Technologies / Tecnologias da Informação e Comunicação

INCoDe.2030 – Iniciativa Nacional de Competências Digitais e.2030

IoT – Internet of Things (Internet das Coisas)

NATO – Organização do Tratado do Atlântico Norte

NIS / NIS2 – Diretiva sobre Segurança das Redes e da Informação (versão revista)

OCDE – Organização para a Cooperação e Desenvolvimento Económico

OES – Operadores de Serviços Essenciais

PRR – Plano de Recuperação e Resiliência

RGPD – Regulamento Geral sobre a Proteção de Dados

PME – Pequenas e Médias Empresas

UE – União Europeia

Lista de figuras

Figura 1. Esquema conceptual inspirado no modelo em camadas de “The Stack”, de Benjamin Bratton (2015).	26
Figura 2. Diagrama conceptual que sintetiza o RGPD.	31
Figura 3. Diagrama que ilustra que o tribunal considerou o Privacy Shield inadequado devido à possibilidade de vigilância governamental norte-americana.	34
Figura 4. Representação simplificada do processo de encriptação ponta-a-ponta (E2EE).	36
Figura 5. Dependência digital europeia face à China e aos EUA (2019)..	46

Introdução

O que acontece quando um Estado “perde” o controlo sobre os seus próprios dados e infraestruturas digitais? Esta pergunta torna-se cada vez mais urgente num mundo onde a informação e a tecnologia determinam relações de poder e competitividade. A soberania digital emerge, assim, como um conceito estratégico mas paradoxal que implica simultaneamente autonomia nacional e partilha de decisões num bloco supranacional.

Embora existam diversos estudos que abordam a soberania digital no plano global e europeu, a literatura tende a concentrar-se em grandes potências tecnológicas, como os Estados Unidos, a China e a própria União Europeia (Floridi, 2020; DeNardis, 2014; Zuboff, 2019). Autores como Bellanova, Carrapico e Duez (2022) e Broeders, Cristiano e Kaminska (2023) analisam a governação digital europeia e o papel da UE como poder normativo global, enquanto Metakides (2021) e Rone (2024) discutem a soberania digital como instrumento de autonomia estratégica do bloco. No entanto, permanece pouco explorado o modo como Estados de média dimensão, como Portugal, vivenciam essa soberania num contexto de forte dependência tecnológica e integração supranacional. Falta compreender como o país equilibra a autonomia tecnológica com as exigências de harmonização digital de Bruxelas e de que forma a dependência de infraestruturas externas (EUA, China) condiciona a sua soberania. Assim, esta dissertação procura responder à seguinte questão central: como se configura a soberania digital partilhada no contexto europeu, tomando Portugal como caso de estudo?

Nos últimos anos, as tecnologias digitais passaram a desempenhar um papel central em todos os domínios da vida económica, social e política. A pandemia de *Covid-19* acelerou dramaticamente a adoção de soluções digitais em Portugal e na Europa, impulsionando serviços públicos e privados para o meio digital. De igual modo, o conflito na Ucrânia revelou que os alvos estratégicos não se limitam ao espaço físico, mas atingem também o espaço digital. Nesse contexto, a expressão soberania digital ganhou relevo nas agendas nacionais e europeias. Tal conceito refere-se à capacidade de um Estado ou bloco regional gerir autonomamente a sua infraestrutura digital, dados e políticas tecnológicas, protegendo simultaneamente os interesses dos cidadãos e os seus valores fundamentais. Com base nos trabalhos consultados e na pesquisa realizada, o presente estudo propõe a seguinte definição operacional: a soberania digital consiste

na capacidade de um Estado agir de forma independente e segura no domínio digital, preservando o controlo sobre os seus dados, infraestruturas e políticas tecnológicas. Esta definição alinha-se com as abordagens de Floridi (2020), DeNardis (2014) e Zinovieva & Bulva (2021), que entendem a soberania digital como uma extensão funcional da soberania clássica, expressa na autonomia normativa e tecnológica face a atores externos. A necessidade de assegurar essa autonomia estratégica tem-se tornado evidente em face das vulnerabilidades globais: por exemplo, as dificuldades no acesso a semicondutores essenciais demonstraram quão dependente continua a ser a Europa de potências tecnológicas externas.

A nível europeu, a soberania digital converteu-se num objetivo estratégico explícito. Nas orientações políticas da Comissão Europeia para 2019-2024, reforçar a soberania digital da União Europeia (UE) foi destacado como meta central. Neste período, a UE aprovou legislação inovadora no domínio digital: destacam-se o *Digital Markets Act* (DMA)¹ e o *Digital Services Act* (DSA)² – visando regular grandes plataformas digitais – bem como a pioneira Lei da Inteligência Artificial (IA). Paralelamente, o Regulamento Geral de Proteção de Dados (RGPD), estabeleceu padrões rigorosos de privacidade, projetando valores europeus no tratamento de dados pessoais. Estes diplomas europeus alargam o alcance da UE uma vez que empresas que atuam no mercado interno devem cumprir normas definidas em Bruxelas.

Em linha com estas iniciativas, a estratégia *Shaping Europe's Digital Future* (enquadrada na Década Digital 2021-2030) reforça a ambição europeia de “alcançar uma maior soberania digital num contexto global”. No âmbito desta visão, o Programa Europa Digital (2021-2027) canaliza investimentos substanciais (mais de 7,5 mil milhões de euros) para tecnologias críticas – como supercomputação, inteligência artificial, cibersegurança e *big data* – com vista a aumentar a autonomia tecnológica do bloco. Assim, através de políticas comuns e do financiamento de infraestruturas e competências digitais, a UE procura moldar a sua agenda tecnológica e harmonizar as políticas digitais dos Estados-Membros. Num mundo cada vez mais interligado, este enquadramento europeu impõe-se aos países do bloco, influenciando decisivamente as escolhas nacionais em matérias digitais.

¹ *Regulamento (UE) 2022/1925* — visa assegurar mercados digitais justos e contestáveis na União, impondo obrigações específicas às grandes plataformas em linha (“gatekeepers”), a fim de limitar práticas anti concorrenciais e promover a inovação.

² *Regulamento (UE) 2022/2065* — estabelece um regime de responsabilidade e transparência para os prestadores de serviços digitais, impondo deveres de diligência, supervisão e moderação de conteúdos em plataformas em linha, em conformidade com os direitos fundamentais europeus.

O presente estudo centra-se na União Europeia, com especial enfoque em Portugal, e considera o período 2014–2024. O ano de 2014 foi escolhido por assinalar o início de uma fase estruturante da política digital europeia, marcada pela adoção da Estratégia para o Mercado Único Digital e pelo reforço das competências da Comissão Europeia no domínio da economia e sociedade digitais. Nesse ano, o então Comissário Günther Oettinger assumiu a pasta da Economia Digital, impulsionando a formulação de políticas integradas de conectividade, dados e cibersegurança que viriam a culminar no Regulamento Geral de Proteção de Dados (RGPD, 2018) e, posteriormente, no *Digital Single Market Strategy* (2015). Este recorte temporal permite, portanto, acompanhar a evolução da soberania digital europeia desde o início da consolidação das suas bases políticas e regulatórias até à atual Década Digital (2021–2030), abrangendo as principais iniciativas de integração digital e os seus impactos em Portugal.

Portugal integra-se neste cenário através das suas próprias estratégias nacionais (por exemplo, o Plano de Ação para a Transição Digital, 2020) alinhadas às diretivas europeias. Neste âmbito, salientam-se também iniciativas como o Plano de Recuperação e Resiliência, que direcionou cerca de 22% dos seus fundos (aproximadamente 4,5 mil milhões de euros) à transição digital em Portugal. Esta delimitação permite analisar o processo evolutivo das políticas de soberania digital da UE e a sua articulação com as políticas portuguesas ao longo da última década.

O quadro europeu de governação digital é marcado por tensões inerentes entre dinamismos supranacionais e interesses intergovernamentais. Por um lado, a UE tende a harmonizar legislações e a centralizar decisões (ex. regulamentações digitais comuns); por outro, os Estados-Membros procuram preservar parcelas da sua autonomia soberana. As iniciativas legislativas europeias (como DSA, DMA e regulamentações de mídia ou IA) foram desenhadas para responder às crises digitais atuais, mas simultaneamente apresentam novos desafios à soberania e à sua perceção dos Estados-Membros. Ou seja, à medida que a UE exerce maior controlo sobre o espaço digital, surge o dilema de equilibrar o controle nacional com a necessária cooperação europeia diante de desafios globais.

Em Portugal este dilema manifesta-se claramente. Portugal é um Estado soberano, mas cuja soberania é exercida no contexto da UE. Isto significa que Portugal voluntariamente limita parte da sua soberania em domínios específicos (como as políticas digitais) em função da participação comunitária. Na Presidência Portuguesa do Conselho da UE (2021/22), o Primeiro-Ministro António Costa sublinhou que a tecnologia e os direitos têm de ser duas faces da mesma moeda, reafirmando um alinhamento total de Portugal com a estratégia digital da UE. O mesmo relatório destaca que Portugal se considera totalmente alinhado com a estratégia europeia no que toca à área digital, em concreto no tema da soberania digital, prevendo inclusive contribuir de forma eficaz para a promoção da soberania digital na UE. A análise destas tensões – entre decisões comunitárias e interesses nacionais – será, portanto, um eixo central deste trabalho.

Um desafio crítico para a soberania digital na Europa (e em Portugal) é a forte dependência de tecnologias e infraestruturas controladas fora do bloco, sobretudo nos EUA e na China. A UE ainda depende significativamente de fornecedores externos de inteligência artificial e outras tecnologias. Esta dependência de insumos tecnológicos externos (*chips*, plataformas *cloud*, equipamentos de rede, etc.) fragiliza a autonomia estratégica europeia e pode condicionar outros objetivos políticos.

Em Portugal, há preocupação com a importação de *hardware* e serviços essenciais (por exemplo, debates sobre fornecedores de 5G ou plataformas de *cloud*) e com a implementação de iniciativas europeias de autonomia (como o projeto GAIA-X, ou redes 5G seguras). Têm-se levantado vozes exigindo uma política europeia unificada de soberania para infraestruturas críticas. Assim, o problema da dependência externa (quer dos EUA, quer da China, quer de outros atores) será examinado nesta dissertação, avaliando em que medida condiciona a soberania digital de Portugal e quais as iniciativas em curso para a mitigar.

A escolha deste tema assenta em motivações pessoais e académicas. Em termos académicos, a soberania digital é um conceito emergente, interdisciplinar e de grande atualidade, cujo desenvolvimento prático suscita questões profundas de poder, política e segurança. Embora a literatura aborde a soberania digital no contexto global ou da UE, há carência de estudos centrados em países de média dimensão como Portugal. Este trabalho visa preencher essa lacuna, aplicando uma ótica de Relações Internacionais para explicar como as dinâmicas de integração europeia afetam a soberania nacional no domínio digital. A perspetiva realista justifica-se porque enfatiza

os interesses estatais e as relações de poder entre entidades (estado nacional, UE, potências estrangeiras). Do ponto de vista pessoal, o tema alinha-se com o interesse nas interseções entre tecnologia, geopolítica e políticas públicas. A relevância política é patente: à medida que a economia e a sociedade se digitalizam, entender a soberania digital é crucial para formular estratégias que garantam competitividade, privacidade e segurança nacional.

Em termos metodológicos, será utilizada uma abordagem qualitativa, incluindo:

- **Revisão bibliográfica e documental:** análise de literatura académica sobre soberania digital e governação tecnológica, de legislações e estratégias oficiais da UE (Jornal Oficial, Comunicados de Bruxelas), e, no caso português, exclusivamente de documentos oficiais de instituições nacionais e europeias (Planos nacionais, discursos oficiais, relatórios do Gabinete de Estratégia e Estudos (GEE), etc.).
- **Análise de discursos políticos:** estudo comparativo de declarações de líderes europeus e portugueses (discursos parlamentares, entrevistas, comunicados) sobre soberania digital bem como instituições e as suas comunicações públicas.
- **Análise comparativa de dados:** uso de indicadores quantificáveis (por exemplo, o Índice da Década Digital da UE, investimento em TI, parcerias tecnológicas) para contextualizar o posicionamento português face à média europeia.

Esta combinação metodológica permitirá traçar um panorama rigoroso da governação digital partilhada, articulando evidências documentais com perceções empíricas. Em síntese, esta investigação pretende clarificar como a soberania digital partilhada se concretiza na prática, contribuindo tanto para o debate académico quanto para o processo de formulação de políticas públicas. Espera-se que os resultados forneçam uma compreensão aprofundada do equilíbrio entre integração europeia e autonomia nacional em matéria digital, destacando os constrangimentos impostos pelas dependências tecnológicas externas. Para o meio académico, o estudo enriquecerá a teoria das relações internacionais aplicando-a a um tema contemporâneo e prático. Politicamente, poderá subsidiar decisores em Portugal e na UE na formulação de estratégias que reforcem a soberania digital, sugerindo caminhos para mitigar dependências e potenciar alianças estratégicas dentro do mercado digital europeu. Como tal, ambiciona-se que esta dissertação seja uma contribuição relevante para a compreensão e o fortalecimento da posição de Portugal na nova arena digital global.

1. Enquadramento teórico

A soberania constitui um dos conceitos estruturantes das Relações Internacionais e um elemento fundacional do sistema político moderno. Tradicionalmente entendida como o poder supremo e exclusivo de um Estado sobre o seu território, população e recursos, a soberania consolidou-se como princípio organizador da ordem vestefaliana, alicerçada na territorialidade e na autoridade centralizada (Caporaso, 2000). No entanto, a transição para uma sociedade interconectada e digitalizada desafiou profundamente esta conceção clássica. O advento da globalização, a interdependência económica e a digitalização das infraestruturas alteraram as fronteiras do poder político, deslocando a soberania do domínio meramente territorial para dimensões tecnológicas e informacionais (Floridi, 2020).

As infraestruturas críticas, os fluxos de dados e os serviços digitais não reconhecem fronteiras físicas e operam através de redes transnacionais, dominadas em larga medida por corporações privadas e plataformas digitais globais. Este fenómeno gera um desequilíbrio entre a autoridade formal do Estado e o controlo efetivo sobre os meios digitais que sustentam a economia, a segurança e a governação contemporânea (Ruohonen, 2020). A soberania, outrora definida pelo monopólio da força física e pela delimitação geográfica, passou a ser também uma questão de capacidade normativa, tecnológica e cibernética. Assim, como sublinha Zinovieva e Bulva (2021), a soberania digital emerge como uma nova dimensão da autonomia política, uma forma de soberania “não territorial”, que se manifesta na regulação de fluxos de dados, no controlo das infraestruturas tecnológicas e na definição de normas de cibersegurança.

A literatura recente tem procurado repensar este conceito face às dinâmicas do ciberespaço. Bellanova, Carrapico e Duez (2022) argumentam que o modelo vestefaliano, assente na autoridade hierárquica e na exclusividade jurisdicional, já não é adequado a uma realidade em rede, caracterizada por interdependências assimétricas e fluxos transfronteiriços de informação. Neste contexto, a soberania digital surge como uma forma de governação distribuída, onde Estados, instituições supranacionais e empresas tecnológicas partilham responsabilidades e poder de regulação (Broeders, Cristiano & Kaminska, 2023).

No espaço europeu, esta tensão manifesta-se de forma particularmente evidente. A União Europeia (UE) assumiu nas últimas décadas um papel central como regulador global, transformando o poder normativo em instrumento de projeção estratégica, o chamado Brussels Effect (Codagnone & Weigl, 2023). Através de instrumentos como o RGPD, o DMA e a Diretiva NIS2, a UE procura consolidar uma soberania digital coletiva, baseada em princípios de confiança, transparência e proteção de direitos fundamentais (Carrapico & Farrand, 2024). Esta abordagem traduz-se numa tentativa de conciliar o duplo imperativo da integração europeia: garantir uniformidade e segurança através da regulação supranacional, sem suprimir completamente as prerrogativas soberanas dos Estados-membros.

Contudo, este processo não está isento de ambiguidades. Por um lado, a soberania digital europeia reforça a autonomia do bloco face a potências tecnológicas externas, afirmando o poder normativo da UE no cenário global (Metakides, 2021). Por outro, evidencia as tensões entre o nível europeu e o nacional, dado que as políticas digitais implicam cedências de autoridade, partilha de dados e coordenação política. Esta dialética entre soberania partilhada e autonomia nacional é, de facto, constitutiva da integração europeia e reflete o carácter híbrido da governação no domínio digital (Romanova, 2021). Tal como defende Ruohonen (2020), a soberania não é uma condição absoluta, mas uma relação dinâmica que depende da capacidade de um ator definir, proteger e exercer controlo sobre os seus recursos estratégicos, sejam eles materiais, informacionais ou normativos. A digitalização, ao multiplicar os pontos de vulnerabilidade e interdependência, exige novas formas de soberania adaptadas à complexidade das redes globais.

Assim, o enquadramento teórico desta dissertação parte da premissa de que a soberania digital não substitui o modelo vestefaliano, mas transforma-o. Ela traduz a transição de um paradigma centrado na autoridade territorial para outro baseado na capacidade funcional e normativa. Neste novo contexto, o poder estatal mede-se não apenas pela posse de território ou forças armadas, mas também pela capacidade de proteger infraestruturas críticas, regular fluxos de dados e desenvolver tecnologias estratégicas (Floridi, 2020; Broeders et al., 2023). A soberania digital, portanto, representa uma síntese entre política, tecnologia e direito, um campo onde se decide a autonomia estratégica das democracias modernas.

A reflexão teórica sobre esta transição serve de base para compreender os desafios específicos da UE e, mais adiante, o caso português. A UE, enquanto espaço de soberania partilhada, oferece um laboratório único para observar a evolução deste conceito e as suas implicações políticas. O equilíbrio entre integração supranacional e autonomia nacional no domínio digital é o eixo analítico que sustenta a presente investigação.

1.1. Conceito de Soberania Digital: Definição e Evolução

A emergência do conceito de soberania digital é indissociável da transformação estrutural do sistema internacional provocada pela digitalização e pela globalização. O termo não possui uma definição única nem consensual, a sua polissemia reflete a multiplicidade de atores e lógicas que o utilizam. Dependendo da perspetiva teórica, a soberania digital pode significar autonomia tecnológica, controlo sobre dados e infraestruturas, poder normativo no ciberespaço, ou ainda capacidade de autodefesa face à coerção digital. Como argumenta Floridi (2020), a digitalização reconfigura as fronteiras do poder político e epistemológico, obrigando os Estados e as instituições supranacionais a repensar o próprio significado de soberania.

No plano conceptual, a soberania digital situa-se na confluência entre tecnologia, direito e política internacional. Para Broeders, Cristiano e Kaminska (2023), ela constitui uma extensão funcional da soberania clássica, onde a autoridade estatal é redefinida pela capacidade de legislar e governar no domínio digital. Esta transposição do conceito vestefaliano para o ciberespaço reflete o reconhecimento de que a infraestrutura digital é hoje tão vital quanto o território físico.

A soberania digital, nesse sentido, traduz-se na capacidade de um ator, seja ele Estado, organização regional ou empresa, de controlar os elementos essenciais que compõem o seu ecossistema digital: infraestruturas, fluxos de dados, algoritmos, padrões técnicos e sistemas de segurança (Zinovieva & Bulva, 2021).

A ausência de uma definição universal deve-se, em parte, à diversidade de dimensões que o conceito abrange. Gálik (2022) identifica quatro vertentes fundamentais: a infraestrutura física, as plataformas e software críticos, os fluxos e a propriedade dos dados, e o enquadramento legal e operacional. Estas dimensões interagem de forma dinâmica, refletindo a natureza transversal da soberania digital. Ela não é apenas uma questão técnica ou regulatória, mas um conceito estratégico, que liga a política interna, a economia global e a segurança internacional.

A literatura identifica três fases principais na evolução do conceito de soberania digital no contexto europeu e global (Metakides, 2021; Carrapico & Farrand, 2024): A primeira fase, de natureza tecnocrática e regulatória (2010–2016), tem início com a adoção da Agenda Digital para a Europa (Comissão Europeia, 2010), integrada na estratégia “Europa 2020”.

Este documento representou a primeira tentativa institucional da UE de definir objetivos concretos para o desenvolvimento digital, centrando-se em áreas como a conectividade, a proteção de dados, a segurança das redes e a criação de um mercado digital único. A partir deste marco, o digital passou a ser enquadrado como um domínio estratégico, estabelecendo as bases para as subseqüentes políticas de soberania e autonomia tecnológica. Esta fase culmina com a aprovação do RGPD que simboliza a consolidação da soberania normativa europeia no ciberespaço ao impor regras extraterritoriais, o que projetou o poder regulatório da UE além das suas fronteiras, definindo padrões globais de tratamento de dados. Este fenómeno ficou conhecido como o efeito Bruxelas, onde a regulação europeia se torna referência internacional (Bradford, 2020).

A segunda fase, geopolítica e securitária (2016–2020), foi catalisada pelas revelações sobre vigilância massiva (Snowden³) e pelo aumento de ciberameaças estatais e criminosas. A percepção de vulnerabilidade digital levou à expansão do conceito de soberania digital para incluir segurança das comunicações, defesa cibernética e redução de dependências tecnológicas externas (Bellanova, Carrapico & Duez, 2022). A soberania passou a significar também resiliência — a capacidade de resistir à coerção tecnológica e à manipulação de dados estratégicos. Nesse período, a UE

³ O caso Snowden refere-se à divulgação, em 2013, de documentos classificados da Agência de Segurança Nacional dos Estados Unidos por Edward Snowden, um ex-contratante da agência. As revelações expuseram programas de vigilância em larga escala conduzidos pelos Estados Unidos e aliados, que monitorizavam comunicações digitais globais, incluindo de governos europeus, empresas e cidadãos. O impacto político foi profundo: desencadeou debates sobre privacidade, soberania digital e dependência tecnológica face a infraestruturas e serviços controlados por potências externas, levando a UE a reforçar políticas de proteção de dados e segurança cibernética.

desenvolveu a *Cyber Diplomacy Toolbox* e reforçou o papel da ENISA (Agência da UE para a Cibersegurança), institucionalizando a resposta coletiva a incidentes digitais.

A terceira fase, operacional e estratégica (2020–presente), caracteriza-se pela convergência entre política industrial e regulação. A soberania digital torna-se uma agenda integrada, combinando legislação, investimento e inovação. O DMA, o DSA e o *European Chips Act* (ECA)⁴ e a Diretiva NIS2 consolidam esta fase, reforçando o objetivo de autonomia tecnológica europeia. Como observa Rone (2024), esta transição representa “a transformação da soberania digital de um discurso político para uma política operacional e industrial”.

