Estágio Académico EuroDefense - Portugal 2025

A Soberania Digital e a Cibersegurança:
Estratégias da União Europeia para Proteger Infraestruturas Críticas na Era das Tecnologias Emergentes

Autoria
Carlota Honoré Wilson
Érica Eduardo
Lara Rodrigues
Leonor Gonçalves
Valentina Ruas

Índice

1. Introdução

1.1 Enquadramento do tema

A digitalização profunda das sociedades contemporâneas tornou a esfera digital num novo espaço de poder, vulnerabilidade e disputa estratégica. Com a crescente interdependência entre sistemas tecnológicos e setores vitais como o da energia, saúde, transportes, finanças ou segurança, a proteção das infraestruturas críticas assumiu uma dimensão central nas políticas de segurança nacional e supranacional.

Neste novo paradigma, a soberania digital corresponde à capacidade de um Estado ou bloco regional, como a União Europeia, para controlar autonomamente os seus dados, infraestruturas tecnológicas e sistemas digitais. Esta soberania torna-se particularmente desafiante num contexto global marcado pela concentração tecnológica nas mãos de grandes potências extra-europeias como por exemplo os Estados Unidos ou a China, cujos interesses nem sempre coincidem com os da Europa.

Paralelamente, a cibersegurança emerge como um campo prioritário para garantir a continuidade funcional, a proteção de dados sensíveis e a resiliência estrutural das democracias. A proteção das infraestruturas críticas, cada vez mais digitalizadas e interligadas, passou a ser uma preocupação transversal das autoridades europeias, sobretudo após sucessivos episódios de ciberataques com consequências materiais e institucionais reais.

1.2 Relevância e atualidade no contexto europeu

O contexto europeu recente tem demonstrado de forma inequívoca a crescente vulnerabilidade dos Estados e das suas infraestruturas face a ciberataques.

Em Portugal, em 2022, um ataque de ransomware ao Centro Hospitalar de Lisboa Ocidental comprometeu o acesso a registos clínicos e paralisou serviços médicos por várias horas. No mesmo ano, a empresa de transportes Barraqueiro foi alvo de um ciberataque que afetou os sistemas de bilhética e gestão operacional.

No plano europeu, destaca-se o ataque dirigido à Agência Europeia de Medicamentos, em que dados relacionados com vacinas contra a COVID-19 foram acedidos e manipulados .

Outro exemplo, em 2023, a empresa alemã de energia E.ON foi também alvo de um ciberataque de larga escala, expondo falhas em sistemas considerados críticos para a estabilidade energética do continente.

Estes incidentes demonstram que não se trata de riscos abstratos, mas de ameaças reais e em expansão, com potencial para comprometer serviços essenciais, abalar a confiança pública e gerar impactos socioeconómicos profundos.

Face a este cenário, a União Europeia tem vindo a reforçar o seu quadro normativo e institucional, promovendo iniciativas como a Diretiva NIS2 , o Digital Compass 2030 bem como o fortalecimento da ENISA, a agência europeia responsável pela cibersegurança. Estas medidas refletem a ambição de garantir uma abordagem coordenada à proteção digital das infraestruturas críticas.

1.3 Objetivos e estrutura do trabalho

Este trabalho tem como objetivo analisar de forma crítica e fundamentada as estratégias da União Europeia para proteger as infraestruturas críticas num contexto marcado pela emergência de novas tecnologias digitais e pelo aumento das ameaças cibernéticas. O foco incide na forma como a UE procura articular a soberania digital com a resiliência tecnológica e a proteção cibernética, de modo a garantir segurança, autonomia estratégica e estabilidade institucional.

A estrutura do trabalho organiza-se da seguinte forma:

- ➔ O Capítulo 1 corresponde à introdução;

- ➔ O Capítulo 2 apresenta o enquadramento conceptual dos principais termos como soberania digital, cibersegurança e infraestruturas críticas, oferecendo uma base teórica para a análise subsequente;

- ➔ O Capítulo 3 analisa as estratégias europeias para reforçar a soberania digital, incluindo as principais políticas, iniciativas legislativas adotadas e os mecanismos de financiamento;

- ➔ O Capítulo 4 examina a proteção cibernética das infraestruturas críticas, com foco nas ameaças atuais e nos mecanismos de resposta;

- ➔ O Capítulo 5 discute os desafios ainda presentes e explora propostas para o futuro, nomeadamente no que toca à cooperação, inovação e capacitação digital;

- ➔ O Capítulo 6 encerra com uma síntese da análise desenvolvida e com reflexões finais sobre as implicações políticas e estratégicas do tema.