A soberania digital assume três dimensões interdependentes: A dimensão normativa, central à abordagem europeia, refere-se à capacidade de definir regras e padrões de conduta para o espaço digital. Ao estabelecer o RGPD, o DMA e o DSA, a UE projetou uma forma de poder normativo digital, transformando valores democráticos — como privacidade e transparência — em instrumentos de influência global (Broeders et al., 2023). Esta estratégia reflete o conceito de *normative power Europe*⁵, segundo o qual a União exerce poder através da regulação e da exportação de normas (Manners, 2002). A dimensão económica relaciona-se com o controlo sobre infraestruturas e cadeias de valor. A dependência europeia de fornecedores estrangeiros de semicondutores, plataformas e serviços de *cloud* tornou-se uma questão de soberania económica (Metakides, 2021). Iniciativas como o *GAIA-X* e o ECA procuram fortalecer a autonomia tecnológica e industrial do continente, reduzindo a exposição a riscos externos. Por fim, a dimensão geopolítica traduz-se na capacidade de um Estado ou bloco regional exercer poder no ciberespaço. A digitalização criou novas formas de competição estratégica, onde o controlo sobre dados e tecnologia equivale a poder político. Floridi (2020) argumenta que a luta pela soberania digital é, na essência, uma luta pela autonomia cognitiva — o direito de decidir como uma sociedade define, processa e protege a informação que produz.

⁴ *Regulamento (UE) 2023/1781* — define um quadro de medidas destinado a reforçar o ecossistema europeu de semicondutores, promovendo a autonomia tecnológica estratégica da União e reduzindo a dependência de cadeias globais vulneráveis.

⁵ Segundo Manners, a UE exerce poder normativo quando molda o comportamento de outros atores internacionais — Estados, organizações e empresas — através da difusão de valores, princípios e normas em vez de coerção ou incentivos materiais. Este poder deriva da própria natureza da UE como um projeto político pós-vestefaliano, fundado em valores como a democracia, o Estado de direito, os direitos humanos e a economia social de mercado. Ao transformar esses princípios em regras jurídicas e políticas públicas, a União exporta um modelo de governação que influencia a ordem internacional, mesmo para além das suas fronteiras formais. No contexto da soberania digital, este conceito adquire particular relevância: a UE utiliza o seu poder regulatório para definir valores democráticos e éticos aplicáveis ao espaço digital, transformando a regulação tecnológica num instrumento de política externa. Assim, em vez de competir tecnologicamente com potências como os EUA ou a China, a União procura afirmar a sua autonomia estratégica através da liderança normativa — exportando padrões de privacidade, segurança e transparência digital que refletem o seu quadro político e moral

A soberania digital não é um estado fixo, mas uma condição relacional. Depende da interação entre atores públicos e privados, das redes tecnológicas e dos regimes normativos. Como destaca Ruohonen (2020), a soberania no ciberespaço não se traduz em exclusividade, mas em “capacidade de coordenação e controlo relativo”.

Os Estados já não detêm monopólio sobre a força informacional, mas continuam a desempenhar um papel essencial na definição de normas e na proteção de infraestruturas críticas. Neste sentido, a soberania digital pode ser entendida como uma forma de soberania partilhada e adaptativa, que evolui à medida que as interdependências globais se intensificam. A UE exemplifica esta evolução: o seu modelo de governação digital combina centralização normativa e descentralização operacional, permitindo que os Estados-membros mantenham espaço de manobra político dentro de uma arquitetura regulatória comum (Bellanova et al., 2022; Carrapico & Farrand, 2024).

1.2. Supranacionalização e Intergovernamentalismo na União Europeia

O debate sobre soberania digital na UE não pode ser dissociado da tensão estrutural entre supranacionalização e intergovernamentalismo, dois paradigmas que moldam historicamente a integração europeia. Esta dualidade traduz-se na escolha dos instrumentos políticos e institucionais através dos quais a UE procura construir autonomia estratégica num domínio que transcende fronteiras, jurisdições e competências nacionais.

A supranacionalização implica a transferência de autoridade decisória para instituições europeias, como a Comissão Europeia, o Parlamento Europeu e o Tribunal de Justiça da União Europeia, que exercem poder regulatório direto sobre os Estados-membros. Já o intergovernamentalismo privilegia a cooperação entre governos nacionais, preservando a soberania e o controlo político a nível estatal. No domínio digital, estas duas lógicas coexistem e entram frequentemente em tensão, refletindo as ambiguidades inerentes à natureza híbrida da governação europeia (Rosamond, 2000).

O ciberespaço, pela sua natureza transnacional, evidencia esta ambivalência. Nenhum Estado-membro possui, isoladamente, a capacidade de garantir segurança, resiliência e competitividade digital num mercado global dominado por plataformas extracomunitárias. Como argumenta Broeders, Cristiano e Kaminska (2023), a digitalização reconfigura as interdependências entre os Estados, tornando inevitável a partilha de soberania. Ao mesmo tempo, o controlo sobre infraestruturas críticas e fluxos de dados continua a ser percebido como um atributo essencial da autonomia nacional. Assim, a soberania digital na UE é construída num equilíbrio delicado entre coordenação coletiva e preservação de prerrogativas nacionais.

A supranacionalização no domínio digital manifesta-se principalmente através da ação regulatória da Comissão Europeia, que tem assumido um papel central na criação de um quadro jurídico comum. O RGPD, o DMA, o DSA e a Diretiva NIS2 constituem pilares fundamentais dessa arquitetura. Estes instrumentos consagram o poder normativo europeu, traduzindo valores de transparência, responsabilidade e proteção de direitos fundamentais em normas vinculativas com efeito extraterritorial (Bradford, 2020).

Como observa Carrapico e Farrand (2024), a estratégia digital da UE reflete uma forma de mercantilismo regulatório, no sentido em que a regulação se torna uma ferramenta de poder económico e geopolítico. A União atua como um “*rule-maker*” global, impondo padrões que condicionam o funcionamento das grandes empresas tecnológicas internacionais. Este poder regulatório, conhecido como o *Brussels Effect*⁶, reforça a autonomia europeia no plano normativo, projetando a soberania digital como instrumento de afirmação internacional (Bradford, 2020).

Contudo, a supranacionalização encontra limites estruturais. O domínio digital abrange áreas sensíveis — como defesa, segurança e política industrial — que continuam fortemente ancoradas nas competências nacionais. A Comissão Europeia possui capacidade de iniciativa e coordenação, mas depende da implementação e da vontade política dos Estados-membros. Em setores críticos, como as redes 5G, a computação em nuvem e os semicondutores, as decisões

⁶ Cunhado pela jurista Anu Bradford, refere-se à capacidade da UE de exercer influência global através da exportação das suas normas e regulamentos internos, mesmo sem recorrer a coerção política, económica ou militar. Em vez de poder duro (*hard power*), trata-se de poder normativo e de mercado: a UE cria regras tão rigorosas e abrangentes — em domínios como a privacidade, o ambiente, a concorrência, a segurança alimentar ou a regulação digital — que as empresas multinacionais acabam por adotá-las globalmente, para não perderem acesso ao mercado europeu.

estratégicas ainda são tomadas num quadro predominantemente intergovernamental (Metakides, 2021).

O intergovernamentalismo permanece particularmente relevante na política de cibersegurança e defesa digital. A “*Cyber Diplomacy Toolbox*”, adotada em 2017, ilustra este modelo: trata-se de um conjunto de instrumentos de resposta coordenada a ciberataques, que dependem da deliberação e unanimidade dos Estados-membros (Bellanova, Carrapico & Duez, 2022). O seu funcionamento demonstra que, embora exista vontade de agir coletivamente, o processo decisório continua ancorado na lógica de consenso nacional.

De modo semelhante, a ENISA, reforçada pelo *Cybersecurity Act* de 2019, atua como estrutura de coordenação técnica, mas não possui poder executivo direto sobre os Estados. A implementação das medidas de segurança continua descentralizada, cabendo às autoridades nacionais a execução e monitorização. Em Portugal, por exemplo, o Centro Nacional de Cibersegurança (CNCS) é responsável pela articulação com as estruturas europeias e pela resposta a incidentes a nível nacional, integrando-se nas redes de cooperação da UE, mas mantendo autonomia operacional.

Este modelo reflete uma característica histórica da integração europeia: a coexistência entre centralização normativa e descentralização política. A UE cria o quadro comum e define os objetivos estratégicos, mas a execução depende de capacidades domésticas. Esta dualidade é particularmente visível na aplicação da Diretiva NIS2, que harmoniza requisitos de segurança nos setores críticos (energia, transportes, finanças e saúde), mas exige que cada Estado desenvolva mecanismos próprios de supervisão e resposta (European Commission, 2023).

Assim, a soberania digital europeia assume a forma de soberania partilhada: os Estados delegam competências na UE para ganhar escala e coerência, mas mantêm margem de manobra nacional. Como sintetiza Rone (2024), a integração digital europeia é um processo de “centralização estratégica com execução descentralizada”, no qual a autonomia operacional dos Estados é preservada dentro de uma moldura normativa comum.

A natureza interconectada do ciberespaço torna a interdependência inevitável. Nenhum Estado europeu dispõe sozinho dos recursos tecnológicos, industriais ou financeiros necessários para assegurar soberania plena no domínio digital. Essa limitação estrutural levou a UE a adotar uma abordagem cooperativa e pragmática, baseada em três pilares: resiliência conjunta, partilha de informação e investimento coordenado (Bendiek & Schulze, 2022).

Instrumentos como o *European Cybersecurity Industrial, Technology and Research Competence Centre* (ECCC) e os programas de investimento do *Horizon Europe* e do *Digital Europe Programme* procuram reforçar capacidades estratégicas coletivas. Estas iniciativas representam uma tentativa de construir autonomia tecnológica europeia sem regressão nacionalista, equilibrando integração e diversidade.

Ao mesmo tempo, a partilha de dados e inteligência sobre incidentes cibernéticos exige confiança mútua e alinhamento político. A transparência imposta por diretivas como a NIS2 pode revelar vulnerabilidades nacionais, o que explica a relutância de alguns Estados em adotar mecanismos de cooperação total (Carrapico & Farrand, 2024). Assim, a soberania digital europeia é tanto um projeto político de integração quanto um processo de negociação permanente entre segurança e autonomia.

A soberania é um dos conceitos mais persistentes e debatidos das ciências sociais, mas também um dos que mais sofreu transformação conceptual desde o início do século XXI. O modelo clássico, baseado na autoridade suprema do Estado sobre um território definido, tornou-se insuficiente para explicar os desafios introduzidos pela digitalização. Krasner (1999) mostrou que, mesmo nas relações internacionais tradicionais, a soberania nunca foi absoluta, funcionando antes como um conjunto de práticas e convenções moldadas por interesses políticos. Agnew (2005) reforça esta perspetiva ao demonstrar que a soberania não deve ser vista como algo fixo ou monolítico, mas como diferentes combinações de autoridade, territorialidade e legitimidade que variam ao longo do tempo e dos contextos.

A transição para o digital acentuou todas estas tensões. Infraestruturas críticas, como centros de dados, cabos submarinos ou plataformas de *cloud*, são frequentemente detidas por empresas privadas situadas fora da jurisdição estatal; algoritmos utilizados em serviços públicos dependem de fornecedores multinacionais; dados de cidadãos circulam por redes distribuídas globalmente. Como descreve DeNardis (2014), a governança da Internet é uma arena de disputa

entre atores públicos e privados, cada qual com diferentes capacidades técnicas e políticas, que se interligam numa arquitetura global de poder difícil de territorializar. Ruohonen (2021) vai mais longe ao mostrar que, quando se tenta aplicar diretamente os conceitos clássicos de soberania ao domínio digital, surgem paradoxos, precisamente porque as fronteiras políticas não coincidem com a infraestrutura técnica que sustenta o digital.

É neste contexto que ganha relevância o conceito, aqui desenvolvido como contributo sustentado em outras bases, mas desenvolvido nesta dissertação, de “soberania digital partilhada”. Em vez de uma noção rígida de soberania baseada no controlo exclusivo, este conceito descreve a soberania digital como uma capacidade distribuída, cooperativa e inevitavelmente interdependente. A soberania digital partilhada reconhece que nenhum Estado europeu controla isoladamente os recursos tecnológicos essenciais ao seu funcionamento político, económico e administrativo. Reconhece também que o poder digital se exerce através de redes globais, regulações supranacionais, infraestruturas privadas e relações tecnopolíticas que ultrapassam fronteiras. Assim, a soberania no digital adquire uma natureza relacional, mais próxima de uma prática articulada entre níveis de poder, do que de uma autoridade unívoca.

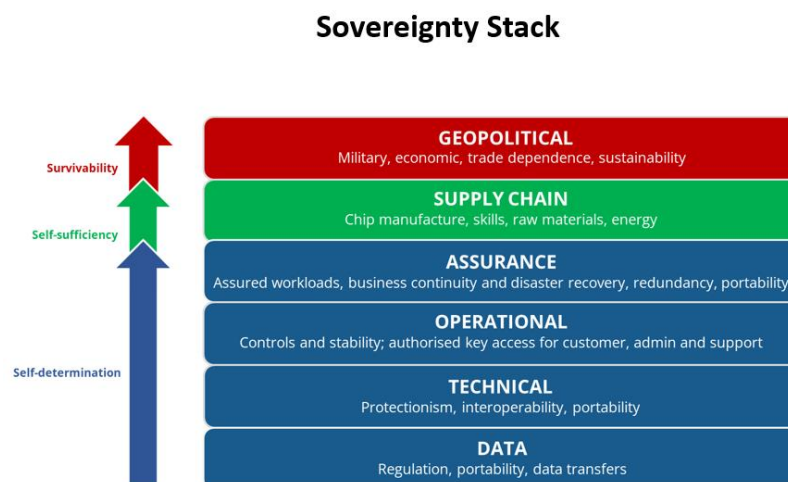
Esta transformação torna-se particularmente evidente no caso português. O Plano de Ação para a Transição Digital sublinha explicitamente que a digitalização do país depende do alinhamento com estratégias europeias e de uma coordenação institucional multissetorial (Governo de Portugal, 2020). Paralelamente, o relatório TE 100 – Soberania Digital demonstra que a autonomia tecnológica nacional é limitada pela dependência de infraestruturas, plataformas e fornecedores estrangeiros, que desempenham um papel central nos serviços digitais utilizados tanto pelo setor público como pelo privado (GEE, 2025).

Assim, o estudo do contexto europeu da soberania digital exige compreender como a UE procura construir capacidades coletivas, desenvolver autonomia regulatória e enfrentar pressões externas, ao mesmo tempo que reconhece a inevitabilidade da interdependência no domínio digital. É neste equilíbrio entre autonomia e dependência, entre poder nacional e coordenação supranacional, que se materializa a lógica conceptual da soberania digital partilhada que orienta esta dissertação.

A Estratégia Digital da UE constitui uma resposta estruturada à transformação profunda que o digital imprime à forma como o poder é exercido no século XXI. O digital não respeita fronteiras físicas, redistribui capacidades entre atores públicos e privados e cria novos espaços de autoridade que não podem ser regulados exclusivamente através de instrumentos estatais tradicionais. A soberania, historicamente associada ao controlo territorial, enfrenta agora um ambiente em que dados, algoritmos, infraestruturas de computação e plataformas globais operam numa escala transnacional que frequentemente não corresponde às jurisdições políticas estabelecidas. Vários autores têm demonstrado que esta tensão entre soberania formal e prática se torna particularmente evidente no contexto digital (Krasner, 1999).

A ausência de fronteiras no digital assume um papel central na discussão contemporânea sobre soberania. Bratton (2015) argumenta que o mundo digital se organiza numa arquitetura pós-territorial composta por múltiplas camadas — infraestruturais, lógicas, aplicacionais e sociais — que atravessam Estados, plataformas e utilizadores, constituindo um modelo de governação que já não depende de fronteiras geográficas, mas da posição relativa de cada ator dentro dessas camadas. Deste modo, o exercício do poder no digital torna-se uma função de acesso, controlo e influência sobre estas camadas tecnológicas, e não da mera posse territorial de infraestruturas.

Figura 1. Esquema conceptual inspirado no modelo em camadas de “The Stack”, de Benjamin Bratton (2015). Representa a distribuição de poder no ecossistema digital através de diferentes níveis: infraestruturas globais, regulação supranacional, Estado e utilizadores. A figura ilustra como a soberania digital se exerce de forma distribuída e interdependente.



Fonte: <https://www.idc.com/resource-center/blog/the-evolution-of-digital-sovereignty-moving-beyond-data-and-cloud/>

Esta leitura é reforçada pela vasta literatura sobre governação digital. Autores como Zuboff (2019), DeNardis (2014) e Ruohonen (2021) demonstram que o ecossistema tecnológico contemporâneo é marcado por assimetrias de poder estruturais, decorrentes da centralidade das plataformas digitais, da natureza extraterritorial dos protocolos e da importância política das infraestruturas técnicas. As plataformas, em particular, adquirem uma capacidade regulatória que ultrapassa o domínio económico e se estende ao domínio político.

Zuboff observa que *“surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data”* (2019, p. 14) e que estas empresas procuram *“anticipate what you will do now, soon, and later”* (2019, p. 14), revelando a profundidade do controlo comportamental que exercem. O poder destas entidades reside não apenas na gestão de dados, mas na modelação de preferências, comportamentos e relações sociais.

DeNardis (2014) acrescenta que *“much of Internet governance is enacted by private corporations and nongovernmental entities (...) private industry (...) influences traditional governmental actions”* (p. 21), evidenciando que as plataformas não operam apenas como fornecedores de serviços, mas como atores políticos estruturantes, capazes de moldar normas, práticas e até decisões estatais.

Ruohonen (2021) aprofunda esta análise ao argumentar que a soberania digital enfrenta paradoxos conceptuais, dado que as infraestruturas da Internet não se alinham com fronteiras políticas, permitindo que empresas privadas detenham capacidades historicamente associadas a entidades soberanas. Como sublinha, é possível identificar formas de “soberania privada” quando empresas exercem poder coercivo ou estrutural num ambiente transnacional: *“There is also another lesson closely related to Westphalia. When fast-forwarding in time, it is possible to find another kind of sovereign via conceptual stretching. That is, a private company raging private or quasi-private wars to advance commercial goals; and, again, military innovation and the capacity to exert power, but not balance, were present just as sovereignty was (...)”* (Ruohonen, 2021).

Neste contexto, torna-se evidente que a soberania digital estatal não pode ser entendida como controlo absoluto, mas como capacidade de intervir, influenciar e adaptar-se a um ecossistema de autoridade distribuída. A circulação global de dados, a dependência tecnológica externa e o domínio de empresas transnacionais tornam insuficiente o modelo de soberania centrado na autoridade exclusiva sobre o território.

É neste enquadramento que se torna particularmente pertinente o conceito — desenvolvido nesta dissertação — de soberania digital partilhada. Este conceito descreve a forma como os Estados preservam a sua autoridade através de cooperação e articulação com entidades supranacionais e infraestruturas tecnológicas que não controlam diretamente. A soberania, neste domínio, funciona como um conjunto relacional de capacidades que se exerce através de redes, mecanismos regulatórios e parcerias institucionais.

Instituições internacionais reforçam esta leitura. A OCDE (2021) destaca a necessidade de coordenação multinível para garantir resiliência e autonomia em sistemas digitais globais; o Conselho da Europa (2020) assinala que a proteção de direitos fundamentais no digital exige mecanismos cooperativos de governação.

Zürn (2018) demonstra que parte da autoridade previamente concentrada nos Estados se encontra hoje distribuída por instituições internacionais: *“International institutions, in this view, have the potential, and are expected, to exercise authority to the extent that it is A Theory of Global Governance necessary to foster global common good and to protect some individual rights.”* (Zürn, 2018, p. 35-36). Esta deslocação de autoridade não implica um esvaziamento da soberania estatal, mas antes a emergência de uma arquitetura multinível de governação, na qual diferentes instituições. Num ambiente digital altamente interdependente, esta transferência funcional de autoridade torna-se ainda mais visível. A regulação de plataformas globais, a proteção de dados, a definição de normas técnicas e a segurança das infraestruturas críticas exigem competências especializadas e estruturas de coordenação que refletem precisamente o tipo de autoridade distribuída que Zürn descreve.

Moravcsik (1998) fornece uma base teórica particularmente robusta para compreender a lógica da soberania digital partilhada. Para o autor, os Estados delegam competências a organismos supranacionais para reforçar a sua capacidade coletiva de influenciar desfechos políticos, económicos e tecnológicos. Como refere, ao analisar a delegação institucional, é necessário considerar teorias que incluem a ideologia federalista, a eficiência da centralização tecnocrática e a necessidade de aumentar a credibilidade de compromissos nacionais: *“To explain decisions to delegate powers to international institutions, I evaluate theories that stress federalist ideology, the greater efficiency of centralizing the generation of technocratic information, and the need to increase the credibility of national commitments.”* (p. 19).

Deste modo, a soberania digital partilhada emerge como uma forma contemporânea de delegação estratégica, através da qual os Estados procuram recuperar capacidade de influência num ecossistema dominado por atores não estatais e tecnologias globais.

A relevância do digital para a transformação da soberania é igualmente evidenciada por Manuel Castells, cuja análise estrutural das sociedades em rede revela a profundidade da reconfiguração do poder na era da informação. Castells demonstra que “*Power is exercised by means of coercion (or the possibility of it) and/or by the construction of meaning on the basis of the discourses through which social actors guide their action.*” (2009, p. 6), sugerindo que o poder político e institucional depende cada vez mais da capacidade de produzir, controlar e interpretar fluxos de informação num ambiente globalizado. Ao afirmar que “*Networks constitute the fundamental pattern of life, of all kinds of life. As Fritjof Capra writes, “the network is a pattern that is common to all life. Wherever we see life, we see networks”.*” (Castells, 2009, p. 21), o autor identifica uma mudança estrutural que desloca o exercício da autoridade para sistemas em rede que atravessam fronteiras estatais e reorganizam relações de poder entre atores públicos e privados.

Esta conceptualização reforça a tese de que a soberania digital não pode ser entendida através de categorias territoriais tradicionais, mas exige um enquadramento que reconheça a centralidade das redes informacionais e das infraestruturas tecnológicas na distribuição de poder contemporânea.

A UE é o laboratório político mais visível desta transformação. A UE não substitui os Estados-Membros, mas multiplica a sua capacidade de intervenção ao reunir escala regulatória, recursos e autoridade política capazes de enfrentar desafios impossíveis de resolver isoladamente. A Estratégia Digital europeia traduz esta visão ao reforçar mecanismos comuns de cibersegurança, governança de dados, regulação de plataformas e desenvolvimento de infraestruturas estratégicas.

Portugal integra-se plenamente nesta dinâmica. O *Plano de Ação para a Transição Digital* reconhece que a autonomia tecnológica nacional depende do alinhamento com as estratégias europeias, enquanto o relatório *TE 100 – Soberania Digital* evidencia dependências estruturais face a plataformas, fornecedores e infraestruturas externas. Para Portugal, como para outros Estados pequenos e médios, a soberania digital torna-se efetiva na medida em que é exercida através de uma governação europeia articulada, capaz de aumentar capacidade regulatória, escalar recursos e defender interesses nacionais num ecossistema tecnológico global.

Assim, a Estratégia Digital da UE demonstra que a soberania no digital não se constrói por isolamento, mas por cooperação estruturada. A soberania digital partilhada emerge como o modelo mais adequado para compreender o exercício de poder no século XXI: uma soberania relacional, interdependente e tecno-politicamente distribuída, ajustada às exigências de um ambiente global que nenhum ator controla sozinho.