2. Enquadramento Conceptual

2.1 Soberania digital: definição e evolução na União Europeia

A soberania é um conceito que surgiu e evoluiu historicamente em associação com a ideia de território, povo e poder (Hinsley, 1988). Apesar de até ao último século se pensar que soberania não era um mero ato de legislar ou governar conforme a lei, mas sim o poder de decidir quando a lei já não era suficiente, e agir fora desta para salvar a ordem, as atrocidades das Grandes Guerras conduziram inexoravelmente à reformulação da sua ideia. O Estado soberano já não podia correr o risco de ser totalmente livre, devendo portanto estar sujeito a limitações internas e externas (Motha, 2008).

No contexto contemporâneo, a soberania enfrenta novos desafios resultantes da transformação digital. A conceção tradicional de soberania estatal foi questionada pela natureza imaterial, transnacional e difusa do novo espaço criado pelas tecnologias digitais (Svantesson, 2014). Neste cenário, emerge o conceito de soberania digital, que assume uma relevância crescente e transversal, afetando até aqueles que não recorrem diretamente a dispositivos digitais. Refere-se à capacidade de uma certa entidade atuar com autonomia e poder de regulação sobre dados, software, normas e protocolos, processos, equipamentos e infraestruturas (Floridi, 2020). A luta pelo controlo digital, marcada por uma complexa rede de alianças variáveis, tanto entre atores estatais e entidades privadas, constitui um conflito de escala histórica. Neste sentido, a soberania digital revela-se essencial para que um país, ou

região, possa definir e organizar autonomamente o seu modelo de desenvolvimento económico, social e tecnológico.

Contudo, poucos governos têm adotado uma postura estratégica e coordenada na definição das suas políticas de educação, investigação, desenvolvimento industrial, expansão de infraestruturas digitais e governação de dados, visando o reforço dessa soberania (Belli et al, 2023). É precisamente neste enquadramento que se compreende o aparecimento das reivindicações por soberania digital no contexto europeu. Estas surgiram, em grande medida, de uma perceção crescente de dependência face ao papel considerado excessivo das empresas tecnológicas estrangeiras. De facto, o mercado de produtos e serviços digitais encontra-se amplamente dominado por corporações multinacionais sediadas nos Estados Unidos e na China (Bedingfield, 2020), o que levanta riscos significativos associados à incapacidade europeia de controlar plenamente os seus dados e infraestruturas digitais. Perante este cenário, a União Europeia passou a encarar a restauração da soberania sobre o segmento do ecossistema digital como uma estratégia fundamental para proteção do seu modelo único de direitos fundamentais, valores e interesses económicos. Com esse objetivo, têm sido lançadas várias iniciativas, tanto pelos Estados-Membros como pela própria União (Celeste, 2021).

2.2 Cibersegurança: conceito e importância estratégica

A cibersegurança pode ser definida como o conjunto de tecnologias, medidas e processos desenvolvidos com o objetivo de proteger computadores, componentes de hardware, software, redes e dados contra acessos não autorizados e contra a exploração de vulnerabilidades, sobretudo aquelas facilitadas através da Internet por cibercriminosos, grupos terroristas e hackers. Trata-se de uma área intrinsecamente ligada à proteção de equipamentos digitais e das respectivas informações armazenadas ou transmitidas via rede ou Internet, prevenindo acessos indevidos e alterações não autorizadas (Goutam, 2015).

Nos tempos atuais, a Internet não se limita a ser uma fonte de informação, assumiu-se como um meio fundamental para o funcionamento da sociedade e da economia. A multiplicidade de benefícios permite a execução de tarefas com maior rapidez, menor esforço humano e custos reduzidos, potenciando oportunidades sem precedentes no que respeita à comunicação, inovação e eficiência organizacional. Importa, contudo, recordar que a Internet não foi originalmente concebida para fins de monitorização comportamental. A sua criação

visava, essencialmente, a interligação de sistemas informáticos autónomos, permitindo a partilha de recursos e fomentando a cooperação científica, nomeadamente através da criação de uma plataforma comum destinada à comunidade académica (Lipson, 2002).

Paralelamente aos benefícios proporcionados, este ecossistema abriu espaço para a proliferação de atividades maliciosas. O cibercrime, enquanto fenómeno complexo e multifacetado, engloba um vasto leque de condutas ilícitas praticadas através da Internet ou de infraestruturas tecnológicas interligadas, tais como phishing, fraude com cartões de crédito, espionagem industrial, criação e disseminação de malware, spam e ciberterrorismo. Neste contexto, a cibersegurança adquire uma dimensão estratégica fundamental, enquanto ferramenta de defesa contra ameaças que comprometem não apenas os sistemas informáticos, mas também a estabilidade social, económica e institucional (UNODC, 2012).