2. Contexto Europeu: O Regulamento Geral de Proteção de Dados (RGPD) e as Implicações para os Estados-Membros

O Regulamento Geral de Proteção de Dados (RGPD) consolidou-se como um dos pilares centrais da governação digital europeia, representando a capacidade da UE para projetar normas regulatórias que protegem direitos fundamentais num ecossistema tecnológico globalizado. A sua entrada em vigor, em 2018, redefiniu profundamente a relação entre indivíduos, Estados e empresas na gestão de dados pessoais, ao instituir um regime jurídico harmonizado que estabelece princípios, direitos e obrigações aplicáveis de forma uniforme nos Estados-Membros.

Estudos recentes apontam o RGPD como uma manifestação clara de soberania normativa europeia, pela forma como condiciona juridicamente atores extraterritoriais, impondo requisitos substanciais de conformidade que refletem uma visão europeia dos direitos digitais (Carrapico & Farrand, 2025). Uma das características mais distintivas do RGPD é o seu alcance extraterritorial, consagrado no Artigo 3.º, que obriga qualquer entidade que trate dados de indivíduos situados na UE a cumprir as normas europeias, independentemente do local onde essa entidade esteja estabelecida. Esta disposição amplifica a capacidade regulatória da UE e reduz assimetrias face a corporações tecnológicas globais, reforçando o controlo europeu sobre fluxos internacionais de dados.

O RGPD funciona também como instrumento de soberania informacional individual ao reposicionar os cidadãos europeus como agentes dotados de um conjunto alargado de direitos, acesso, portabilidade, limitação do tratamento, oposição e apagamento, que lhes permitem controlar de forma mais efetiva o ciclo de vida dos seus dados.

Figura 2. Diagrama conceptual que sintetiza o RGPD como eixo da soberania digital europeia, destacando os seus seis pilares centrais: direitos dos titulares, obrigações das organizações, fluxos internacionais de dados, supervisão e sanções, impacto económico e dimensão geopolítica.



Fonte: Grácio, Bruno (2026)

Para os Estados-Membros, a implementação do RGPD implica exigências substanciais em termos de capacidades administrativas, reforço das autoridades nacionais de proteção de dados e adaptação das legislações internas. O cumprimento das obrigações administrativas, a necessidade de garantir auditorias contínuas e a operacionalização de mecanismos técnicos de conformidade exigem investimentos elevados, tanto em recursos humanos especializados como em infraestruturas tecnológicas. Estudos no contexto português, como o de Osório (2023), mostram que a transposição do RGPD envolveu não apenas alterações legislativas, mas também um esforço significativo de capacitação institucional, demonstrando que a implementação do regulamento constitui um processo complexo que ultrapassa a mera adoção formal de normas jurídicas.

As implicações do RGPD para a soberania digital tornam-se ainda mais evidentes quando se analisam as transferências internacionais de dados. A exigência de que apenas países que asseguram níveis adequados de proteção possam receber dados pessoais europeus reforça a posição da UE enquanto poder regulatório global.

A governação digital na UE assenta numa arquitetura institucional de carácter multinível, que reflete o próprio modelo político e regulatório da integração europeia. A formulação, adoção e execução das políticas digitais envolvem diferentes instituições e mecanismos de coordenação entre o nível europeu e os Estados-Membros, configurando um sistema de decisão partilhado e

interdependente. No plano político, a Comissão Europeia constitui o principal motor da ação digital europeia. Compete-lhe propor legislação, supervisionar a execução das políticas e monitorizar o cumprimento das normas europeias. A Comissão atua também como autoridade regulatória e de *enforcement* em matérias de concorrência, privacidade e mercados digitais. No domínio digital, destacam-se a DG CONNECT e a DG COMP, responsáveis pela preparação e implementação de instrumentos como o DSA, o DMA, o AI Act e a NIS2, entre outros.

O Conselho Europeu representa os governos nacionais e participa na definição das políticas digitais através da codecisão legislativa com o Parlamento Europeu. As formações de Telecomunicações, Competitividade e Mercado Interno são as principais responsáveis pela aprovação das propostas relacionadas com o digital. Este nível assegura a dimensão intergovernamental do processo e garante que as posições nacionais são refletidas nas decisões finais. O Parlamento Europeu desempenha um papel crescente e determinante na regulação digital, representando a dimensão democrática do processo decisório. É colegislador em praticamente todas as matérias relevantes e intervém diretamente na definição de instrumentos como o RGPD, o AI Act e o ECA. As comissões IMCO e LIBE têm particular relevância neste domínio, abordando questões ligadas à proteção de dados, moderação de conteúdos e direitos digitais.

A execução das políticas digitais é partilhada entre a Comissão Europeia e os Estados-Membros. A nível técnico, diversas agências da UE têm um papel operacional essencial. A ENISA coordena a aplicação da NIS2 e apoia os Estados-Membros na construção de resiliência cibernética, enquanto o *European Data Protection Supervisor* supervisiona a conformidade com as normas de privacidade no seio das instituições europeias. Estas estruturas asseguram a ligação entre a regulação supranacional e a execução nacional.

O Conselho Europeu, embora sem funções legislativas diretas, define as grandes orientações estratégicas da política digital europeia, incluindo as ligadas à autonomia tecnológica e à soberania digital. Foi neste âmbito que se enquadraram iniciativas estruturantes como a Bússola Digital 2030 e o Plano para a Década Digital, que estabelecem os objetivos e metas da transição digital da UE.

Em síntese, a estrutura de decisão da UE no domínio digital combina dimensões supranacionais e intergovernamentais, articulando funções legislativas, executivas e de supervisão entre diferentes instituições. Este modelo de governação híbrida garante coerência e coordenação

entre níveis, mas também introduz complexidade e assimetrias na implementação das políticas. A soberania digital europeia resulta, assim, de uma constelação de atores e processos interligados que, em conjunto, moldam o espaço regulatório europeu e influenciam a forma como os Estados-Membros, como Portugal, exercem a sua própria soberania digital.

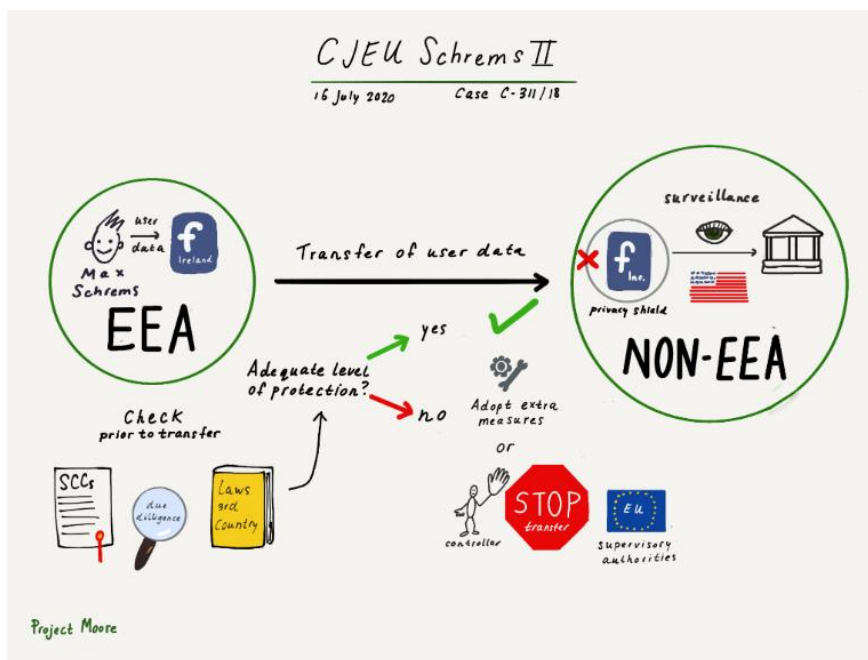
2.1 - Schrems II

Decisões judiciais como *Schrems II* acentuaram esta tendência ao invalidarem mecanismos de transferência internacional de dados que não ofereciam proteção adequada contra formas de vigilância estatal estrangeira. No acórdão de 2020, o Tribunal de Justiça da União Europeia (TJUE) concluiu que o regime jurídico norte-americano — designadamente as práticas de recolha de informação por parte das autoridades de inteligência ao abrigo do *Foreign Intelligence Surveillance Act*⁷ — não assegurava garantias equivalentes às previstas pelo RGPD, particularmente no que respeita aos princípios de proporcionalidade, controlo independente e possibilidade de recurso efetivo por parte dos titulares dos dados.

Esta decisão obrigou empresas tecnológicas e governos a reconfigurar profundamente as suas práticas de *compliance* e estratégias de transferência internacional de dados, tornando evidente que a proteção dos cidadãos europeus não depende apenas de normas internas, mas também da capacidade da UE de condicionar juridicamente atores extraterritoriais.

⁷ Estabelece o quadro legal que permite às agências de inteligência norte-americanas recolher informação sobre cidadãos estrangeiros para fins de segurança nacional. Alterações posteriores, nomeadamente a Secção 702, autorizam a vigilância eletrónica sem mandato individualizado, incluindo o acesso a comunicações armazenadas ou processadas por empresas tecnológicas sediadas nos EUA. Este regime de vigilância foi central na decisão *Schrems II*, dado que o Tribunal de Justiça da UE considerou que o FISA não oferece garantias equivalentes às asseguradas pelo RGPD, especialmente no que respeita a proporcionalidade, controlo independente e vias eficazes de recurso para cidadãos europeus.

Figura 3. O diagrama ilustra que o tribunal considerou o Privacy Shield inadequado devido à possibilidade de vigilância governamental norte-americana, obrigando entidades europeias a verificar se o país de destino oferece um nível de proteção equivalente ao da UE. Quando isso não acontece, devem ser adotadas medidas adicionais ou a transferência deve ser suspensa, recorrendo a instrumentos como as SCCs (Standard Contractual Clauses) e avaliações de risco sobre a legislação do país terceiro. A figura evidencia o impacto direto da decisão na governação das transferências internacionais de dados.



Fonte: <https://projectmoore.com/schrems-ii-implications-for-your-organisation/>

O impacto de *Schrems II* convergiu, assim, com análises académicas e institucionais — incluindo estudos sobre encriptação, vigilância e proteção de direitos fundamentais publicados por instituições como o Parlamento Europeu — que sublinham a necessidade de garantir que qualquer fluxo transnacional de dados esteja protegido contra intrusões incompatíveis com os standards europeus de privacidade e soberania digital. Neste sentido, o RGPD constitui não apenas um regulamento interno, mas um instrumento de governação global que afirma a autonomia normativa da UE e reforça a capacidade dos Estados-Membros para proteger os direitos dos seus cidadãos num ambiente transnacional.

2.2 - CSA - Regulation to Prevent and Combat Child Sexual Abuse

Apesar do seu papel estruturante, o RGPD não opera num vazio político. Propostas orientadas para a segurança, como o CSA - *Regulation to Prevent and Combat Child Sexual Abuse*

— amplamente e informalmente conhecido como “*Chat Control*”⁸— revelam tensões internas na UE entre a proteção de dados e as exigências securitárias. Esta proposta pretende introduzir mecanismos de deteção automática de conteúdos ilícitos, potencialmente recorrendo a tecnologias de *scanning client-side* que poderiam comprometer a encriptação ponto-a-ponto que podem permitir a análise automática de mensagens e ficheiros, algo que é tecnicamente problemático ou mesmo impossível sem comprometer a própria segurança dos sistemas de comunicação. A análise do grupo *Fight Chat Control* sublinha que a implementação de esquemas de digitalização em tempo real e do *scan* de mensagens privadas ameaça a integridade da encriptação e cria vulnerabilidades que afetariam todos os utilizadores, não apenas no contexto de deteção de abuso, mas também em termos de segurança contra *hackers*, espionagem ou intrusões governamentais indevidas.

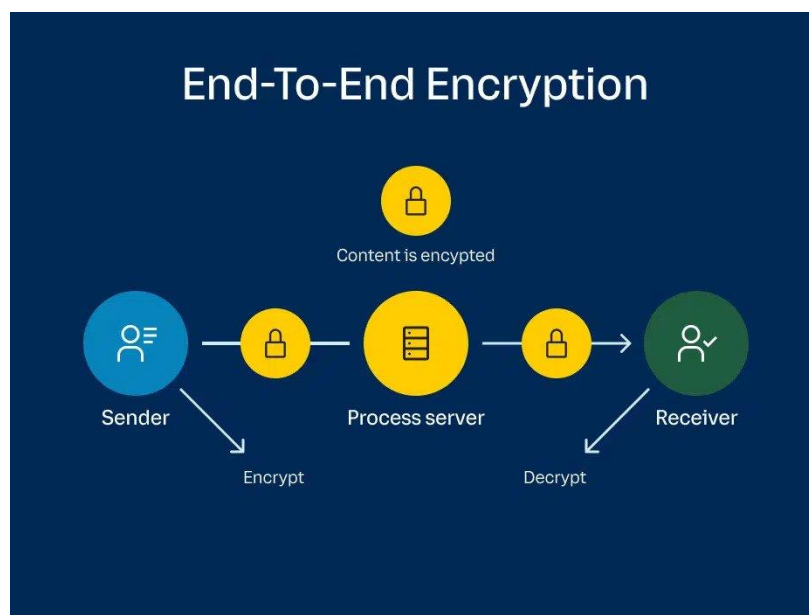
Esta posição é reforçada por estudos académicos que demonstram que a encriptação constitui uma infraestrutura essencial para a proteção de direitos digitais fundamentais. Chousou, Magaud, Pavoni e Willams (2023), num relatório académico produzido para a *Sciences Po*, analisam o enquadramento jurídico e técnico da encriptação na UE e concluem que a comunicação cifrada é indispensável para assegurar a confidencialidade das comunicações, a liberdade de expressão e a proteção contra vigilância arbitrária. O estudo demonstra que a encriptação forte funciona como um mecanismo de redistribuição de poder, equilibrando a assimetria entre cidadãos e entidades públicas ou privadas que processam grandes volumes de informação. As autoras argumentam que qualquer tentativa de enfraquecimento da encriptação — seja por *backdoors*, mecanismos de *scanning client-side*⁹ ou obrigações de vigilância integrada — introduz vulnerabilidades sistémicas que comprometem a segurança global das infraestruturas digitais e, por consequência, a própria soberania digital dos Estados, na medida em que estes perdem a

⁸ Designação informal da proposta legislativa da Comissão Europeia para a Regulação relativa à prevenção e combate ao abuso sexual de crianças, apresentada em 2022, que pretende obrigar prestadores de serviços digitais a detetar, analisar e reportar automaticamente conteúdos ilícitos nas comunicações dos utilizadores, incluindo mensagens protegidas por encriptação ponta-a-ponto. A iniciativa surgiu na sequência da pressão crescente para reforçar mecanismos de proteção de menores online, mas tornou-se altamente controversa por implicar formas de vigilância preventiva e generalizada das comunicações privadas, segundo críticas de especialistas em cibersegurança, juristas, organizações de direitos digitais e estudos do Parlamento Europeu.

⁹ Mecanismo que analisa conteúdos privados diretamente no dispositivo do utilizador antes da encriptação, permitindo a deteção automática de material considerado ilícito. Embora concebido como ferramenta de segurança, é amplamente criticado por comprometer a encriptação ponta-a-ponto, introduzir riscos de vigilância massiva e criar vulnerabilidades técnicas em dispositivos pessoais.

capacidade de garantir comunicações seguras aos seus cidadãos e entidades críticas (Chousou et al., 2023).

Figura 4. Representação simplificada do processo de encriptação ponta-a-ponta (E2EE). O conteúdo enviado pelo utilizador (sender) é encriptado antes de sair do dispositivo e apenas pode ser desencriptado pelo destinatário (receiver), mantendo-se ilegível para o servidor intermediário (process server). O servidor apenas gere o transporte da mensagem, sem capacidade de aceder ao seu conteúdo. Este modelo garante confidencialidade, integridade e proteção contra vigilância não autorizada, constituindo um elemento essencial para a soberania digital individual e para a segurança das comunicações num contexto de riscos crescentes de vigilância estatal e privada.



Fonte: <https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption>

Patrick Breyer (2023), jurista e eurodeputado especializado em privacidade e proteção de dados, reforça esta leitura ao analisar o impacto potencial da proposta do *Chat Control*. Nos seus pareceres e documentos de análise, Breyer demonstra que a vigilância automatizada de mensagens cifradas não só fragiliza a integridade técnica da encriptação ponta-a-ponta, como altera o equilíbrio de direitos no espaço digital europeu ao introduzir mecanismos de deteção massiva sem suspeita individualizada. Para Breyer, tal modelo representa uma mudança estrutural na relação entre o Estado e o cidadão, uma vez que transforma tecnologias concebidas para proteger a privacidade em instrumentos de vigilância preventiva, incompatíveis com os requisitos de necessidade e proporcionalidade estabelecidos pelo direito europeu.

O estudo independente do Parlamento Europeu (2023) converge com estas preocupações ao avaliar a viabilidade técnica do *Chat Control* e concluir que não existem métodos fiáveis para detetar automaticamente conteúdo ilegal em mensagens cifradas sem comprometer garantias fundamentais de segurança digital: *“This study concludes that the overall effectiveness of the CSA proposal is expected to be limited. This is due to a variety of factors that, when taken together, make it difficult to conclude that the CSA proposal will be effective.”* (Op ’t Hoog et al., 2023, p.3).

O relatório destaca que o enfraquecimento da encriptação teria efeitos sistémicos sobre a proteção de dados, a segurança nacional e a confiança pública nas instituições digitais, criando riscos não intencionais que ultrapassam largamente os benefícios esperados: *“(...) despite the potential for their abuse, technologies to detect known sexual abuse material are accurate, whereas technologies to detect new child sexual abuse material and grooming are of substantially lower accuracy and that detection of material in end-to-end-encrypted communication poses risks and vulnerabilities for individuals and society (...)”* (Op ’t Hoog et al., 2023, P.3). Além disso, salienta que tais mecanismos podem violar normas estruturantes da ordem jurídica europeia, nomeadamente os princípios de proporcionalidade, minimização de dados e limitação de finalidades previstos no RGPD.

Em conjunto, estes autores e instituições demonstram que o enfraquecimento da encriptação para permitir mecanismos de vigilância automatizada tem implicações profundas para a soberania digital individual e coletiva. Ao deslocar o eixo de poder do cidadão para o Estado ou para empresas tecnológicas que seriam encarregadas de monitorizar comunicações privadas, tais medidas alteram a própria arquitetura da governação digital europeia e colocam em causa a capacidade da União de sustentar um modelo de soberania baseado na proteção de direitos fundamentais e na integridade tecnológica das suas infraestruturas.

Assim, o RGPD deve ser entendido não apenas como um instrumento jurídico isolado, mas como um elemento central da soberania digital partilhada da UE, articulando direitos individuais, coordenação institucional e influência normativa global (Aueamnuay et al., 2024). Este enquadramento reflete a ambição europeia de afirmar autonomia tecnológica e proteger os direitos digitais dos cidadãos, especialmente no contexto de uma competição global marcada pelos modelos norte-americano e chinês (Calzada, 2019).

Como observa Herian, a própria retórica do RGPD insere-se numa “fantasia de soberania sobre os dados”, onde o controlo e a transparência são simultaneamente ideais regulatórios e desafios práticos (Herian, 2020). No entanto, a experiência prática demonstra que a sua implementação tem revelado tensões significativas entre Estados-Membros. Autoridades de proteção de dados nacionais têm expressado preocupações sobre a falta de recursos, a complexidade administrativa e a dificuldade de aplicar de forma uniforme disposições que exigem elevada especialização técnica, o que gera desigualdades na execução e reduz a eficácia do modelo europeu (Gentile & Lynskey, 2022). A literatura recente mostra que o *enforcement* transnacional do RGPD é estruturalmente deficiente, refletindo assimetrias de poder entre as autoridades de controlo e lacunas processuais. Casos concretos, como as divergências entre a CNIL (França) e a BfDI (Alemanha), ilustram a fragmentação regulatória e a dificuldade de garantir uma aplicação coerente em toda a União (Joswig & Kurz, 2025)

Em paralelo, organismos internacionais como a OCDE e o Comité das Regiões alertam que o RGPD pode impor custos desproporcionais às PME, especialmente em Estados-Membros com menor maturidade digital, potenciando assimetrias estruturais e limitando a competitividade dos mercados nacionais (OCDE, 2021). Estudos empíricos confirmam que as PME enfrentam obstáculos significativos para cumprir as obrigações do regulamento, devido à escassez de recursos técnicos e humanos (Sirur et al., 2018). Essa carga regulatória é agravada pela necessidade de cumprir simultaneamente o RGPD e o AI Act¹⁰, criando um duplo desafio que ameaça a inovação e a competitividade (Joswig & Kurz, 2025)

Além disso, evidências económicas sugerem que o RGPD, embora aumente a proteção da privacidade, tem efeitos negativos sobre o desempenho e a inovação empresarial, especialmente em contextos menos digitalizados. Vários governos têm também sublinhado que o regulamento, apesar de reforçar direitos fundamentais, cria um quadro jurídico por vezes rígido, difícil de conciliar com as dinâmicas aceleradas da inovação, da inteligência artificial e do desenvolvimento de dados industriais europeus.

¹⁰ Proposta legislativa da UE que visa estabelecer o primeiro quadro jurídico abrangente para o desenvolvimento, a comercialização e o uso de sistemas de inteligência artificial no espaço europeu. O objetivo principal é garantir que as tecnologias de IA sejam seguras, transparentes, rastreáveis, não discriminatórias e supervisionadas por humanos, em conformidade com os valores e direitos fundamentais da União.

Neste contexto, a soberania digital europeia revela-se um equilíbrio instável entre ambição normativa e desafios operacionais. Embora o RGPD constitua o esforço mais robusto para preservar a autonomia individual, reforçar direitos e projetar a UE como potência regulatória global, subsistem receios quanto à sua capacidade de acompanhar a evolução tecnológica e às consequências práticas que pode gerar para Estados-Membros com diferentes níveis de capacidades institucionais e económicas.

2.3. Diretiva NIS e a Segurança das Redes e Sistemas de Informação

A Diretiva (UE) 2016/1148, conhecida como Diretiva NIS (*Network and Information Security Directive*), foi o primeiro instrumento jurídico europeu a estabelecer uma base comum para a proteção das redes e sistemas de informação em toda a UE. A sua adoção representou um passo decisivo na construção de um quadro normativo europeu para a cibersegurança, reconhecendo que a interdependência tecnológica e as ameaças digitais afetam diretamente o funcionamento do mercado interno e a segurança dos Estados-Membros. Como afirmam Markopoulou, Papakonstantinou e Hert, “(...) *the NIS Directive constitutes the first EU-wide cybersecurity framework, aiming to achieve a high common level of network and information systems security.*” (2019, p. 2, ll. 10–14).

A Diretiva NIS introduziu obrigações específicas para os operadores de serviços essenciais (OES) e para os fornecedores de serviços digitais (DSP), impondo medidas de gestão de risco e mecanismos de notificação de incidentes. Aleksandrowicz observa que “*Member States are required to adopt national strategies for the security of networks, and information and communication systems, to designate national authorities for the security of networks and information systems covering at least the sectors listed above, and to operate an Internet trading platform, Internet search engines and cloud computing services.*” (2020, p. 182).

Além disso, a diretiva estabeleceu o Grupo de Cooperação e a Rede de CSIRTs para promover a troca de informações e a coordenação estratégica entre Estados-Membros — elementos que se tornaram pilares do modelo europeu de governação digital. Szádeczky sublinha que “*The formation of an EU Cybersecurity Act and filling NIS with more practical guidance is*

an ongoing process nowadays.” (2020, p. 83, ll. 12-14), e acrescenta que “*ENISA¹¹ was established in 2004 as a consultative body. Both the EU and the Hungarian Cybersecurity Strategy was accepted in 2013. The strategies implied changes in the treatment of the field of cybersecurity at the higher level. The objectives and tasks of ENISA have been changed, and the Hungarian authority was formed that year. The next step was the NIS directive and its implementation in the member states’ law, which also provides reinforcement to EU legislation to improve ENISA.*” (p. 91, ll. 1-6), consolidando-se como a autoridade técnica de referência da União.

A NIS 2¹² amplia o âmbito de aplicação, abrangendo novos setores críticos e introduzindo uma abordagem baseada na dimensão e criticidade das entidades. Lucini explica que a NIS 2 “*(...) replaces the complex identification process in the hand of the Member States as established in Article 5 of the NIS 1 with a self-identification system based on sectors and dimension of the entity.*” (2023, p. 147). Além disso, “*The NIS 2 revises also most of cybersecurity requirements of the previous discipline by providing a list of new obligations as well as revised procedural terms and liabilities.*” (2023, p. 145), reforçando a responsabilização das empresas e dos seus gestores.

A nova diretiva reflete também uma resposta política e estratégica às ameaças transfronteiriças. Szpor assinala que “*(...) the rapid increase in threats, referred to as the ‘cyberpandemic,’ requires prompt adaptation of legal instruments to new needs (...)*” (2021, p. 219). Essa aceleração regulatória visa assegurar coerência e resiliência em todo o bloco europeu, embora, como nota Szádeczky, “*(...) the practical implementation today is far away from the strategic objectives.*” (2020, p. 83). A Diretiva NIS 2 insere-se, assim, num ecossistema regulatório mais amplo, que integra medidas complementares destinadas a consolidar a soberania digital europeia.

Entre estas destacam-se o DMA e o DSA, que estabelecem regras de transparência e concorrência justa nas plataformas digitais, o ECA, que visa garantir a autonomia estratégica europeia na produção de semicondutores, e o projeto *GALA-X*¹³, uma infraestrutura federada de dados que promove interoperabilidade e segurança em conformidade com as normas da UE.

¹¹ *European Union Agency for Cybersecurity* — é a Agência da UE para a Cibersegurança, criada em 2004 pelo Regulamento (CE) n.º 460/2004.

¹² A NIS2 (Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022) é o novo quadro jurídico da UE para a cibersegurança, que substitui e atualiza a anterior *Diretiva NIS (2016/1148/UE)*.

¹³ Iniciativa europeia de infraestrutura federada de dados, lançada em 2020, que visa criar um ecossistema digital aberto e interoperável, garantindo soberania, transparência e segurança na partilha de dados na Europa.

Em última instância, o conjunto normativo constituído pela Diretiva NIS 2, pelo *GAIAX*, pelo ECA e pelo pacote regulatório digital europeu projeta a autonomia estratégica e digital da UE no cenário internacional. Como defende Calzada, “(...) *technological sovereignty aims at breaking down the dependence on proprietary programs and encouraging public leadership through data sovereignty—safeguarding the privacy of citizens—and transparency—or constant scrutiny and auditing in the public eye.*” (2019, p. 9).

Estes instrumentos traduzem, portanto, uma estratégia de autonomia sem isolamento, em que a União procura equilibrar inovação, segurança e direitos fundamentais face à preponderância tecnológica dos EUA e da China. Assim, a NIS 2 surge não apenas como um instrumento jurídico de cibersegurança, mas como pilar estruturante de uma política europeia de poder normativo digital, destinada a assegurar que a Europa não seja mera utilizadora de tecnologias alheias, mas produtora de regras, padrões e confiança no domínio digital global.

A política digital portuguesa inscreve-se num espaço de interdependência complexa entre segurança, economia e soberania. Na era pós-globalização, o digital tornou-se uma extensão da política externa e de defesa, e Portugal, enquanto pequeno Estado europeu com fortes vínculos transatlânticos, encontra-se no cruzamento de três eixos de poder: a NATO e os Estados Unidos, como garantes de segurança e interoperabilidade; a UE, como promotora de soberania tecnológica e regulação; e a China, como ator económico e tecnológico global em busca de influência estratégica. Esta tríade molda as escolhas portuguesas em matéria de cibersegurança, infraestrutura digital e inovação, num contexto de dependências estruturais que desafiam a ideia de autonomia digital nacional.

NATO

A NATO, enquanto aliança militar fundada em 1949, tem vindo a reconfigurar-se como ator central na ciberdefesa. Desde a Cimeira de Gales (2014), o ciberespaço foi reconhecido como um domínio operacional, equiparado aos tradicionais domínios terrestre, aéreo e marítimo. Essa decisão, posteriormente reafirmada em Bruxelas (2021), inscreve a ciberdefesa no núcleo da segurança coletiva euro-atlântica (Ilves et al., 2016).

A Aliança promove uma arquitetura comum de resposta a ataques digitais, através do *Cooperative Cyber Defence Centre of Excellence*, sediado em Tallinn, que desenvolve normas,

exercícios e doutrina de defesa cibernética partilhada. O envolvimento português, manifestado na adesão a exercícios como o *Locked Shields*¹⁴, traduz-se num alinhamento estreito com as doutrinas de segurança norte-americanas, que priorizam a resiliência das infraestruturas críticas e a vigilância das cadeias de fornecimento tecnológico.

Esta articulação implica, contudo, uma dependência de *standards* e tecnologias de origem americana, uma vez que o ecossistema digital da NATO é fortemente ancorado em fornecedores e sistemas dos Estados Unidos. O paradigma de interoperabilidade promovido pela Aliança, que visa assegurar a compatibilidade entre forças e sistemas, transfere também para o espaço europeu um modelo de segurança digital assente na primazia técnico-militar de Washington. Portugal beneficia dessa inserção, adquirindo competências e interoperabilidade, mas vê limitada a sua margem de manobra em decisões estratégicas sobre infraestrutura e soberania de dados. Como argumenta Gur (2022), a soberania digital europeia é condicionada pelas pressões rivais dos Estados Unidos e da China, sendo a regulação europeia uma tentativa de reafirmar o poder normativo europeu em matéria de cibersegurança.

EUA

A influência dos Estados Unidos ultrapassa a dimensão militar. O domínio económico e tecnológico americano é onnipresente na infraestrutura digital portuguesa — das plataformas de comunicação (Microsoft, Google, Meta) aos sistemas de *cloud computing*, inteligência artificial e ciberdefesa. Esta hegemonia tecnológica traduz o monopólio que as *big tech* norte-americanas exercem sobre os serviços digitais, os sistemas operativos e a infraestrutura de dados. Para Portugal, tal dependência cria uma assimetria estrutural: enquanto adere às normas europeias de soberania digital e proteção de dados, o país opera, na prática, num ecossistema digital dominado por atores privados norte-americanos. Esta dissonância entre discurso político e realidade tecnológica fragiliza a capacidade de execução de políticas de autonomia digital.

Raimundo e Ferreira-Pereira (2022) descrevem esta posição como um “*hedging* pragmático”, um equilíbrio estratégico entre fidelidade atlântica e integração europeia. No entanto, esta duplicidade tem um custo. O compromisso simultâneo com Bruxelas e Washington obriga Portugal a navegar entre dois modelos normativos distintos: o europeu, baseado na regulação e na

¹⁴ Maior exercício internacional de ciberdefesa em tempo real do mundo, organizado anualmente desde 2010 pelo *Cooperative Cyber Defence Centre of Excellence*, o centro de excelência em ciberdefesa da NATO, sediado em Tallinn, Estónia.

soberania de dados; e o norte-americano, centrado na inovação orientada pelo mercado e no controlo corporativo das infraestruturas digitais. Assim, mesmo integrado na UE, o país permanece dependente de infraestruturas de comunicação, software e segurança geridas fora do seu espaço político, o que transforma a autonomia digital num ideal político mais do que numa condição técnica alcançada.

China

A influência chinesa introduz, neste quadro, uma dimensão distinta: a penetração económica e tecnológica em setores estratégicos. Desde a crise financeira de 2011, Portugal tornou-se recetor privilegiado de investimento direto chinês, especialmente através de conglomerados como a *China Three Gorges*¹⁵ (na EDP) e a *State Grid*¹⁶ (na REN). No setor das telecomunicações, a Huawei emergiu como um parceiro relevante na expansão das redes 5G, colocando Lisboa no centro de uma disputa geopolítica global. Como demonstra Pinto Arena (2022), “*Lisbon has become a battlefield for both states’ geostrategic political ploys.*” (Pinto Arena, 2022, *abstract*), num contexto em que os Estados Unidos e a China competem pela definição de padrões tecnológicos.

A integração europeia acrescenta aqui uma camada de ambivalência. Portugal é simultaneamente um Estado-membro que subscreve os princípios da soberania digital europeia e um país periférico que depende de investimentos externos para modernizar o seu tecido tecnológico. Esta ambivalência manifesta-se na política de *non-alignment* tecnológico: Lisboa procura preservar a sua autonomia negocial com a China, enquanto se compromete com as diretrizes de segurança impostas por Bruxelas e pela NATO. O resultado é uma política digital compósita, em que cada vetor de influência — americano, chinês e europeu — se sobrepõe de forma seletiva às prioridades nacionais.

A ambivalência estratégica reflete uma tensão identitária mais profunda: a de Portugal como Estado europeu, atlântico e pós-imperial, que procura afirmar relevância num sistema

¹⁵ Empresa estatal chinesa criada em 1993, conhecida pela construção da Barragem das Três Gargantas, o maior projeto hidroelétrico do mundo. Em 2011, no contexto do programa de ajustamento financeiro português, a CTG adquiriu 21,35% do capital da EDP – Energias de Portugal, tornando-se o seu principal acionista privado. O investimento, no valor de 2,7 mil milhões de euros, concedeu à China acesso a um setor estratégico de infraestruturas energéticas interligadas a sistemas digitais (*smart grids* e plataformas de dados energéticos).

¹⁶ Maior empresa elétrica do mundo e igualmente estatal, adquiriu 25% da REN – Redes Energéticas Nacionais em 2012, no valor de 387 milhões de euros. A REN é responsável pela gestão da rede nacional de transporte de eletricidade e gás, considerada infraestrutura crítica em Portugal e na UE. A presença da SGCC é frequentemente interpretada como um vetor de influência tecnológica e geoestratégica chinesa, dada a digitalização crescente dos sistemas energéticos e o acesso a dados industriais sensíveis.

internacional assimétrico. Farrand, Carrapico e Turobov (2024) demonstram que o discurso europeu da soberania digital fundiu racionalidades de segurança e economia, transformando a autonomia tecnológica num pilar da política industrial e externa da União: “*The EU’s depiction of its cybersecurity as impacted by dependence on externally manufactured products resulted in the merging of security and economic rationales. This has translated into efforts for greater control, either through promoting production within the European physical space through security-influenced industrial policies or—when this is not possible—by exerting regulatory influence beyond Europe’s borders.*” (Farrand, Carrapico e Turobov, 2024). Contudo, a capacidade efetiva dos Estados-membros para concretizar essa soberania é desigual. Nos casos periféricos, como o português, a dependência de capital estrangeiro e a fragilidade das infraestruturas nacionais tornam a autonomia digital um processo mais discursivo que material, apoiado em regulação, mas não em produção tecnológica.

A hegemonia das empresas norte-americanas reforça esta vulnerabilidade. As dez maiores plataformas digitais do mundo — *Google, Amazon, Microsoft, Meta, Apple, Oracle, Cisco, Intel, IBM e Nvidia* — são todas de origem norte-americana. Estas empresas controlam mais de 80% do mercado global de *cloud computing* e a quase totalidade das infraestruturas de redes sociais e publicidade digital (Synergy Research Group, 2024). Portugal, como a maioria dos Estados europeus, não possui alternativa tecnológica doméstica ou europeia comparável. Assim, ainda que a UE promova o discurso da “nuvem soberana” e da autonomia estratégica, o funcionamento quotidiano das suas economias digitais permanece alicerçado em tecnologias que operam sob jurisdição americana, sujeitas ao *Cloud Act*¹⁷ e ao controlo das autoridades de segurança dos EUA.

Este monopólio digital americano não é apenas técnico, mas normativo: determina os padrões de inovação, privacidade e concorrência global. Portugal, enquanto utilizador dessas plataformas e signatário do RGPD, encontra-se no paradoxo de aplicar legislação europeia de proteção de dados através de sistemas geridos por empresas estrangeiras que operam sob regimes jurídicos distintos. Tal contradição expõe os limites da soberania regulatória num contexto de dependência tecnológica.

¹⁷ Acrónimo de *Clarifying Lawful Overseas Use of Data Act* - é uma lei federal norte-americana e o seu objetivo é clarificar e expandir o acesso das autoridades de segurança e justiça dos EUA a dados armazenados fora do território americano, desde que esses dados pertençam a empresas sediadas nos Estados Unidos, como Microsoft, Google, Amazon, Apple, Meta ou outras.

Neste contexto, a condição portuguesa ilustra de forma paradigmática a operacionalização prática daquilo que nesta dissertação se define como soberania digital partilhada. A impossibilidade de exercer um controlo exclusivo sobre as infraestruturas digitais, devido à hegemonia tecnológica norte-americana, à interdependência regulatória europeia e à penetração económica chinesa, não elimina a soberania, mas transforma a sua natureza. Portugal não abdica da sua autoridade digital; antes, redistribui-a estrategicamente entre níveis de governação e redes de cooperação que ampliam a sua capacidade de agir num ecossistema global.

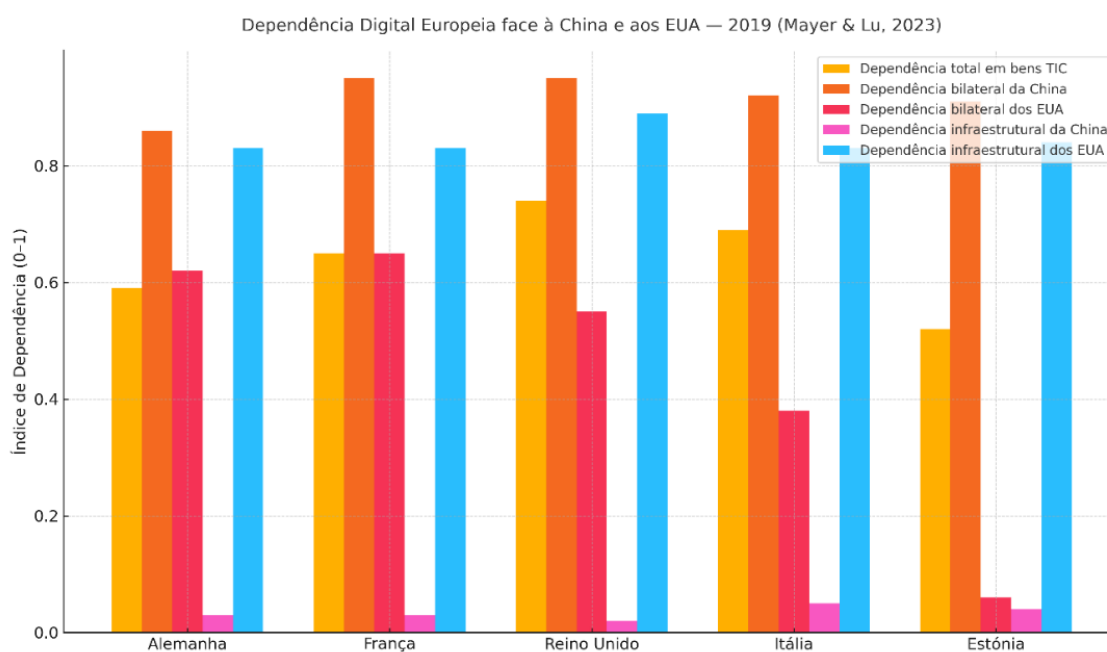
Assim, a adesão às normas europeias de cibersegurança, a participação em mecanismos de defesa da NATO e a atração seletiva de investimento chinês constituem formas complementares de exercício soberano, ainda que mediado. A soberania digital portuguesa manifesta-se, portanto, não na exclusividade territorial, mas na capacidade de coordenar múltiplas dependências em torno de objetivos nacionais e europeus convergentes.

Sob esta perspetiva, a dependência tecnológica de infraestruturas americanas, frequentemente interpretada como sinal de subordinação, pode ser reinterpretada como uma forma de delegação funcional, necessária à participação em sistemas complexos de segurança e inovação. O mesmo se aplica à integração europeia, que não anula a soberania dos Estados-Membros, mas a reconstrói como soberania partilhada, um poder distribuído que se exerce através de normas, plataformas e alianças transnacionais. Portugal, ao articular a sua política digital entre a NATO, a UE e as dinâmicas económicas globais, não apenas se adapta às constrições externas como prioriza uma soberania digital relacional, na qual a interdependência não é fraqueza, mas condição de relevância política num sistema tecnológico mundial profundamente assimétrico.

Contudo, vários autores contestam esta leitura funcionalista da interdependência, argumentando que a soberania digital europeia permanece mais discursiva do que material. Calderaro e Blumfelde (2022) consideram que a UE mantém uma “soberania digital reativa”, dependente da regulação e incapaz de projetar poder tecnológico autónomo. De modo semelhante, Broeders, Cristiano e Kaminska (2023) denunciam uma “cacofonia estratégica” entre o ideal de autonomia e a realidade da dependência de infraestruturas norte-americanas, que compromete a coerência entre os objetivos geopolíticos e as capacidades efetivas da União. Estudos quantitativos reforçam esta visão: Mayer e Lu (2023) demonstram empiricamente que os Estados europeus são hoje mais dependentes digitalmente do que há uma década, sobretudo em áreas críticas como *cloud*

computing e semicondutores: “European countries have maintained a highly vulnerable status while their autonomy gap to the US, China, and South Korea widened. The degree of digital dependence of EU members is far greater, more pervasive, and multifaceted than often assumed.” (Mayer & Lu, 2023, p. 7). Helwig (2023), por sua vez, vai mais longe ao classificar a autonomia estratégica europeia como um “sonho recorrente, mas inalcançável”, dada a persistente subordinação tecnológica e militar ao aliado transatlântico.

Figura 5. Dependência digital europeia face à China e aos EUA (2019). O gráfico apresenta índices de dependência em bens TIC e infraestruturas de comunicação para cinco países europeus. Fonte: Mayer & Lu (2023), “Digital Autonomy? Measuring the Global Digital Dependence Structure”, SSRN Electronic Journal.



Fonte: <https://ssrn.com/abstract=4404826>

O gráfico ilustra empiricamente a assimetria de poder tecnológico global que sustenta o conceito de *soberania digital partilhada*:

- A Europa (e Portugal) não possui capacidade de controlo pleno;
- A soberania digital é delegada e relacional, exercida através da regulação e da integração institucional;
- Esta condição de interdependência controlada é tanto uma estratégia de sobrevivência quanto um limite estrutural à autonomia tecnológica.

3. O Caso de Portugal: Soberania Digital e Integração Europeia

A soberania digital portuguesa inscreve-se num contexto de profunda transformação tecnológica e política, marcada pela crescente interdependência global e pela necessidade de autonomia estratégica no domínio digital. A transição para uma economia baseada em dados, inteligência artificial e conectividade de alta capacidade redefine as noções clássicas de soberania e desafia Estados de pequena e média dimensão, como Portugal, a reposicionarem-se num ecossistema dominado por grandes potências tecnológicas. Neste enquadramento, a integração europeia surge simultaneamente como uma âncora de segurança e uma limitação à margem de decisão nacional.

De acordo com o índice *Digital Economy and Society Index* (DESI) da Comissão Europeia, Portugal ocupava a 15.^a posição entre os 27 Estados-Membros em 2022, mantendo-se ligeiramente abaixo da média europeia em termos de desempenho digital global (Comissão Europeia, 2022). Embora o país demonstre pontos fortes significativos — particularmente nos serviços públicos digitais, onde se posiciona entre os líderes europeus —, enfrenta desafios estruturais persistentes em dimensões críticas como o capital humano e a transformação digital das empresas (Trade.gov, 2024). Esta dualidade entre avanços pontuais e fragilidades sistémicas caracteriza o posicionamento português no espaço digital europeu e condiciona as suas possibilidades de afirmação de soberania tecnológica.

O Governo português tem afirmado repetidamente a ambição de consolidar o país como uma "verdadeira nação digital", articulando este objetivo com o projeto europeu de transformação digital (Governo de Portugal, 2024). Esta visão pretende promover uma modernização inclusiva e sustentável, onde a digitalização é concebida como fator de competitividade económica, eficiência administrativa e coesão social. Todavia, a concretização desta ambição encontra constrangimentos estruturais e institucionais que condicionam o grau efetivo de soberania tecnológica e operacional do país.

O Plano de Ação para a Transição Digital (Governo de Portugal, 2020) define uma estratégia assente em três eixos centrais: capacitação das pessoas, digitalização das empresas e modernização do Estado. O documento reconhece que a soberania tecnológica é inseparável da capacidade de inovar e de controlar infraestruturas críticas, mas identifica também dependências

significativas de fornecedores estrangeiros, sobretudo em áreas como cloud computing, cibersegurança e semicondutores. A centralidade do setor público na implementação da estratégia digital exige, por isso, uma articulação estreita entre políticas nacionais e europeias, bem como uma maior coordenação institucional entre ministérios, agências e entidades reguladoras.

O relatório TE 100 – Soberania Digital (Xavier & Osório de Barros, 2021) argumenta que Portugal enfrenta uma forma de "soberania digital condicionada", caracterizada pela limitação da capacidade tecnológica e pela necessidade de recorrer a alianças estratégicas no seio da União Europeia. Esta dependência reflete-se na escassez de infraestruturas nacionais de grande escala, na ausência de centros de dados próprios de dimensão significativa e na dependência de plataformas de comunicação e armazenamento controladas por empresas não europeias. Embora a integração europeia mitigue alguns riscos — nomeadamente através da harmonização regulatória e da criação de normas comuns —, também impõe constrangimentos à autonomia nacional, dado que a soberania digital é partilhada entre Estados-membros e instituições da UE.

Os relatórios da Comissão Europeia sobre a Década Digital (Comissão Europeia, 2023; 2024) reforçam esta leitura. Portugal apresenta um desempenho sólido em conectividade e serviços públicos digitais, mas continua a registar défices significativos na adoção de tecnologias avançadas e na formação de especialistas em Tecnologias da Informação e Comunicação (TIC). Segundo dados de 2022, apenas 2,4% da população empregada em Portugal eram especialistas em TIC, comparados com uma média europeia superior, colocando o país na 25.^a posição do ranking europeu (DESI, 2022).

Adicionalmente, 26% da população portuguesa não possuía quaisquer competências digitais básicas, comparados com apenas 9% na média da UE (CaixaBank Research, 2022). A carência de capital humano qualificado e a reduzida capacidade de investigação e desenvolvimento tecnológico são fatores que limitam a capacidade nacional de inovação e o controlo sobre as cadeias de valor digitais. Além disso, a lenta transposição de diretivas europeias no domínio da cibersegurança, como a NIS2, concretizada apenas em dezembro de 2025 através do Decreto-Lei n.º 125/2025, muito após o prazo inicial de outubro de 2024, demonstra as dificuldades de coordenação interna e a insuficiência de mecanismos de execução legislativa (Two Birds, 2025; Ezine Eversheds-Sutherland, 2025).

A dimensão securitária da soberania digital é particularmente relevante no caso português. O ataque cibernético de 15 e 16 de outubro de 2024, que paralisou múltiplos serviços públicos online incluindo o portal Gov.pt, os sistemas de autenticação digital e outras plataformas críticas da Agência para a Modernização Administrativa (AMA), revelou fragilidades persistentes nas infraestruturas do Estado e sublinhou a urgência de uma abordagem sistémica à ciber-resiliência (Portugal Resident, 2024; The Portugal News, 2024). Este incidente, que utilizou técnicas de *ransomware* e afetou serviços essenciais durante vários dias, expôs não apenas vulnerabilidades técnicas mas também limitações na capacidade de resposta coordenada entre entidades estatais. A falta de redundância tecnológica e a dependência de soluções externas tornam o país vulnerável a falhas e coerções externas. Estas vulnerabilidades não resultam apenas de insuficiências técnicas, mas também de uma cultura administrativa ainda pouco adaptada à gestão integrada do risco digital.

A geopolítica acrescenta outra camada de complexidade. Como reporta o Diário de Notícias (2023), as tensões entre Estados Unidos e China têm implicações diretas para a política tecnológica europeia e, por consequência, para Portugal. As restrições impostas a investimentos chineses em setores estratégicos, como telecomunicações e energia, mostram como a soberania digital nacional está enredada em disputas globais por controlo tecnológico. A Resolução do Conselho de Ministros n.º 32/2023 impôs limitações ao uso de equipamentos de fornecedores considerados de alto risco nas redes 5G nacionais, refletindo a pressão crescente de aliados transatlânticos, particularmente dos Estados Unidos, para restringir a presença de empresas chinesas como Huawei e ZTE em infraestruturas críticas. Portugal, tal como outros Estados-membros, vê-se obrigado a equilibrar a abertura económica com a necessidade de proteger ativos críticos, participando numa estratégia coletiva europeia de autonomia estratégica aberta.

A nível interno, as instituições portuguesas desempenham um papel essencial na tradução das metas europeias em políticas concretas. O Centro Nacional de Cibersegurança (CNCS) e a Agência para a Modernização Administrativa (AMA) são exemplos de estruturas que funcionam como mediadores entre a regulação europeia e a execução nacional (Comissão Europeia, 2024). A consolidação destas entidades é determinante para assegurar a resiliência digital e a proteção de dados sensíveis, mas requer um reforço continuado de recursos humanos, capacidades técnicas e financiamento adequado.

O relatório TE 100 salienta que a soberania digital não deve ser entendida como um objetivo absoluto de autossuficiência tecnológica, mas como um processo contínuo de fortalecimento da capacidade nacional de decisão, inovação e controlo sobre infraestruturas críticas. A digitalização do Estado e das empresas portuguesas tem produzido resultados visíveis, sobretudo na desmaterialização de serviços públicos, no crescimento do comércio eletrónico e no aumento gradual da literacia digital. Todavia, a autonomia tecnológica permanece limitada por dependências estruturais que só podem ser superadas através de uma estratégia de longo prazo, combinando investimento público sustentado, parcerias industriais estratégicas, retenção e formação de talento qualificado e cooperação europeia efetiva.

3.1. Infraestruturas Digitais em Portugal: Dependência de Plataformas Externas

A transformação digital tem sido uma prioridade estratégica para Portugal na última década, evidenciada por um conjunto de políticas públicas e investimentos que visam modernizar as infraestruturas tecnológicas do país e promover a sua integração plena na economia digital europeia. Este esforço é parte integrante dos objetivos traçados pela UE para a Década Digital 2030. Todavia, este avanço encontra-se fortemente condicionado por uma dependência estrutural de plataformas tecnológicas externas, sobretudo de origem norte-americana, o que coloca em causa a soberania digital e compromete a autonomia do Estado português em matérias críticas como a cibersegurança, o armazenamento de dados e o controlo de infraestruturas críticas.

Segundo o relatório *Digital Decade Country Report – Portugal* (Comissão Europeia, 2023), Portugal tem alcançado progressos assinaláveis na cobertura de redes de muito alta capacidade (VHCN). De acordo com dados da Autoridade Nacional de Comunicações (ANACOM), em 2024, aproximadamente 95,3% das habitações e estabelecimentos em Portugal dispunham de acesso a redes de alta velocidade, representando um aumento de 1 ponto percentual face ao ano anterior (ANACOM, 2024). A expansão da fibra ótica tem sido particularmente significativa: as redes de fibra ótica até à habitação (FTTH/B) tornaram-se a principal via de acesso à Internet fixa, representando 68,9% das ligações de Internet fixa e 66,6% das ligações de televisão paga

(ANACOM, 2024). Estima-se que, no final de 2024, pelo menos 6,2 milhões de lares estivessem conectados a uma rede de alta velocidade, consolidando Portugal como um dos países mais avançados da União Europeia nesta dimensão, ocupando a quarta posição no ranking europeu em termos de velocidade de banda larga (ANACOM, 2024).

No que respeita à implantação da infraestrutura 5G, Portugal tem registado uma evolução acelerada. No final do quarto trimestre de 2024, o país contava com 13.089 estações base com tecnologia 5G, distribuídas por todos os 308 municípios portugueses (100% do território administrativo) e presentes em 2.259 freguesias, correspondendo a 73% das freguesias do país (ANACOM, 2025). Este crescimento de 24% face ao trimestre anterior deveu-se, em larga medida, à entrada do quarto operador comercial 5G, a DIGI Portugal, que se juntou aos três operadores incumbentes: NOS, Vodafone e MEO. A NOS liderava em número de estações instaladas (4.786), seguida pela Vodafone (4.611), DIGI (2.130) e MEO (1.562). A densidade de estações 5G alcançou, no final de 2024, uma estação por cada 7 km² e uma média de 127 estações por 100.000 habitantes. Contudo, a distribuição não é homogénea: a maior concentração verifica-se ao longo da faixa costeira ocidental, entre Viana do Castelo e Setúbal, e na faixa costeira sul (Algarve), refletindo padrões de densidade populacional e atividade económica (ANACOM, 2025).

Apesar dos avanços na cobertura física das redes, persistem assimetrias significativas entre zonas urbanas e rurais. A área territorial correspondente às freguesias sem estações 5G representava, no final de 2024, 12,9% do território nacional, correspondendo a cerca de 6,4% da população portuguesa segundo o Censo de 2021 (ANACOM, 2025). É importante notar que a presença de uma ou mais estações 5G numa freguesia não equivale a cobertura integral da sua população, pelo que a penetração efetiva da tecnologia 5G na utilização quotidiana permanece em crescimento. De acordo com a ANACOM (2024), das ligações móveis efetivamente utilizadas, 31,7% usavam a rede 5G no final de 2024 (um aumento de 14,6 pontos percentuais face a 2023), 49,6% usavam a rede 4G e 18,7% ainda recorriam às redes 2G+3G. Esta clivagem entre a disponibilidade técnica de infraestrutura e a sua utilização efetiva reforça desigualdades regionais e limita o acesso equitativo às oportunidades do digital.

Mais ainda, apesar da modernização substancial da infraestrutura de base, a utilização de plataformas tecnológicas, serviços em nuvem e sistemas operacionais continua a ser dominada por grandes empresas multinacionais como *Amazon Web Services*, *Microsoft Azure* e *Google Cloud Platform*, cujos servidores, centros de decisão e protocolos operacionais se localizam fora da jurisdição europeia. Esta realidade cria um ecossistema digital altamente dependente e vulnerável, tanto do ponto de vista tecnológico quanto político e jurídico.

O Governo português, no seu Plano de Ação para a Transição Digital (Governo de Portugal, 2020), reconhece implicitamente essa dependência ao admitir que grande parte da transformação digital nacional será operacionalizada com soluções tecnológicas internacionais. Embora o plano seja ambicioso em metas, como a digitalização de 90% dos serviços públicos e a capacitação digital de 80% da população, não define uma estratégia clara e detalhada para reduzir a vulnerabilidade causada pelo outsourcing tecnológico massivo. Tal modelo de integração acrítica de plataformas estrangeiras compromete a capacidade de o país assegurar o controlo sobre os seus próprios dados, algoritmos e infraestruturas críticas, criando potenciais riscos de interferência externa, descontinuidade de serviços e sujeição a jurisdições legais estrangeiras.

O GEE no relatório Soberania Digital em Portugal (2022), apresenta uma análise mais direta dos riscos associados à dependência tecnológica externa. O documento sublinha que a ausência de um setor tecnológico nacional robusto impede o país de desenvolver soluções próprias para áreas estratégicas como serviços cloud soberanos, inteligência artificial de base nacional, cibersegurança avançada ou software público auditável e de código aberto. Essa limitação torna-se ainda mais crítica quando se observa que grande parte das ferramentas digitais utilizadas por entidades públicas e privadas portuguesas está sujeita a regulamentações estrangeiras, especialmente dos Estados Unidos, cuja legislação, como o *CLOUD Act (Clarifying Lawful Overseas Use of Data Act)*, permite o acesso a dados armazenados por empresas norte-americanas independentemente da sua localização física, mesmo quando esses dados se encontram fisicamente em território europeu.

Este cenário é particularmente problemático no contexto da proteção de dados pessoais e da cibersegurança. A centralização do armazenamento de dados em servidores localizados fora do território nacional levanta preocupações sérias relativamente à conformidade com o RGPD, apesar dos mecanismos de adequação existentes. Além disso, como evidenciado pelo ataque informático de outubro de 2024 que afetou serviços online essenciais do Estado português, incluindo o portal Gov.pt e os sistemas de autenticação da AMA (Expresso, 2024; RTP, 2024), a vulnerabilidade das infraestruturas digitais é real e está diretamente associada ao uso de soluções tecnológicas cuja manutenção, segurança e atualização não são controladas internamente pelo Estado português.

A fragilidade institucional perante estes riscos é agravada por atrasos legislativos significativos. A transposição da Diretiva NIS2 (Diretiva (UE) 2022/2555 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União), que visa reforçar os requisitos de cibersegurança a nível europeu e estabelecer obrigações mais rigorosas para entidades essenciais e importantes, foi concretizada apenas em 4 de dezembro de 2025, através do Decreto-Lei n.º 125/2025, com entrada em vigor prevista para 3 de abril de 2026 (*Two Birds*, 2025; Copla, 2025). Este prazo situa-se muito depois do prazo inicial estipulado pela Comissão Europeia (17 de outubro de 2024), tendo Portugal sido alvo de cartas de notificação formal em novembro de 2024 e de parecer fundamentado em maio de 2025, juntamente com outros Estados-Membros em incumprimento (*Digital Strategy EC*, 2025). Tal atraso não só coloca Portugal em incumprimento das suas obrigações europeias mas também demonstra uma falta de agilidade institucional e de capacidade de coordenação interministerial na adaptação ao novo contexto de ameaças digitais. Esta morosidade na transposição de diretivas críticas expõe o país a vulnerabilidades tecnológicas ampliadas, potenciais sanções europeias e perda de credibilidade na governação digital.

A implantação da infraestrutura 5G em Portugal, embora tecnologicamente promissora e alinhada com as metas europeias de conectividade, também se insere num contexto geopolítico altamente sensível. A presença de empresas chinesas como a Huawei e a ZTE em projetos de redes móveis tem gerado preocupações significativas entre aliados transatlânticos, especialmente os Estados Unidos, que têm instado os seus parceiros europeus a restringirem ou eliminarem o envolvimento de fornecedores chineses em redes de comunicações críticas, invocando riscos de espionagem, sabotagem e controlo remoto de infraestruturas vitais.

Esta tensão geoestratégica repercutiu-se diretamente em Portugal, onde o governo evitou inicialmente alinhar-se explicitamente com posições restritivas radicais, optando por uma abordagem técnica e regulatória supostamente neutra, baseada em critérios de risco e certificação de segurança. No entanto, em 2023, a Resolução do Conselho de Ministros n.º 32/2023 acabou por impor limitações concretas ao uso de equipamentos de fornecedores considerados de alto risco nas redes 5G nacionais, especialmente nas componentes nucleares da rede (core network). Esta decisão insere-se num movimento mais amplo da UE para reforçar a segurança das infraestruturas digitais e reduzir dependências estratégicas de fornecedores externos considerados potencialmente arriscados, embora continue a suscitar críticas e debates quanto à real eficácia das medidas, à dependência de fornecedores alternativos (maioritariamente europeus e norte-americanos como Ericsson, Nokia, Samsung) e aos custos económicos e técnicos associados à substituição de equipamentos já instalados.

No plano internacional, a dependência tecnológica de Portugal está alinhada com a tendência geral da União Europeia, que tem vindo a debater intensamente o conceito de "soberania digital" como uma resposta estratégica ao domínio global das Big Tech norte-americanas e chinesas. No entanto, como alerta o Council on Foreign Relations (CFR, 2023), esta retórica europeia frequentemente contrasta com a realidade de um ecossistema digital altamente dependente de infraestruturas, serviços, protocolos e standards externos. O artigo defende que, em vez de falar de soberania digital em termos absolutos de autossuficiência tecnológica (objetivo inatingível a curto e médio prazo), a UE e os seus Estados-membros deveriam adotar uma abordagem baseada em "responsabilidade digital", que privilegia o controlo regulatório rigoroso, a transparência algorítmica, a auditabilidade dos sistemas e a interoperabilidade sem pretensões de autossuficiência tecnológica total.

Para Portugal, esta proposta pode ser particularmente relevante, uma vez que o país não dispõe de escala económica, capacidade industrial consolidada nem massa crítica de recursos humanos especializados para competir diretamente com os gigantes tecnológicos globais na produção de hardware, desenvolvimento de sistemas operacionais ou criação de plataformas digitais dominantes. Todavia, pode contribuir de forma significativa para uma regulação europeia mais eficaz, para a promoção de plataformas tecnológicas interoperáveis, auditáveis e baseadas em standards abertos, e para a criação de nichos de especialização tecnológica em áreas como a

cibersegurança, a inteligência artificial aplicada a domínios específicos e as tecnologias de língua portuguesa.

Neste contexto, Portugal tem procurado mitigar parcialmente esta dependência através da integração em iniciativas coletivas europeias, como os *European Digital Innovation Hubs* (EDIHs), os projetos IPCEI (*Important Projects of Common European Interest*) focados em microeletrónica, *cloud* e inteligência artificial, e o programa *Horizon Europe* para investigação e inovação. Particularmente relevante é a participação portuguesa no projeto Gaia-X, uma iniciativa franco-alemã que visa criar uma infraestrutura europeia de cloud federada, soberana, interoperável e baseada em princípios de transparência e controlo de dados (Autolitano & Pawlowska, 2021). Embora Portugal não lidere o projeto, a participação de universidades como a Universidade do Minho, de centros de investigação como o INESC TEC e de algumas empresas tecnológicas nacionais em consórcios europeus demonstra uma tentativa de alinhamento com a estratégia europeia de autonomia digital aberta. Contudo, a efetividade destas parcerias e a capacidade de Portugal para influenciar as agendas e captar benefícios substanciais permanecem limitadas pela sua posição periférica no ecossistema tecnológico europeu.

O fator humano constitui outro vetor essencial e frequentemente subestimado na análise da dependência tecnológica. A formação em competências digitais avançadas, a capacidade de inovação tecnológica de base e o investimento sustentado em ciência e tecnologia são determinantes para a construção de uma autonomia tecnológica efetiva e duradoura. Xu e Wu (2025), embora analisando primariamente o contexto chinês, demonstram que a rápida evolução das tecnologias digitais, especialmente no domínio da inteligência artificial generativa, aprendizagem automática e computação quântica, está a ultrapassar significativamente a capacidade de adaptação dos sistemas educativos e de formação profissional tradicionais. Este diagnóstico pode ser facilmente transposto para Portugal, onde a oferta formativa em áreas críticas como cibersegurança avançada, engenharia de redes de nova geração, ciência de dados, desenvolvimento de software de infraestrutura ou arquitetura de sistemas distribuídos permanece limitada, fragmentada e assimétrica geograficamente. O défice estrutural de capital humano qualificado compromete não apenas a utilização crítica, consciente e segura das plataformas digitais existentes, mas também, e talvez mais gravemente, a capacidade endógena de criação, manutenção, auditoria e evolução de soluções tecnológicas próprias.

Neste sentido, a ausência de um ecossistema tecnológico nacional competitivo, articulado, sustentado e de dimensão crítica é um dos fatores que mais contribuem para a perpetuação estrutural da dependência externa. Portugal possui, indubitavelmente, polos de inovação relevantes (como o Taguspark, a Braga Tech Hub, o UPTEC no Porto), universidades com centros de investigação de reconhecida excelência internacional (INESC, IT, IEETA, entre outros) e várias *startups* tecnológicas emergentes que têm alcançado visibilidade global. Importa destacar que o ecossistema de *startups* português produziu sete unicórnios (empresas tecnológicas avaliadas em mais de mil milhões de dólares), incluindo Talkdesk (avaliada em 10 mil milhões de dólares), OutSystems (4,3 mil milhões), Sword Health (4 mil milhões), Remote (3 mil milhões), Anchorage Digital (3 mil milhões), TEKEVER (1,3 mil milhões) e Feedzai (1 mil milhões) (Portugal Business News, 2025; TechRound, 2024). Estes sucessos empresariais, concentrados sobretudo em áreas como *software* empresarial, *contact centers* em nuvem, saúde digital, recursos humanos remotos, criptomoedas, drones de vigilância e prevenção de fraude, demonstram capacidade de inovação e execução em nichos específicos.

No entanto, apesar destes sucessos pontuais, falta um investimento público e privado coordenado, de longo prazo e de escala significativa que transforme estas iniciativas dispersas em políticas de Estado estruturantes e sustentáveis. O apoio sistemático a *startups* de base tecnológica, o incentivo direto e eficaz à criação e proteção de propriedade intelectual nacional, a retenção estratégica de talento especializado (evitando a "fuga de cérebros" para outros países europeus e para os Estados Unidos), a criação de condições para a reindustrialização tecnológica e a articulação efetiva entre universidades, centros de investigação, empresas e Estado são áreas que requerem intervenção política direta, continuada e dotada de recursos financeiros substanciais.

No plano europeu, Portugal tem procurado mitigar parcialmente esta dependência e impulsionar a transformação digital através da integração ativa em iniciativas coletivas e da captação de financiamento europeu. Estas parcerias e programas permitem aceder a financiamento significativo, conhecimento especializado, redes de colaboração transnacionais e economias de escala que, de outro modo, estariam fora do alcance de um país de dimensão média. Contudo, continuam a colocar Portugal numa posição frequentemente periférica ou de seguidor, em vez de líder ou cocriador das agendas tecnológicas europeias. Para que estas oportunidades produzam efeitos estruturais duradouros e não apenas benefícios pontuais, é imperativo que o país assuma

uma postura mais ativa, assertiva e estratégica na definição de prioridades, na liderança de consórcios internacionais, na mobilização de recursos próprios substantivos (cofinanciamento) e no desenvolvimento de capacidades nacionais de absorção e aplicação do conhecimento adquirido.

Por outro lado, o Plano de Recuperação e Resiliência (PRR), financiado pelo instrumento *Next Generation EU*, apresenta-se como uma oportunidade crítica e historicamente única para o reforço estrutural das infraestruturas digitais nacionais. O plano inclui investimentos significativos, na ordem dos 2,5 mil milhões de euros destinados à digitalização da administração pública, à modernização profunda do setor educativo (incluindo equipamento, formação de professores e curricula adaptados) e à transição digital acelerada do tecido empresarial, com particular enfoque nas PME. No entanto, a eficácia real destas medidas depende criticamente da sua execução estratégica, tecnicamente rigorosa, coordenada institucionalmente e orientada para a capacitação endógena e sustentável, e não apenas para o atingimento superficial de metas numéricas ou indicadores quantitativos de digitalização. O simples recurso massivo e acrítico a soluções tecnológicas externas, sem desenvolvimento paralelo de competências internas, infraestruturas próprias e capacidade de auditoria e controlo, poderá, paradoxalmente, agravar em vez de resolver a dependência tecnológica estrutural atual, tornando-a ainda mais profunda e difícil de reverter no futuro.

Diante deste panorama complexo e multidimensional, torna-se evidente que o desenvolvimento das infraestruturas digitais em Portugal está fortemente condicionado por limitações estruturais (escala económica, base industrial reduzida), políticas (descontinuidades governamentais, falta de visão estratégica de longo prazo), económicas (investimento insuficiente em I&D, dependência de financiamento externo) e humanas (escassez de talento qualificado, "fuga de cérebros"). O país encontra-se indubitavelmente num processo acelerado de modernização tecnológica e de adaptação às exigências da economia digital global. Todavia, esse processo tem sido alicerçado predominantemente em soluções, plataformas, serviços e tecnologias produzidos no exterior, o que levanta sérias dúvidas fundamentais quanto à sustentabilidade a longo prazo, à autonomia estratégica efetiva e à segurança sistémica do ecossistema digital nacional.

A questão central que emerge de forma incontornável é se o país pretende continuar indefinidamente a desempenhar o papel de consumidor maioritariamente passivo, dependente e periférico de tecnologias concebidas, produzidas e controladas no exterior, ou se está política, económica e socialmente disposto a investir de forma sustentada, estratégica e ambiciosa numa estratégia nacional de capacitação interna, inovação tecnológica endógena, regulação assertiva e soberana, cooperação europeia ativa e formação massiva de capital humano qualificado, que permita construir, ao longo das próximas décadas, um futuro digital verdadeiramente soberano, resiliente, seguro e sustentável.

3.2. Políticas Digitais Nacionais no Contexto da União Europeia

A transformação digital tornou-se uma prioridade central no projeto europeu. A UE tem vindo a estabelecer um conjunto robusto de metas, regulamentos e estratégias para garantir uma transição digital justa, segura e inclusiva para todos os Estados-Membros. Neste contexto, Portugal tem procurado alinhar as suas políticas digitais nacionais com os objetivos estratégicos da UE, não apenas através da transposição legislativa obrigatória, mas também com a formulação de programas e iniciativas próprias, que refletem as prioridades europeias. Este capítulo explora o percurso português no domínio da política digital à luz das exigências e oportunidades trazidas pela integração europeia. O alinhamento nacional com a UE tem sido conduzido por planos estratégicos como a Estratégia Digital Nacional e impulsionado por instrumentos financeiros como o Plano de Recuperação e Resiliência (PRR), mas também enfrenta diversos desafios ao nível da execução, inclusão e capacidade institucional.

A base do enquadramento europeu é hoje a Bússola Digital 2030, apresentada pela Comissão Europeia em 2021, que estabelece metas ambiciosas para a transição digital da UE até ao final da década. Estas metas incluem a formação de competências digitais básicas para pelo menos 80% da população, a digitalização plena dos serviços públicos, a implementação de infraestruturas digitais seguras e sustentáveis e a transformação digital do tecido empresarial (Comissão Europeia, 2021). A convergência com estas metas requer, por parte dos Estados-Membros, políticas públicas nacionais que articulem estas prioridades com os contextos

económicos e sociais internos. Portugal tem respondido a este desafio com um conjunto de estratégias e mecanismos institucionais que procuram garantir não apenas a conformidade com a UE, mas também a afirmação de uma visão própria para a digitalização do país.

Desde 2020, a principal referência para a política digital nacional é a Estratégia Portugal Digital, um documento estruturado em torno de três grandes eixos: a capacitação e inclusão digital das pessoas, a digitalização das empresas e a modernização da administração pública. Este plano foi desenvolvido para responder diretamente às metas da UE e é operacionalizado pela Estrutura de Missão Portugal Digital, uma entidade criada com o objetivo de coordenar a execução da estratégia e de funcionar como ponto de contacto com os parceiros europeus (Portugal Digital, 2025) No domínio da capacitação, destaca-se o programa INCoDe.2030, que visa fomentar competências digitais em todas as fases da vida, desde o ensino básico até à requalificação profissional. Ao nível empresarial, foram criadas linhas de financiamento para incentivar a adoção de tecnologias emergentes como IA, *big data e IoT*, bem como para fortalecer a cibersegurança nas PME. Quanto à administração pública, os esforços têm incidido na digitalização de serviços, na interoperabilidade entre sistemas e na melhoria da experiência do cidadão na interação com o Estado.

Esta estratégia é complementada por um esforço de alinhamento regulatório com os principais diplomas da UE no domínio digital. Portugal transcreveu e adaptou os regulamentos como o RGPD, o DSA, o DMA e a diretiva NIS. O país participa ativamente em grupos de trabalho da Comissão Europeia, no Conselho da UE e em redes como a GovTech4All, procurando estar na linha da frente das negociações e da implementação. Instituições como a AMA, o CNCS, a ANACOM e a Secretaria de Estado da Digitalização têm desempenhado papéis centrais na articulação entre os níveis nacional e europeu da governação digital. Esta coordenação interinstitucional tem sido fundamental para garantir a coerência das políticas e para responder às exigências técnicas e legislativas da UE (Interoperable Europe - Governance Portugal, 2025)

Um dos instrumentos mais relevantes para o avanço da digitalização em Portugal é o PRR. Este plano mobiliza cerca de 3,5 mil milhões de euros para a transição digital, cobrindo áreas como a administração pública, a educação e a economia. A componente digital do PRR está totalmente alinhada com a Bússola Digital da UE, sendo a sua execução monitorizada com base em metas e

indicadores europeus. No setor público, prevê-se a reengenharia de serviços e a modernização de sistemas de informação. No domínio educativo, o plano apoia a digitalização de escolas e a formação de professores em competências digitais. Já nas empresas, o foco está no apoio à transição digital das PME e na promoção de soluções tecnológicas inovadoras.

Apesar destes avanços, Portugal enfrenta desafios significativos que limitam a profundidade do seu alinhamento com a UE. Em primeiro lugar, subsiste uma capacidade técnica e administrativa reduzida em muitas entidades públicas, o que dificulta a implementação de políticas complexas. A falta de recursos humanos qualificados, sobretudo fora das grandes áreas metropolitanas, compromete a eficiência da transição digital. Em segundo lugar, há uma marcada desigualdade regional no acesso a infraestruturas digitais e na literacia digital da população. As zonas rurais continuam a ter conectividade limitada, e os níveis de competências digitais são particularmente baixos entre os mais idosos e os menos escolarizados. Estes fatores constituem obstáculos à realização dos objetivos europeus de inclusão e coesão.

Outro desafio relevante é a dependência tecnológica de fornecedores estrangeiros. Embora não seja exclusivo de Portugal, este fenómeno levanta questões sobre a soberania digital e a segurança dos dados. A utilização de soluções de *cloud computing* e *software* empresarial fornecidos por gigantes tecnológicos não europeus levanta preocupações sobre a conformidade com a legislação da UE e a vulnerabilidade a pressões geopolíticas (OCDE, 2022). Portugal tem iniciado um debate sobre alternativas mais autónomas, mas ainda há um longo caminho a percorrer para reduzir esta dependência.

A articulação entre estratégias nacionais e metas europeias é também condicionada por fatores políticos e institucionais. A constante reorganização de competências governamentais, a mudança de prioridades com alterações no executivo e a fragmentação das políticas setoriais criam dificuldades na criação de uma visão coerente e duradoura para o digital. A ausência de um quadro legal nacional consolidado sobre soberania digital, que vá além da simples transposição de diretivas da EU, é sintomática desta fragilidade. Embora existam instrumentos e planos, falta uma narrativa estratégica integrada que articule soberania, inovação, segurança e inclusão.

Ainda assim, há sinais positivos pois Portugal tem sido reconhecido pela Comissão Europeia pelo seu envolvimento em projetos-piloto no domínio da interoperabilidade europeia e pelos esforços na digitalização de serviços públicos, como a autenticação digital e os balcões únicos (Comissão Europeia, 2021). O país também demonstrou abertura à experimentação com tecnologias emergentes, incluindo *blockchain*. Além disso, a cooperação com outros Estados-Membros, como Espanha, França e Alemanha, tem sido intensificada através de consórcios europeus para desenvolvimento de infraestruturas digitais comuns, como o *Gaia-X*.

A nível legislativo, Portugal tem dado seguimento à implementação do DSA e do DMA, nomeadamente no reforço dos mecanismos de supervisão das grandes plataformas digitais. A adaptação da administração à nova lógica da regulação digital implica o desenvolvimento de novas competências na ANACOM, que poderá vir a desempenhar o papel de coordenador dos serviços digitais. Esta transição institucional é fundamental para garantir que a implementação dos regulamentos europeus se faz com eficácia e em conformidade com os direitos fundamentais.

A política digital portuguesa tem evoluído significativamente nos últimos anos, com uma clara orientação para o alinhamento com a UE. Este alinhamento não se traduz apenas na transposição normativa, mas também em esforços reais de capacitação, investimento e reforma institucional. No entanto, a concretização plena dos objetivos europeus exige mais do que compromisso político, requer execução eficiente, coordenação institucional robusta e inclusão social profunda. A soberania digital, no contexto de uma UE cada vez mais reguladora, constrói-se a partir de dentro, e Portugal terá de reforçar os seus recursos, capacidades e visão estratégica para se afirmar como um ator digital relevante e resiliente.

3.3. Parcerias com Empresas Estrangeiras no Setor Tecnológico

A construção da soberania digital nacional exige uma leitura crítica das relações com os grandes atores tecnológicos internacionais. Em Portugal, as parcerias com empresas estrangeiras têm assumido um papel central na transformação digital, com impactos que vão desde o desenvolvimento de infraestruturas até à gestão de dados estratégicos. Estas colaborações, embora impulsionem a inovação e atraiam investimento, também levantam preocupações quanto à

dependência estrutural, à segurança digital e à compatibilidade com os objetivos estratégicos da UE (Carvalho & Batista, 2023).

Nas últimas duas décadas, Portugal tem adotado uma política de abertura ao IDE no setor das TIC. Programas como o *Tech Visa*, regimes fiscais atrativos e a criação de *hubs* tecnológicos em Lisboa, Braga, Aveiro e Coimbra contribuíram para atrair multinacionais como AWS, Cisco, Huawei, Google, Accenture, IBM e Siemens (Relatório Nacional de Inovação 2022). Estas empresas têm colaborado com o Estado, universidades e setor privado em áreas como *cloud*, IA, cibersegurança, formação e transformação digital.

A AWS tem reforçado a sua presença através de acordos com o setor público e instituições de ensino, incluindo os programas AWS Educate e AWS Academy. Através destes, escolas e universidades adotam ferramentas e conteúdos didáticos desenvolvidos pela empresa. Paralelamente, existem colaborações com o governo para suporte técnico à migração de serviços públicos para a *cloud*, com aplicações em áreas como educação, justiça e saúde. Embora estas soluções ofereçam vantagens técnicas, levantam riscos relacionados com a gestão de dados fora da UE e a conformidade com o RGPD.

A Huawei mantém operações relevantes no país, especialmente no desenvolvimento de redes 5G e projetos-piloto em *smart cities*. Apesar das diretrizes da UE sobre fornecedores de alto risco, Portugal optou por manter a colaboração com a empresa, sujeitando-a a critérios técnicos. Esta decisão reflete uma abordagem pragmática, mas suscita dúvidas quanto ao alinhamento estratégico com os princípios da UE no domínio da segurança digital (Comissão Europeia, 2023).

A Cisco tem sido uma das principais parceiras em cibersegurança. Através de acordos com o CNCS e instituições académicas, tem oferecido formação técnica especializada e apoiado a criação de CSIRT. Embora esta colaboração fortaleça capacidades nacionais, há risco de dependência excessiva de soluções e plataformas de um único fornecedor (Batista & Costa, 2022).

No campo da IA, empresas como Google, Accenture e IBM estão ativamente envolvidas em projetos com instituições públicas e *start-ups* nacionais. Estas parcerias focam-se em aplicações de IA para modernização administrativa, análise preditiva e serviços digitais inteligentes (Brigola, 2025). Embora promovam inovação, colocam em causa a transparência

algorítmica, a auditoria das decisões automatizadas e a gestão de dados em ambientes sob jurisdição não europeia.

Ao nível da capacitação digital, empresas como Google, Microsoft e Cisco lideram programas de formação como *Grow with Google*, *Microsoft Learn* e *Cisco Networking Academy*. Estas plataformas são amplamente utilizadas no ensino secundário e superior. Apesar de aumentarem a literacia digital, podem condicionar a diversidade metodológica e acentuar a dependência de tecnologias proprietárias (Carvalho & Batista, 2023).

O tratamento e transferência de dados é um dos aspetos mais críticos destas parcerias. A maioria das plataformas utilizadas por cidadãos e entidades públicas, incluindo redes sociais, motores de busca e serviços *cloud*, é operada por empresas sediadas fora da UE. Mesmo com cláusulas contratuais-tipo ou decisões de adequação, a aplicação do RGPD nem sempre é eficaz, sobretudo quando as autoridades de supervisão enfrentam limitações técnicas e jurídicas (OCDE, 2022).

Portugal tem procurado reduzir estas vulnerabilidades através da participação em iniciativas como o *Gaia-X*, que visa criar uma infraestrutura europeia de *cloud* soberana. Apesar de o país não liderar o projeto, a participação de universidades e empresas em consórcios europeus demonstra uma tentativa de alinhamento com a estratégia da EU (Autolitano & Pawlowska, 2021).

A nível local, várias câmaras municipais portuguesas têm vindo a desenvolver e implementar projetos de cidades inteligentes em parceria com empresas tecnológicas e plataformas digitais, abrangendo áreas como mobilidade urbana inteligente, sensores ambientais, gestão de dados e videovigilância, e plataformas para decisões em tempo real. Eventos e redes como o *Portugal Smart Cities Summit* e iniciativas de governação inteligente mostram esta colaboração entre municípios, empresas e instituições inovadoras para responder aos desafios urbanos. Em Lisboa, por exemplo, a Plataforma de Gestão Inteligente integra tecnologia e dados para apoiar serviços municipais estratégicos. Estas parcerias podem aumentar a eficiência urbana, mas também levantam preocupações sobre vigilância digital, opacidade algorítmica e governança de dados em ambientes que muitas vezes operam fora de marcos regulatórios nacionais específicos.

As políticas públicas refletem esta ambiguidade: por um lado, promovem a abertura a parcerias e à digitalização como catalisadores de crescimento económico e modernização, por outro admitem a necessidade de fortalecer a autonomia digital. Documentos como a Estratégia Digital Nacional, que afirma o objetivo de reforçar a soberania tecnológica no quadro da competitividade digital, e a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, que estrutura a capacidade nacional em matéria de segurança digital, destacam a importância da soberania, mas não apresentam mecanismos concretos para reduzir dependências tecnológicas externas ou criar um ecossistema tecnológico totalmente autónomo.

Portugal também carece de um quadro legal robusto que limite a atuação de fornecedores estrangeiros em setores digitais críticos. Ao contrário de países como Alemanha ou Suécia, o país ainda não implementou legislação nacional para excluir empresas de alto risco. A aplicação dos regulamentos da UE, como o DSA, o DMA e o RGPD, é feita de forma ainda incipiente, dificultando a fiscalização efetiva (Carvalho & Batista, 2023).

Outro fator relevante é o défice de inovação endógena. Apesar de existirem *startups* tecnológicas promissoras, a balança comercial digital é desequilibrada. A maior parte do *software* utilizado é importado, e a propriedade intelectual pertence, na sua maioria, a empresas estrangeiras. Esta situação limita a criação de valor nacional e acentua a vulnerabilidade externa (OCDE, 2022).

O domínio da saúde digital é paradigmático em Portugal. A digitalização crescente dos hospitais e unidades de cuidados de saúde implica a utilização de plataformas de gestão de dados clínicos e sistemas interoperáveis, exigindo integração entre diferentes fontes de dados e serviços. Documentos oficiais sobre a estratégia de dados em saúde realçam a necessidade de estruturas robustas de governança, privacidade e segurança de dados, reconhecendo que estes aspetos são desafios centrais para o Serviço Nacional de Saúde (SPMS, 2020). Esta dependência de infraestruturas e soluções tecnológicas, muitas vezes desenvolvidas fora do espaço regulamentar português ou europeu, levanta questões éticas e legais em torno da soberania dos dados dos cidadãos e da interoperabilidade entre sistemas nacionais, especialmente na ausência de soluções nacionais amplamente certificadas.

Outro exemplo relevante é o setor energético. Empresas como *Siemens* e *General Electric* colaboram com operadores portugueses na digitalização de redes e sistemas inteligentes de gestão de energia. Estas parcerias são essenciais para a transição energética digital, mas também implicam a integração de infraestruturas críticas sob controlo tecnológico externo, com potenciais implicações em caso de conflitos ou falhas de fornecimento.

No setor da justiça, estão em curso projetos de digitalização dos tribunais e sistemas judiciais, com apoio técnico de empresas externas. Embora a modernização seja positiva, o outsourcing de funções sensíveis, como a transcrição automática ou a análise de processos, levanta preocupações quanto à segurança e independência do sistema judicial (Batista & Costa, 2022).

A crescente automatização do setor público português, com recurso a algoritmos desenvolvidos por terceiros, exige maior escrutínio técnico e jurídico. A auditoria dos sistemas, a explicabilidade das decisões e a neutralidade das ferramentas são requisitos centrais da estratégia da UE, mas a sua aplicação em Portugal ainda é limitada (Comissão Europeia, 2023).

O setor educativo também ilustra os riscos da dependência tecnológica. Embora plataformas como *Google Workspace for Education*, *Microsoft Teams* e outras estejam amplamente disseminadas nas escolas, a sua utilização massiva levanta dúvidas quanto à privacidade dos dados dos alunos e à soberania pedagógica (Carvalho & Batista, 2023). Há uma necessidade urgente de diversificar os fornecedores e criar soluções nacionais interoperáveis com os princípios europeus. A ausência de uma estratégia nacional sólida para a promoção de tecnologia nacional, combinada com a aplicação frágil dos regulamentos europeus, coloca em risco os objetivos de soberania digital defendidos pela UE. É imperativo que Portugal avance para uma política digital mais assertiva, que combine abertura à inovação com exigência de autonomia, transparência e controlo democrático.

3.4. O Papel de Portugal nas Políticas Digitais da União Europeia

Portugal tem assumido um papel relevante e crescente no processo de construção e implementação das políticas digitais da UE, posicionando-se como um Estado-membro empenhado na consolidação de um espaço digital europeu assente na competitividade, inovação, inclusão e respeito pelos direitos fundamentais. A sua participação nas dinâmicas comunitárias não se limita à adoção passiva das diretivas e regulamentos emanados das instituições europeias; pelo contrário, Portugal tem procurado intervir de forma ativa, quer no debate político, quer na operacionalização dos instrumentos jurídicos e estratégicos que orientam a transição digital europeia.

O quadro das políticas digitais da UE tem evoluído de forma acelerada, em resposta à necessidade de reforçar a soberania tecnológica, reduzir dependências externas e assegurar uma transformação digital que beneficie todos os cidadãos e empresas europeias. Neste contexto, o papel de Portugal reflete-se em três dimensões essenciais: a contribuição política e diplomática na definição das agendas comunitárias; a cooperação técnica e legislativa na implementação de regulamentos estruturantes como o DSA e o DMA; e a participação em programas de financiamento e capacitação que sustentam o avanço do Mercado Único Digital.

Durante a sua Presidência do Conselho da UE, no primeiro semestre de 2021, Portugal desempenhou um papel decisivo na promoção de consensos entre os Estados-membros em torno da Declaração Europeia sobre os Direitos e Princípios Digitais, documento que viria a ser adotado pela Comissão Europeia em 2022 e que constitui a base ética e política da Década Digital (Comissão Europeia, 2022). Essa declaração consagra um conjunto de princípios que orientam o desenvolvimento tecnológico europeu, sublinhando a importância da centralidade do ser humano, da inclusão digital, da proteção dos dados pessoais e da sustentabilidade ambiental no uso das tecnologias digitais. O envolvimento português neste processo ilustra uma diplomacia digital centrada em valores, na medida em que Lisboa defendeu, desde o início das negociações, que a transição digital deveria ser acompanhada por uma transição ética e social, assegurando que a inovação tecnológica não agrava desigualdades nem compromete direitos fundamentais.

Portugal também se destacou no apoio à criação e implementação do Pacote dos Serviços Digitais, composto pelo DSA e pelo DMA, dois regulamentos estruturantes aprovados em 2022 que visam modernizar o quadro jurídico europeu relativo à economia digital. O DSA introduz obrigações reforçadas para as plataformas em linha, impondo-lhes deveres de transparência e de mitigação de riscos sistémicos, enquanto o DMA tem por objetivo assegurar uma concorrência leal no mercado digital, prevenindo práticas abusivas por parte dos denominados “*gatekeepers*” (Comissão Europeia, 2025). Desde o início do processo legislativo, Portugal manifestou-se favorável à adoção destes instrumentos, defendendo a necessidade de equilibrar a liberdade de inovação das plataformas com a responsabilidade social e legal das mesmas.

No plano interno, Portugal tem desenvolvido esforços para transpor e aplicar as disposições destes regulamentos. O Governo português aprovou, em 2025, um projeto de diploma que cria o Coordenador dos Serviços Digitais, entidade responsável por supervisionar a aplicação do DSA a nível nacional, em articulação com a Comissão Europeia e com os reguladores dos restantes Estados-membros (Governo de Portugal, 2025). Esta estrutura visa garantir a eficácia da supervisão das plataformas e o cumprimento das normas europeias relativas a conteúdos ilegais, publicidade e moderação algorítmica. Todavia, o processo não tem estado isento de desafios. Em maio de 2025, a Comissão Europeia decidiu instaurar processos de infração contra vários Estados-membros, incluindo Portugal, por atrasos na plena implementação do DSA e na nomeação dos respetivos coordenadores nacionais (Reuters, 2025). Tal situação evidencia as dificuldades de coordenação administrativa e técnica que podem emergir quando os Estados procuram alinhar as suas estruturas nacionais com novos modelos regulatórios europeus, especialmente em áreas tecnologicamente complexas e juridicamente inovadoras.

A nível político, Portugal tem procurado afirmar-se como mediador entre posições divergentes no seio da UE, particularmente no que respeita à regulação das grandes plataformas e à governação dos dados. O país tem defendido, em diversos fóruns europeus, a necessidade de encontrar um equilíbrio entre a soberania digital europeia e a abertura à cooperação internacional, bem como entre a inovação tecnológica e a proteção dos consumidores. Esta postura diplomática é visível nas intervenções portuguesas em grupos de trabalho do Conselho da UE e em iniciativas como o Conselho Europeu da Inovação Digital, onde representantes nacionais têm contribuído para a definição de parâmetros técnicos sobre interoperabilidade e cibersegurança (Run, 2023).

A Estratégia Europeia para os Dados constitui outra das áreas em que Portugal tem desempenhado um papel relevante. O objetivo central desta estratégia é criar um espaço comum de dados, sustentado por princípios de confiança, interoperabilidade e inovação aberta (Comissão Europeia, 2025). A nível europeu, Portugal tem apoiado a criação dos *Common European Data Spaces*, que permitirão a partilha segura de dados entre setores como saúde, energia, transportes e administração pública. O país tem também desenvolvido iniciativas nacionais complementares, como o programa *AI Portugal 2030*, que integra as orientações da UE sobre IA responsável e estabelece um quadro estratégico nacional para promover o uso ético e seguro da IA (INCoDe.2030, 2023).

Além do papel legislativo e técnico, Portugal tem participado ativamente na execução de programas de financiamento europeu, que visam acelerar a transição digital nos Estados-membros. No âmbito do programa Europa Digital e do Mecanismo Interligar a Europa (CEF Digital), Portugal beneficiou de fundos destinados à expansão das infraestruturas 5G, à modernização dos serviços públicos digitais e ao reforço das capacidades de cibersegurança (Comissão Europeia, 2025). Estes investimentos são fundamentais para reduzir a desigualdade territorial em matéria de conectividade e para consolidar o papel de Portugal como um polo de inovação tecnológica no espaço europeu.

Os relatórios da Comissão Europeia no âmbito da Década Digital evidenciam que Portugal se encontra entre os países com melhor desempenho em serviços públicos digitais e integração tecnológica nas PME, embora ainda enfrente lacunas significativas na área das competências digitais básicas e avançadas (Comissão Europeia, 2025). Estes resultados reforçam a importância da articulação entre políticas europeias e nacionais, uma vez que a concretização dos objetivos da Década Digital depende tanto da implementação harmonizada dos regulamentos da UE como da capacidade dos Estados em traduzir essas orientações em medidas de proximidade, formação e apoio à inovação.

No domínio da cibersegurança, Portugal tem igualmente seguido de perto a evolução das políticas europeias, contribuindo para o reforço das capacidades conjuntas da UE. A participação portuguesa na Rede Europeia de Centros de Cibersegurança e na Agência Europeia para a Cibersegurança (ENISA) tem permitido partilhar boas práticas e desenvolver infraestruturas de segurança comuns, fundamentais para enfrentar ameaças híbridas e ataques informáticos transnacionais. Estas iniciativas são também relevantes para o cumprimento do Regulamento NIS2, que estabelece novas obrigações de segurança para operadores de serviços essenciais e prestadores de serviços digitais (ENISA, 2024).

A nível institucional, Portugal tem mantido uma postura de cooperação estreita com as principais entidades europeias de governação digital, nomeadamente a Comissão Europeia e o Parlamento Europeu. O país participa de forma ativa nos Digital Decade Country Reports, instrumentos de monitorização que avaliam o progresso dos Estados-membros em domínios como conectividade, competências digitais, digitalização empresarial e serviços públicos digitais. No relatório de 2025, Portugal destacou-se positivamente pela elevada taxa de digitalização da administração pública, mas o documento sublinhou a necessidade de intensificar a qualificação digital da população e o apoio à adoção de tecnologias emergentes (Comissão Europeia, 2025).

Outro vetor importante da participação portuguesa prende-se com a promoção da coerência regulatória europeia. Portugal tem defendido, nos fóruns de coordenação do Conselho da UE, que as políticas digitais devem ser aplicadas de forma uniforme e proporcional, evitando disparidades regulatórias que possam prejudicar a competitividade entre Estados-membros. Essa posição reflete a visão de que a integração digital europeia só é plenamente eficaz quando acompanhada por uma harmonização regulatória coerente e por mecanismos de apoio aos países com menor capacidade institucional.

A abordagem portuguesa às políticas digitais europeias também se distingue pelo seu enfoque humanista. Portugal tem insistido em que a digitalização deve servir o desenvolvimento social, o emprego digno e a literacia tecnológica, colocando as pessoas no centro da transformação digital. Esta perspetiva, inspirada em valores europeus de solidariedade e coesão, tem sido reiterada em declarações conjuntas e iniciativas diplomáticas, nomeadamente na Declaração de Lisboa sobre Democracia Digital, adotada em 2021 durante a Presidência Portuguesa da UE (Governo de Portugal, 2021).

3.5 O Papel de Portugal ao nível interno

O papel de Portugal nas políticas digitais ao nível interno reflete um esforço concertado de modernização estrutural e de adaptação às exigências da economia digital e da sociedade da informação. As transformações que o país tem vindo a realizar inserem-se num quadro político e estratégico que visa reforçar a competitividade, a inclusão social e a eficiência administrativa através da integração de tecnologias digitais nos vários setores da governação, da economia e da vida quotidiana. Esta visão está materializada na Estratégia Digital Nacional (EDN), o principal instrumento orientador da política digital portuguesa, aprovada em 2025 e concebida como o eixo estruturante da transição tecnológica e institucional do país (Governo de Portugal, 2025).

A EDN assenta em sete princípios fundamentais: segurança, sustentabilidade ambiental, ética, inclusão, confiança, eficiência e colaboração, que orientam as políticas públicas e os investimentos no domínio digital. Este enquadramento estratégico estabelece metas mensuráveis, como garantir que 80% da população portuguesa possui competências digitais básicas até 2030, assegurar que 90% das pequenas e médias empresas (PME) atinjam um nível de maturidade digital satisfatório e concretizar a cobertura total de redes 5G em território nacional até ao final da década. Para operacionalizar estas metas, o Governo implementou o Plano de Ação 2026-2027, que estrutura as prioridades e define os mecanismos de execução e monitorização das iniciativas públicas (Governo de Portugal, 2025).

O modelo de governação da política digital portuguesa foi igualmente reforçado, através da criação do Conselho de Ministros para a Transição Digital e Modernização e do Conselho para o Digital na Administração Pública. Estes órgãos asseguram a coordenação interministerial e a coerência na implementação das medidas definidas, evitando sobreposição de competências e promovendo sinergias entre as diferentes entidades da administração central e local (Diário da República, 2024). Esta arquitetura institucional tem permitido ao Estado português consolidar uma governação digital mais integrada, sustentada e adaptável às novas exigências tecnológicas e sociais.

A dimensão humana da transição digital constitui um dos eixos centrais da política interna. A capacitação digital da população é entendida como uma condição indispensável para o sucesso da transformação tecnológica. Portugal enfrenta ainda uma lacuna significativa na qualificação em tecnologias da informação e comunicação, sobretudo entre adultos e grupos populacionais menos escolarizados. Para colmatar essa lacuna, foram desenvolvidos programas de formação e requalificação profissional em competências digitais, com destaque para o INCoDe.2030, que promove o desenvolvimento de literacia digital básica e avançada em todo o território nacional. Paralelamente, políticas educativas e vocacionais têm sido adaptadas para incluir a aprendizagem digital e as competências emergentes em áreas como ciência de dados, cibersegurança e inteligência artificial (Cedefop News, 2025).

A inclusão digital também se tornou um pilar essencial da política pública. A digitalização é concebida não apenas como um motor de eficiência económica, mas como um instrumento de coesão social e territorial. O Plano de Ação para a Transição Digital define medidas de acesso equitativo a equipamentos, conectividade e serviços digitais, com especial atenção às populações em situação de vulnerabilidade social e às zonas rurais. O objetivo é garantir que todos os cidadãos, independentemente da idade, localização ou condição económica, possam beneficiar das oportunidades oferecidas pela transformação digital (*Digital Skills and Jobs Platform*, 2025). Estas políticas refletem uma visão inclusiva, em que o desenvolvimento tecnológico é colocado ao serviço da cidadania e da igualdade de oportunidades.

No domínio económico, a digitalização tem sido vista como um vetor de crescimento e inovação. As PME representam mais de 99% do tecido empresarial português e são, por isso, um foco prioritário da política digital. O Governo lançou programas como o Vale Indústria 4.0 e o Comércio Digital, destinados a apoiar as empresas na adoção de tecnologias emergentes e na integração de processos automatizados. Estas iniciativas procuram modernizar os modelos de negócio e aumentar a produtividade, promovendo a digitalização como um fator de competitividade. Paralelamente, a Estratégia Nacional para a Inteligência Artificial, AI Portugal 2030, reforça o compromisso com a utilização ética e responsável da IA, incentivando a inovação em setores estratégicos como energia, saúde e mobilidade (Boletim da OA, 2025).

A economia digital portuguesa tem beneficiado de um ambiente favorável ao empreendedorismo e à inovação, com o surgimento de ecossistemas tecnológicos e centros de incubação que ligam empresas, universidades e entidades públicas. A criação de polos tecnológicos e a atração de investimento estrangeiro direto reforçam o posicionamento de Portugal como um centro de referência na economia digital europeia. De acordo com relatórios internacionais, o país tem vindo a consolidar uma reputação de inovação, impulsionada pela qualidade da infraestrutura digital, pela estabilidade institucional e pela adoção de políticas favoráveis à inovação (OCDE, 2025).

A digitalização da administração pública representa uma das dimensões mais visíveis da política interna. A integração progressiva de serviços eletrónicos e a interoperabilidade dos sistemas públicos têm transformado a relação entre o Estado, os cidadãos e as empresas. O portal ePortugal, a Chave Móvel Digital e o cartão de cidadão eletrónico são exemplos de ferramentas que simplificam o acesso a serviços e reduzem os encargos administrativos. Estas medidas têm contribuído para aumentar a eficiência, a transparência e a confiança nas instituições públicas. A modernização administrativa, contudo, não se resume à informatização de processos; implica uma mudança cultural profunda, que valoriza a inovação, a formação e a colaboração entre organismos públicos (Governo de Portugal, 2025).

No entanto, o aumento da digitalização também trouxe desafios acrescidos em matéria de cibersegurança. O ataque cibernético de 15 e 16 de outubro de 2024, que afetou múltiplas plataformas estatais, incluindo o portal Gov.pt e os sistemas de autenticação digital, demonstrou a vulnerabilidade das infraestruturas públicas. Este ataque, que utilizou técnicas de *ransomware*, provocou a interrupção temporária de serviços críticos e expôs a necessidade de reforçar a resiliência do sistema digital nacional. A resposta articulada entre a Agência para a Modernização Administrativa, o Centro Nacional de Cibersegurança e o Governo revelou a capacidade de gestão de crises, mas também sublinhou a urgência de investir em medidas preventivas e de proteção avançada (RTP, 2024; SAPO TEK, 2024; TVI, 2024; The Portugal News, 2024).

Na sequência deste episódio, o Governo atualizou a Estratégia Nacional de Cibersegurança 2024–2030, reforçando os mecanismos de defesa e a cooperação institucional. O novo enquadramento legal e operacional introduziu medidas como a criação de equipas especializadas de resposta rápida, a realização de auditorias regulares e a formação avançada em segurança digital. Além disso, o Estado português intensificou a colaboração com entidades europeias e internacionais, reconhecendo que a cibersegurança é um domínio de responsabilidade partilhada e interdependente (Centro Nacional de Cibersegurança, 2024).

A dimensão participativa da política digital portuguesa também tem merecido destaque. O país tem promovido a democracia digital através de iniciativas que aproximam os cidadãos dos processos de decisão pública. A plataforma *Participa.gov.pt* constitui um instrumento central desta estratégia, permitindo que os cidadãos contribuam ativamente em consultas públicas e apresentem propostas de políticas. Esta abordagem, sustentada por princípios de transparência e colaboração, reforça a legitimidade das decisões públicas e incentiva o envolvimento cívico (*Open Government Partnership*, 2025).

O financiamento europeu tem desempenhado um papel determinante na concretização da política digital nacional. O Plano de Recuperação e Resiliência destinou mais de dois mil milhões de euros à transição digital, canalizados para projetos de modernização administrativa, reforço da conectividade e qualificação digital. Estas verbas têm sido complementadas pelos fundos do programa Portugal 2030, que estabelecem metas de longo prazo para a inovação, a capacitação e a sustentabilidade tecnológica (Portugal 2030, 2025). A utilização eficiente destes recursos tem permitido acelerar reformas estruturais e promover uma digitalização inclusiva e equilibrada.

A sustentabilidade ambiental é outro pilar relevante da estratégia portuguesa. A EDN incorpora o princípio da dupla transição, digital e verde, promovendo o uso de tecnologias que reduzam a pegada ecológica e aumentem a eficiência energética. A aposta em *data centers* alimentados por energia renovável, a desmaterialização de processos administrativos e a integração de soluções de economia circular no setor tecnológico refletem a preocupação do país com um modelo de desenvolvimento sustentável (Governo de Portugal, 2025).

Apesar dos progressos, Portugal ainda enfrenta desafios significativos. A escassez de profissionais altamente qualificados em áreas tecnológicas, a necessidade de reforçar a interoperabilidade entre sistemas públicos e a resistência cultural à inovação continuam a ser obstáculos à plena maturidade digital. A consolidação da transformação digital exigirá, por isso, uma continuidade política consistente, um investimento público sustentado e uma permanente adaptação às novas dinâmicas tecnológicas e regulatórias (OCDE, 2025).

Portugal apresenta, contudo, uma trajetória sólida e coerente na construção de uma sociedade digital. O país conseguiu transformar a tecnologia num instrumento de inclusão, eficiência e desenvolvimento sustentável. A Estratégia Digital Nacional e os planos subsequentes demonstram que a transição digital portuguesa é um projeto de longo prazo, que combina visão estratégica, planeamento técnico e compromisso político. A política digital interna portuguesa assenta numa conceção equilibrada entre inovação, segurança, ética e cidadania, projetando o país como uma referência europeia na concretização de uma transformação digital ao serviço das pessoas e do bem público.

Conclusão

O presente capítulo sintetiza e interpreta os principais resultados obtidos na investigação, reafirmando o argumento central que orientou o estudo, a soberania digital, no contexto europeu, não corresponde a uma autonomia absoluta dos Estados, mas a uma forma partilhada, relacional e multinível de exercício de autoridade política. A análise teórica e empírica confirmou que o digital se tornou um dos principais domínios de poder no século XXI e que, no seio da UE, essa autoridade é exercida através de processos de coordenação, delegação e interdependência institucional entre os Estados-Membros e as estruturas supranacionais. O estudo demonstrou que a soberania digital é hoje exercida de forma distribuída, refletindo uma lógica de poder cooperativo e não competitivo. No caso português, esta realidade é particularmente evidente, a capacidade de decisão, implementação e defesa no domínio digital é exercida simultaneamente a níveis nacional, europeu e internacional, ilustrando o modelo conceptual desenvolvido nesta dissertação, o de soberania digital partilhada. Este modelo traduz a ideia de que a autoridade política e regulatória sobre o digital não se concentra num único centro de poder, mas se materializa através da interação estratégica entre instituições nacionais e europeias, numa relação de complementaridade, coautoria normativa e interdependência funcional.

Os resultados confirmaram que o digital constitui um domínio de soberania estruturalmente partilhada, caracterizado por uma interdependência funcional profunda entre a UE e os Estados-Membros. O sistema europeu de governação digital combina uma capacidade normativa supranacional robusta com execução descentralizada e contextualizada a nível nacional, configurando um modelo de soberania distribuída que rompe definitivamente com o paradigma vestefaliano clássico de autoridade política territorialmente delimitada e exclusiva. A natureza intrinsecamente transnacional das redes digitais, a circulação global e instantânea de dados, a desterritorialização dos fluxos informacionais e a dependência crítica de infraestruturas tecnológicas controladas por entidades privadas multinacionais tornam inviável, tanto técnica como politicamente, o exercício isolado, unilateral e autossuficiente da autoridade estatal sobre o domínio digital. O digital impõe, assim, uma forma de soberania em rede, sustentada em mecanismos de cooperação institucional, partilha regulatória, delegação de competências e coordenação estratégica.

No caso português, esta soberania partilhada manifesta-se de forma concreta através da integração normativa, regulatória, operacional e estratégica na arquitetura institucional da UE. As políticas nacionais estruturantes, como o PATD, a EDN, o PRR, a estratégia AI Portugal 2030 e a Estratégia Nacional de Segurança do Ciberespaço, encontram-se alinhadas com os instrumentos, metas e calendários definidos pela Bússola Digital 2030 e pela Década Digital europeia. A aplicação direta e a transposição sistemática de regulamentos estruturantes como o RGPD, a NIS2, o DSA, o DMA e o *AI Act* demonstram a transferência significativa de competências decisórias, normativas e técnicas para o nível europeu. Portugal atua como parte integrante de uma rede regulatória multinível, onde a autoridade sobre o digital é exercida de forma cooperativa, coordenada e interdependente, e não de forma isolada ou plenamente autónoma.

A investigação confirmou igualmente que o digital se encontra num processo acelerado de supranacionalização normativa, ainda que mantenha componentes operacionais e securitárias de natureza intergovernamental. A UE consolidou-se como um centro global de formulação política e produção regulatória em matéria digital, dotando-se de instrumentos legislativos de aplicação direta que conferem poderes vinculativos de regulação, supervisão e sanção. Este processo não resulta de imposição unilateral, mas de decisões políticas coletivas dos Estados-Membros, que optaram conscientemente por delegar competências em áreas onde a ação isolada se revelou insuficiente. A regulação das grandes plataformas digitais, a proteção transnacional de dados, a cibersegurança de infraestruturas críticas interconectadas e a governação da IA são domínios onde a escala europeia oferece vantagens evidentes de eficácia, coerência e poder de influência global.

Apesar disso, os Estados-Membros mantêm um papel essencial na execução prática e contextualizada das normas europeias e na proteção das suas infraestruturas críticas nacionais. Em Portugal, entidades como o CNCS, a AMA, a ANACOM, a Secretaria de Estado da Digitalização e a CNPD desempenham funções determinantes na aplicação territorial, fiscalização e adaptação das políticas europeias. Este equilíbrio institucional demonstra que a soberania digital não desaparece a nível nacional, mas transforma-se numa lógica de governação híbrida e multinível, em que a UE define o enquadramento normativo geral e os Estados asseguram a operacionalização concreta e a resposta a ameaças territorializadas.

A escolha estratégica portuguesa de governar o digital no quadro europeu não resulta de perda involuntária de soberania, mas de uma estratégia deliberada de amplificação da autonomia nacional num contexto global profundamente assimétrico. Nenhum Estado europeu de dimensão pequena ou média possui, de forma isolada, escala tecnológica, capacidade industrial ou poder geopolítico suficientes para enfrentar as dinâmicas globais do digital dominadas por grandes potências tecnológicas. A integração europeia surge, assim, como uma resposta racional que permite reforçar a capacidade coletiva de regulação, investimento, negociação internacional e projeção normativa. A UE funciona como um multiplicador de soberania, permitindo que Estados como Portugal reforcem a sua autonomia decisória e relevância estratégica através da ação coletiva.

Os resultados empíricos mostram que Portugal utiliza a sua pertença à UE como instrumento de projeção soberana, participando ativamente em programas e consórcios europeus como o Gaia-X, o *Horizon Europe*, o CEF Digital, os EDIH e os IPCEI. Estes mecanismos compensam limitações estruturais nacionais em termos de financiamento, tecnologia, talento e escala, reforçando simultaneamente a resiliência coletiva europeia. A soberania portuguesa assume, assim, uma natureza funcional e relacional, dependente da integração europeia em termos operacionais, mas simultaneamente fortalecida por essa mesma integração.

A investigação identificou ainda a dependência tecnológica externa como o principal constrangimento estrutural à consolidação de uma soberania digital mais autónoma e resiliente. Portugal permanece fortemente dependente de infraestruturas, plataformas, serviços de *cloud*, sistemas operativos e equipamentos de rede controlados por fornecedores estrangeiros. Uma parte significativa dos dados nacionais encontra-se armazenada fora do território europeu, ficando potencialmente sujeita a jurisdições externas, o que cria vulnerabilidades técnicas, jurídicas e geopolíticas. Esta dependência limita a autonomia estratégica do Estado, expõe infraestruturas críticas a riscos e condiciona a capacidade de inovação endógena.

Apesar disso, a integração europeia tem permitido mitigar parcialmente estas fragilidades através de políticas comuns orientadas para a recuperação de autonomia tecnológica coletiva, como o *European Chips Act*, o Gaia-X e o reforço do quadro europeu de cibersegurança. Portugal participa nestas iniciativas através de universidades, centros de investigação e empresas

tecnológicas nacionais, reforçando a sua capacidade de proteção digital e influência normativa por via da cooperação supranacional.

A análise global permite validar o argumento central desta dissertação, a soberania digital portuguesa é fundamentalmente relacional, partilhada e multinível, refletindo uma interdependência estrutural entre o nível nacional e o nível europeu que é funcionalmente necessária e politicamente escolhida. Longe de representar uma perda de soberania, esta configuração institucional traduz uma forma de soberania cooperativa e adaptativa que reforça a capacidade de decisão, regulação, proteção e influência internacional do Estado português. A soberania digital não se mede pela capacidade ilusória de isolamento tecnológico ou autossuficiência técnica, mas pela capacidade efetiva de influenciar normas, participar em decisões estratégicas, proteger direitos fundamentais e adaptar-se a contextos tecnológicos em rápida transformação.

No plano teórico, o principal contributo deste trabalho reside na consolidação do conceito de soberania digital partilhada como uma modalidade contemporânea de exercício de autoridade política baseada na coordenação institucional entre múltiplos níveis de governação e na interdependência regulada entre Estados e instituições supranacionais. Esta abordagem afasta-se da conceção clássica e exclusiva de soberania e propõe uma leitura centrada na capacidade de influência, participação decisória e ação cooperativa em contextos de interdependência estrutural. A soberania digital partilhada assenta na distribuição vertical de competências, na cooperação horizontal entre Estados-Membros, na delegação condicional de autoridade e numa interdependência funcional que torna a ação isolada tecnicamente inviável e politicamente ineficaz.

Reconhecem-se limitações teóricas e metodológicas que condicionaram o alcance da investigação, nomeadamente a fluidez conceptual do próprio conceito de soberania digital, a escassez de dados públicos detalhados sobre infraestruturas críticas e fluxos de dados, a ausência de comparação sistemática com outros Estados-Membros e a limitada produção académica portuguesa sobre o tema. Estas limitações não invalidam os resultados alcançados, mas antes reforçam a relevância do enquadramento proposto e apontam para a necessidade de investigações futuras de carácter comparativo, empírico e interdisciplinar.

Em síntese, a investigação confirmou que a soberania digital portuguesa se exerce através da interdependência institucionalizada e que essa interdependência constitui a principal fonte da sua eficácia operacional, resiliência e relevância estratégica. No século XXI, a soberania no domínio tecnológico não se constrói através do isolamento, mas através da coordenação estratégica, da influência normativa e da participação ativa em estruturas multilaterais. Portugal demonstra que a autonomia digital não se afirma contra a integração europeia, mas através dela, utilizando a partilha institucionalizada de poder como instrumento de reforço da soberania nacional. A soberania digital portuguesa não reside na impossível autossuficiência tecnológica, mas na capacidade de influenciar as regras do jogo europeu e global, proteger os direitos dos cidadãos, participar na definição de standards internacionais e adaptar-se continuamente às transformações tecnológicas, trata-se de uma soberania exercida em rede, partilhada institucionalmente, mas por isso mesmo mais robusta, eficaz e politicamente relevante no contexto do século XXI.

Referências Bibliográficas

Agnew, J. A. (2005). *Sovereignty regimes: Territoriality and state authority in contemporary world politics*. *Annals of the Association of American Geographers*, 95(2), 437–461. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1111/j.1467-8306.2005.00468.x>

Agência para a Modernização Administrativa. (2023). *Relatório de atividades e balanço da transição digital*. Consultado a 18/01/2026. Disponível em: <https://www.ama.gov.pt>

ANACOM. (2024). *The Communications Sector 2024*. Consultado a 18/01/2026. Disponível em: <https://www.anacom.pt/render.jsp?contentId=1811323&languageId=1>

ANACOM. (2025). *5G stations grow by 24% in the 4th quarter of 2024*. Consultado a 18/01/2026. Disponível em: <https://www.anacom.pt/render.jsp?contentId=1803714&languageId=1>

Aueamnuay, C., Berjón, C., Galehr, S., Graf, L., & Heinemann, A. (2024). *Digital regulation in the European Union*. *EuZ – Zeitschrift für Europarecht*. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.36862/eiz-euz2024-03>

Autolitano, S., & Pawlowska, A. (2021). *Europe's quest for digital sovereignty: GALA-X as a case study*. *Istituto Affari Internazionali*. Consultado a 18/01/2026. Disponível em: <https://www.iai.it/sites/default/files/iaip2114.pdf> cita em texto

Bellanova, R., Carrapico, H., & Duez, D. (2022). *Digital/sovereignty and European security integration: an introduction*. *European Security*, 31(3), 337–355. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/09662839.2022.2101887>

Barrinha, A., & Christou, G. (2022). *Speaking sovereignty: the EU in the cyber domain*. *European Security*, 31(3), 356–376. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/09662839.2022.2102895>

Blancato, F. G. (2023). *The cloud sovereignty nexus: How the European Union integrates cloud and data sovereignty in policy*. *Policy & Internet*, 15(4), 1–20. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1002/poi3.358>

Boletim da OA. (2025, 10 de dezembro). *Governo põe Estratégia Digital e Agenda para a Inteligência Artificial em marcha*. Consultado a 18/01/2026. Disponível em: <https://boletim.oa.pt/2025/12/10/governo-poe-estrategia-digital-e-agenda-para-a-inteligencia-artificial-em-marcha>

Bratton, B. H. (2015). *The Stack: On software and sovereignty*. MIT Press.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1093/oso/9780190088583.001.0001>

Brigola, F. (2025, October 27). *A IA generativa impulsiona uma administração pública mais eficiente e produtiva*. Google. Disponível em: <https://blog.google/intl/pt-pt/noticias-da-empresa/a-ia-generativa-impulsiona-uma-administracao-publica-mais-eficiente-e-produtiva>

Broeders, D., Cristiano, F., & Kaminska, M. (2023). *In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions*. *Journal of Common Market Studies*. Consultado a 18/01/2026. Disponível em: https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/jcms.13462?utm_source=consensus

Calzada, I. (2019). *Technological sovereignty: Protecting citizens' digital rights in the AI-driven and post-GDPR algorithmic and city-regional European realm*. *Regions*. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/13673882.2018.00001038>

Caporaso, J. A. (2000). *Changes in the Westphalian order: Territory, public authority, and sovereignty*. *International Studies Review*. Consultado a 18/01/2026. Disponível em: <https://scispace.com/pdf/changes-in-the-westphalian-order-territory-public-authority-4doa6hxffi.pdf>

Carrapico, H. & Farrand, B. (2025). *EU data sovereignty: An autonomy–interdependence perspective*. *Politics and Governance*, 13(2). Consultado a 18/01/2026. Disponível em: <https://www.cogitatiopress.com/politicsandgovernance/article/viewFile/10331/4478>

Carvalho, A. S., & Restier Poças, I. (2020). *Big data e o Regulamento Geral de Proteção de Dados da União Europeia*. *Revista Ibérica do Direito*, 1(2). Consultado a 18/01/2026. Disponível em: <https://www.revistaibericadodireito.pt/index.php/capa/article/download/13/15/49>

Castells, M. (2009). *Communication power*. Oxford University Press. Consultado a 18/01/2026. Disponível em: <https://maestriacomunicacionibero.files.wordpress.com/2014/03/castells-power-in-the-network-society.pdf>

CaixaBank Research. (2022). *Portugal: can it pick up the pace in the digital race?*. Consultado a 18/01/2026. Disponível em: <https://www.caixabankresearch.com/en/economics-markets/activity-growth/portugal-can-it-pick-pace-digital-race>

Cedefop News. (2025). *Portugal among top 10 digitally advanced nations in EU by 2030*. Consultado a 18/01/2026. Disponível em: <https://www.cedefop.europa.eu/en/news/portugal-among-top-10-digitally-advanced-nations-eu-2030>

Centro Nacional de Cibersegurança. (2024). *Estratégia Nacional de Cibersegurança 2024–2030*. Consultado a 18/01/2026. Disponível em: <https://www.cncs.gov.pt/content/files/estrategia-nacional-ciberseguranca-2024-2030.pdf>

Chousou, S., Magaud, J., Pavoni, L., & Williams, M. (2023). *Is encryption a fundamental right? A case study on CSAM regulation in the EU*. In Professor Florence G'sell, *Comparative Approaches to Big Tech Regulation*. Consultado a 18/01/2026. Disponível em: <https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/07/Encryption.pdf>

Christakis, T. (2020). *European digital sovereignty: Rethinking the EU's external cyber policy*. SSRN. Consultado a 18/01/2026. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*.

Conselho Europeu. (2020). *Conclusões do Conselho Europeu – outubro de 2020*. Consultado a 18/01/2026. Disponível em: <https://www.consilium.europa.eu/en/press/press-releases/>

Comissão Europeia. (2020). *Uma nova estratégia industrial para a Europa*. Consultado a 18/01/2026. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0102>

Comissão Europeia. (2021). *Bússola Digital 2030: O caminho europeu para a Década Digital*. Consultado a 18/01/2026. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52021DC0118>

Comissão Europeia. (2022). *Declaração Europeia sobre os Direitos e Princípios Digitais*. Consultado a 18/01/2026. Disponível em: https://direito.up.pt/digeucit/wp-content/uploads/sites/968/2022/12/Declaracao-Europeia-sobre-os-direitos-e-principios-para-a-decada-digital_PT.pdf

Comissão Europeia. (2022). *Digital Economy and Society Index (DESI) 2022 - Portugal*. Consultado a 18/01/2026. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/desi-portugal>

Comissão Europeia. (2023). *Digital Decade Country Report 2023*. Consultado a 26/01/2026. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/digital-decade-country-reports>

Comissão Europeia. (2024). *Relatório por País sobre a Década Digital de Portugal 2024*. Consultado a 26/01/2026. Disponível em: <https://digital-strategy.ec.europa.eu/en/policies/digital-decade-country-reports>

Correio da Manhã. (2024). *Ataque informático apaga serviços online do Estado*. Consultado a 18/01/2026. Disponível em: <https://www.cmjornal.pt/politica/detalhe/ataque-informatico-apaga-servicos-online-do-estado>

de Carvalho, R. M., Del Prete, C., Martín, Y., Araujo Rivero, R. M., Önen, M., Schiavo, F. P., Cuevas Rumín, Á., Mouratidis, H., Yelmo, J., & Koukovini, M. N. (2020). *Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects*. *SN Computer Science*, 1(4), Article 218. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1007/s42979-020-00218-8>

DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.

Diário de Notícias. (2023, 12 novembro). *América contra investimentos chineses em setores críticos da economia.* Consultado a 18/01/2026. Disponível em: <https://www.dn.pt/internacional/america-contra-investimentos-chineses-em-setores-criticos-da-economia>

Diário da República. (2024). *Resolução do Conselho de Ministros n.º 207/2024: Modelos de governação da Estratégia Digital Nacional.* Consultado a 18/01/2026. Disponível em: <https://files.diariodarepublica.pt/1s/2024/12/25200/0003700073.pdf>

Digital Skills and Jobs Platform. (2025). *Portugal – Action Plan for the Digital Transition.* Consultado a 18/01/2026. Disponível em: <https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/portugal-action-plan-digital-transition>

Eshbaev, G. (2024). *GDPR vs. weakly protected parties in other countries.* *Uzbek Journal of Law and Digital Policy.* Consultado a 18/01/2026. Disponível em: <https://doi.org/10.59022/ujldp.254>

ENISA. (2024). *NIS2 Directive Overview.* Consultado a 18/01/2026. Disponível em: <https://www.enisa.europa.eu/topics/nis-directive>

Estratégia Digital Nacional (Portugal) – documento oficial que define princípios para soberania tecnológica e modernização digital. Consultado a 26/01/2026. Disponível em: <https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3DBQAAAB%2BLCAAAAAAABAAzNDExMQIA5ua1dQUAAAA%3D>

European Data Protection Board (EDPB). (2019). *Guidelines 2/2019 on the CLOUD Act and international data transfers.* Brussels: EDPB Secretariat. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/topic/restrictions_en

European Parliamentary Research Service. (2020). *Digital sovereignty for Europe (EPRS_BRI (2020)651992).* Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI%282020%29651992_EN.pdf?

Expresso. (2024, 8 outubro). *Portugal vai falhar prazo da diretiva europeia da segurança da informação. Lei está prevista para meados de 2025.* Consultado a 18/01/2026. Disponível em: <https://expresso.pt/sociedade/tecnologia/2024-10-08-portugal-vai-falhar-prazo-da-diretiva-europeia-da-seguranca-da-informacao-lei-esta-prevista-para-meados-de-2025-74999ae5>

Ezine Eversheds-Sutherland. (2025). *EU NIS2 Directive - Portugal.* Consultado a 18/01/2026. Disponível em: <https://ezine.eversheds-sutherland.com/eu-nis2-directive/portugal>

Farrand, B., Carrapico, H., & Turobov, A. (2024). *The new geopolitics of EU cybersecurity: Security, economy and sovereignty. International Affairs.* Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1093/ia/iaae231>

Floridi, L. (2020). *The fight for digital sovereignty: what it is, and why it matters, especially for the EU. Philosophy & Technology, 33(3), 369–378.* Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1007/s13347-020-00401-8>

Gabinete de Estratégia e Estudos (GEE). (2025). *TE 100 – Soberania Digital.* Consultado a 18/01/2026. Disponível em: <https://www.gee.gov.pt/fileman/Uploads/TE%20100%20-%20Soberania%20Digital.pdf>

Gentile, G., & Lynskey, O. (2022). *Deficient by design? The transnational enforcement of the GDPR. International and Comparative Law Quarterly, 71(4), 799–830.* Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1017/S0020589322000355>

Gomes, S. M. P. J. (2024). *EU personal data protection standards beyond its borders: External governance and GDPR influence* (Master's thesis). ISCTE. Consultado a 18/01/2026. Disponível em: https://repositorio.iscte-iul.pt/bitstream/10071/32736/1/master_sofia_jesus_gomes.pdf

Governo de Portugal. (2020). *Plano de Ação para a Transição Digital.* Consultado a 18/01/2026. Disponível em: <https://www.portugal.gov.pt/gc22/portugal-digital/plano-de-acao-para-a-transicao-digital-pdf.aspx>

Governo de Portugal. (2021). *Declaração de Lisboa sobre Democracia Digital.* Recuperado de Consultado a 18/01/2026. Disponível em: <https://digital.gov.pt/documentos/declaracao-de-lisboa>

Governo de Portugal. (2024, 28 maio). *Portugal's ambition is to be considered a true digital nation.* Consultado a 18/01/2026. Disponível em: <https://www.portugal.gov.pt/en/gc23/communication/news-item?i=portugals-ambition-is-to-be-considered-a-true-digital-nation>

Governo de Portugal. (2025). *Implementação do DSA em Portugal.* Consultado a 18/01/2026. Disponível em: https://www.plmj.com/xms/files/TMT_Digital_Services_Act_From_European_regulation_to_implementation_in_Portugal.pdf

Governo de Portugal. (2025). *Estratégia Digital Nacional – Plano de Ação 2026-2027.* Consultado a 18/01/2026. Disponível em: <https://www.portugal.gov.pt/pt/gc25/comunicacao/comunicado?i=estrategia-digital-nacional-plano-de-acao-2026-2027>

Gur, B. (2022). *Cybersecurity, European digital sovereignty and the 5G rollout crisis.* *Computer Law & Security Review*, 46, 105736. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1016/j.clsr.2022.105736>

Held, D., & McGrew, A. (2007). *Globalization theory: Approaches and controversies.* Polity Press.

Hermenegildo, R. S., & Cunha, A. (2021). *Portugal and the 2021 Council Presidency: An Unambitious Programme?* *TEPSA Briefs.* Consultado a 18/01/2026. Disponível em: https://www.tepsa.eu/wp-content/uploads/2023/11/TEPSA-Brief-HermenegoldiCunha_FINAL.pdf

Herian, R. (2020). *Blockchain, GDPR, and fantasies of data sovereignty.* *Law, Innovation and Technology*, 12(2), 156–174. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/17579961.2020.1727094>

Ilves, L. K., Evans, T., Cilluffo, F. J., & Nadeau, A. A. (2016). *European Union and NATO global cybersecurity challenges: A way forward.* *Prism*, 6(2), 126–137. Disponível em: www.jstor.org/stable/26470452?

- INCoDe.2030.** (2023). *Estratégia Nacional de Inteligência Artificial – AI Portugal 2030*. Consultado a 18/01/2026. Disponível em: https://incode2030.gov.pt/wp-content/uploads/2023/07/Estrategia-de-Inteligencia-artificial.aspx_.pdf
- Interoperable Europe.** (2025). *Governance Portugal*. Comissão Europeia. *Politics and Governance*. Consultado a 26/01/2026. Disponível em: <https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/governance-portugal>
- Joswig, T., & Kurz, W.** (2025). *Regulatory and compliance requirements for SMEs operating AI systems through data centers in the EU, with a focus on data protection challenges in Germany*. *Journal of Next-Generation Research* 5.0. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.70792/jngr5.0.v1i2.89>
- Kaya, M., & Shahid, H.** (2025). *Cross-border data flows and digital sovereignty: Legal dilemmas in transnational governance*. *Interdisciplinary Studies in Society, Law, and Politics*, 4(2), 219–233. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.61838/kman.isslp.4.2.20>
- Krasner, S. D.** (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.
- Lake, D. A.** (2010). *Hierarchy in international relations*. Cornell University Press. Disponível em: <https://www.cornellpress.cornell.edu/book/9780801447352/hierarchy-in-international-relations/>
- Lisboa inteligente.** (n.d.). *LISBOA ABERTA*. Disponível em: <https://lisboaaberta.cm-lisboa.pt/index.php/pt/lisboa-inteligente?>
- Lynskey, O.** (2015). *The foundations of EU data protection law*. Oxford University Press.
- Manners, I.** (2002). *Normative power Europe: A contradiction in terms?* *Journal of Common Market Studies*, 40(2), 235–258. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1111/1468-5965.00353>
- Marelli, L., Lievevrouw, E., & van Hoyweghen, I.** (2020). *Fit for purpose? The GDPR and the governance of European digital health*. *Policy Studies*, 41(5), 447–467. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/01442872.2020.1724929>

- Martins, T. J. C. (2021).** *A Política Digital Europeia e Portugal: O legado da IV Presidência Portuguesa do Conselho da União Europeia* [Relatório de Estágio, Universidade Nova de Lisboa]. Repositório RUN. Consultado a 18/01/2026. Disponível em: <https://run.unl.pt/entities/publication/6fde1317-8dd3-4bcf-bf24-d7ed5bc0ee4d>
- Mayer, M., & Lu, X. (2023).** *Digital Autonomy? Measuring the Global Digital Dependence Structure*. SSRN Electronic Journal. Consultado a 18/01/2026. Disponível em: <https://ssrn.com/abstract=4404826>
- Metakides, G. (2021).** *A crucial decade for European digital sovereignty*. In *Digital Sovereignty in Europe* (pp. 219–225). Springer. Consultado a 18/01/2026. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-86144-5_29
- Moravcsik, A. (1998).** *The choice for Europe: Social purpose and state power from Messina to Maastricht*.
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2024).** *Locked Shields – The world’s largest and most complex international live-fire cyber defence exercise*. Tallinn: NATO CCDCOE. Consultado a 18/01/2026. Disponível em: <https://ccdcOE.org/exercises/locked-shields/>
- Nye, J. S. (2011).** *The future of power*. PublicAffairs.
- Observatório dos Ecossistemas e Infraestruturas Digitais. (2025).** *25 medidas estratégicas para a criação da cloud soberana em Portugal* (v. final). Consultado em 26/01/2026, disponível em <https://oeid.pt/wp-content/uploads/2025/08/25-Medidas-Estrategicas-CloudSoberana-vfinal.pdf>
- OCDE – Organização para a Cooperação e Desenvolvimento Económico. (2021).** *Digital sovereignty and economic resilience: Policy perspectives*. Consultado a 18/01/2026. Disponível em: <https://www.oecd.org/digital/>

OCDE. (2025). *Using digital technology to strengthen oversight of public procurement in Portugal*. Consultado a 18/01/2026. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/using-digital-technology-to-strengthen-oversight-of-public-procurement-in-portugal_67a76e1e/43add03b-en.pdf

O'Hara, K., & Hall, W. (2018). *Four Internets: The geopolitics of digital governance*. CIGI. Consultado a 18/01/2026. Disponível em: <https://www.cigionline.org/static/documents/documents/Paper%20no.206web.pdf>

Op 't Hoog, G., De Swart, L., Essink, J., Van Der Born, G., Ritmeester, Y., Sekula, A., Smit, G., Vavoula, N., Karapatakis, A., Ecorys, Queen Mary University London, Mifsud-Bonnici, J., Preneel, B., & Mitsilegas, V. (2023). *Proposal for a regulation laying down the rules to prevent and combat child sexual abuse*. In K. Eisele & H. Dalli, *EPRS | European Parliamentary Research Service [Report]*. EPRS | European Parliamentary Research Service. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.2861/016876>

Open Government Partnership. (2025). *Portugal expand digital public participation*. Consultado a 18/01/2026. Disponível em: <https://www.opengovpartnership.org/the-open-gov-challenge/portugal-expand-digital-public-participation>

Osório, S. G. (2023). *Impacto do RGPD no ordenamento jurídico português*. Universidade de Lisboa. Consultado a 18/01/2026. Disponível em: https://repositorio.ulisboa.pt/bitstream/10451/61501/1/ulflpgsosorio_tm.pdf

Pierucci, F. (2025). *Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace*. *Digital Society*, 4(1), Article 27. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1007/s44206-025-00189-4>

Pinto Arena, M. do C. (2022). *Portugal's challenging relationship with China under tense US/EU-China relations*. *The International Spectator*, 57(4), 68–85. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/03932729.2022.2064059>

Portugal 2030. (2025). *Estratégia Portugal 2030*. Consultado a 18/01/2026. Disponível em: <https://portugal2030.pt/en/portugal-2030/o-que-e-o-portugal-2030>

Portugal Business News. (2025). *Top 100 Unicorns in Europe in 2025*. Consultado a 18/01/2026. Disponível em: <https://www.portugalbusinessesnews.com/post/top-100-unicorns-in-europe-in-2025>

Portugal Digital. (2025). *Estratégia Digital Nacional – O digital simplifica*. Consultado a 18/01/2026. Disponível em: <https://digital.gov.pt/documentos/portugal-digital-strategy>

Portugal Resident. (2024, outubro 16). *Ransomware attack targets Agency for Administrative Modernisation*. Consultado a 18/01/2026. Disponível em: <https://www.portugalresident.com/ransomware-attack-targets-agency-for-administrative-modernisation/>

Raimundo, A., & Ferreira-Pereira, L. C. (2022). *Portugal's strategic response to Brexit: Enduring Europeanisation? Journal of Contemporary European Studies*. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/14782804.2022.2106953>

Relatório Nacional de Inovação. (2022). *Fundação para a Ciência e a Tecnologia*. Consultado a 26/01/2026. Disponível em: <https://www.fct.pt/wp-content/uploads/2024/11/RelatorioNacionalInovacao22.pdf>

Reuters. (2025, 7 de maio). *EU sues several countries for not properly implementing Digital Services Act*. Consultado a 18/01/2026. Disponível em: <https://www.reuters.com/technology/eu-sues-several-countries-not-properly-implementing-digital-services-act-2025-05-07>

Resolução do Conselho de Ministros n.º 32/2023. *Diário da República*. Consultado a 18/01/2026. Disponível em: <https://diariodarepublica.pt/>

Romanova, T. (2021). *The EU's discourse on sovereignty: content and implications. European Politics and Society*. Consultado a 29/01/2026. Disponível em: https://www.researchgate.net/publication/356850762_The_EU%27s_Discourse_on_Sovereignty_Content_and_Consequences

Rone, J. (2024). *'The Sovereign Cloud' in Europe: Diverging nation-state preferences and disputed institutional competences in the context of limited technological capabilities. Journal of European Public Policy*, 31(8), 2343–2369. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1080/13501763.2023.2269127>

Rossi, A., & Ducato, R. (2022). *Client-side scanning and EU fundamental rights: Legal tensions in the CSAM proposal*. SSRN. Consultado a 18/01/2026. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4154730

RTP. (2024, 16 de outubro). *Ataque informático: várias plataformas do Estado estão inoperacionais*. Consultado a 18/01/2026. Disponível em: https://www.rtp.pt/noticias/pais/ataque-informatico-varias-plataformas-do-estado-estao-inoperacionais_v1608123

Ruohonen, J. (2021). *The treachery of images in the digital sovereignty debate*. *Minds and Machines*, 31(3), 439–456. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1007/s11023-021-09566-7>

SAPO TEK. (2024, 16 de outubro). *Ataque informático confirmado: plataformas da AMA e serviços digitais afetados*. Consultado a 18/01/2026. Disponível em: <https://tek.sapo.pt/noticias/computadores/artigos/ataque-informatico-confirmado-plataforma-de-autenticacao-do-estado-e-servicos-da-rede-ama-afetados>

Shared Services of the Portuguese Ministry of Health (SPMS). (2020). *Data Strategy for Next Generation Portuguese National Health Service*. Consultado a 26/01/2026. Disponível em: https://www.spms.min-saude.pt/wp-content/uploads/2020/07/Data-Strategy_VERSAOFINAL_07.01.2020.pdf

Sirur, S., Nurse, J. R. C., & Webb, H. (2018). *Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)*. In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS)* (pp. 88–95). ACM. Consultado a 18/01/2026. Disponível em: <https://doi.org/10.1145/3267357.3267368>

Smart Cities | Portugal makes sense. (n.d.). *Portugal Makes Sense*. Disponível em: <https://portugalmakesense.portugalgloba.pt/en/campaigns/smart-cities/>

Synergy Research Group. (2024). *Cloud Market Reaches \$270 Billion in 2024; US Providers Maintain Over 80% Market Share*. Synergy Research Group Cloud Infrastructure Report, Q2 2024. Consultado a 18/01/2026. Disponível em: <https://www.srgresearch.com/articles/cloud-market-reaches-270-billion-in-2024>

TechRound. (2024). *Top Unicorns in Portugal*. Consultado a 18/01/2026. Disponível em: <https://techround.co.uk/startups/top-unicorns-in-portugal/>

The Portugal News. (2024, 17 de outubro). *Most public entities affected by cyber attack back to normal*. Consultado a 18/01/2026. Disponível em: <https://www.theportugalnews.com/news/2024-10-16/most-public-entities-affected-by-cyber-attack-back-to-normal/92878>

TICE.PT. (2021). *Portugal lança hub nacional do projeto europeu Gaia-X*. Consultado em 26/01/2026, disponível em <https://linktoleaders.com/portugal-lanca-hub-nacional-do-projeto-europeu-gaix/>

Trade.gov. (2024). *Portugal - Information and Communications Technology*. Consultado a 18/01/2026. Disponível em: <https://www.trade.gov/country-commercial-guides/portugal-information-and-communications-technology>

Tridgell, J. (2025). *Open or closing doors? The influence of digital sovereignty policy on European cybersecurity*. *Technology in Society*, 66. Consultado a 18/01/2026. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364924001444>

TVI. (2024, 16 de outubro). *Ataque informático deixa plataformas do Estado inoperacionais* [Jornal Nacional, reportagem em vídeo]. Consultado a 18/01/2026. Disponível em: <https://tviplayer.iol.pt/programa/jornal-nacional/63e6588b0cf2665294d4f012/video/671024760cf2f130c2997db2>

Two Birds. (2025). *NIS2 Directive Transposition in Portugal: Status and Brief Overview*. Consultado a 18/01/2026. Disponível em: <https://www.twobirds.com/en/insights/2025/nis2-directive-transposition-in-portugal-status-and-brief-overview>

von Ditzfurth, L. (2025). *The European Union's pursuit of digital sovereignty through legislation*. *JIPITEC*, 16, 286–314. Consultado a 18/01/2026. Disponível em: <https://www.jipitec.eu/jipitec/article/view/442>

Xavier, N., & De Barros, G. O. (n.d.). *TE 100 - Soberania Digital em Portugal: Enquadramento, prioridades e estratégia - GEE*. Consultado a 18/01/2026. Disponível em: <https://www.gee.gov.pt/pt/estudos-e-seminarios/estudos-de-temas-economicos-category/32190-te-soberania-digital-em-portugal-enquadramento-prioridades-e-estrategia>

Xu, W., & Wu, P. (2025). *Foreign language teaching and learning in Chinese higher education: Emerging challenges*. *Frontiers in Education*. Consultado a 18/01/2026. Disponível em: <https://www.frontiersin.org/articles/10.3389/feduc.2025.1668049/full>

Zinovieva, E., & Bulva, V. (2021). *EU Digital Sovereignty. Contemporary Europe*. Consultado a 18/01/2026. Disponível em: <http://dx.doi.org/10.15211/soveurope220214049>

Zuboff, S. (2019). *The age of surveillance capitalism*. *PublicAffairs*.

Zürn, M. (2018). *A theory of global governance*. *Oxford University Press*.