Com o crescimento exponencial das tecnologias de informação e comunicação, grande parte dos processos administrativos e operacionais passaram a ocorrer em ambiente digital. A digitalização da vida quotidiana, incluindo a realização de transações financeiras e a gestão de registos sensíveis, aumentou a vulnerabilidade dos sistemas, tornando imprescindível a implementação de medidas de cibersegurança robustas.

Neste cenário, a cibersegurança assume uma dimensão estratégica crítica. Para além de mitigar riscos associados a ataques informáticos, contribui decisivamente para a confiança nas tecnologias digitais. Esta responsabilidade é particularmente significativa no setor público, onde os organismos governamentais, quer a nível central, regional ou local, detêm vastas quantidades de dados sensíveis e registos digitais que os tornam alvos atrativos para ataques cibernéticos. As principais dificuldades enfrentadas por estas entidades prendem-se com infraestruturas desatualizadas, insuficiente sensibilização e falta de investimento adequado. É, por isso, imperativo que os serviços públicos garantam a segurança da informação, assegurem a prestação de serviços digitais fiáveis à população e promovam uma comunicação transparente e protegida com os cidadãos (CISCO, 2010).

Reconhecendo este desafio, a União Europeia tem vindo a reforçar o seu compromisso através da adoção de uma nova estratégia que visa promover uma digitalização segura, resiliente e soberana. Esta iniciativa destaca a importância de proteger não apenas os sistemas tecnológicos, mas também os direitos fundamentais dos cidadãos, através de uma abordagem integrada que combina instrumentos regulamentares, investimentos e políticas públicas. Para

tal, a cooperação estreita entre os Estados-Membros, os setores público e privado, e parceiros internacionais que partilham os valores de democracia, Estado de direito e direitos humanos, é fundamental. A criação de uma ciberunidade conjunta e a mobilização de recursos coletivos pretendem reforçar a capacidade operacional da UE para prevenir, dissuadir e responder de forma eficaz a ameaças cibernéticas cada vez mais complexas e coordenadas (União Europeia, 2025).

2.3 Infraestruturas críticas e tecnologias emergentes

Nos últimos anos, diversos setores industriais têm sido alvos recorrentes de ciberataques dirigidos às suas infraestruturas críticas. Estes ataques recorrem a técnicas sofisticadas, como a introdução de malware através de software de terceiros, correio eletrónico ou websites comprometidos, por exemplo. Os seus objetivos consistem em aceder a sistemas informáticos sensíveis, com o intuito de comprometer o funcionamento de serviços essenciais, com impactos significativos à escala nacional ou internacional. A eficácia destas ações maliciosas é frequentemente atribuída à insuficiente formação técnica de muitos utilizadores e profissionais envolvidos na operação e proteção destas infraestruturas. Um estudo realizado em 2015 revelou que 31% das falhas de segurança em empresas industriais nesse ano foram causadas por erros humanos (IRM, 2015).

Neste panorama de risco crescente, é essencial considerar o papel das tecnologias emergentes, cuja adoção, embora inevitável, introduz novos desafios à proteção das infraestruturas críticas. As tecnologias emergentes distinguem-se por combinarem atributos sociais, tais como alavancagem, ascensão, ambivalência e materialidade, com características artificiais, nomeadamente a novidade radical, crescimento acelerado, coerência, impacto significativo e ambiguidade, tudo isto tendo em conta um determinado horizonte temporal. Embora geralmente tenham origem em desenvolvimentos técnicos, estas tecnologias evoluem de forma dinâmica e multidimensional, refletindo uma transformação simultaneamente técnica e social (Litvinski, 2018).

No espaço europeu, destacam-se cinco tecnologias emergentes como particularmente estruturantes da sociedade digital: as comunicações móveis de quinta geração (5G), a computação na nuvem, a inteligência artificial, a Internet das Coisas (IoT) e as tecnologias

quânticas. Estas tecnologias são já elementos fundamentais ou encontram-se em franca expansão, sendo indispensáveis para a transição digital em curso. No entanto, ainda não existe uma abordagem sistemática e integrada para lidar com os riscos de cibersegurança associados, quer de forma isolada como na sua utilização combinada (CNCS, 2023).

Face a este cenário, torna-se imperativo reforçar a preparação proativa e estratégica da União Europeia, promovendo uma compreensão aprofundada dos riscos emergentes e desenvolvendo respostas sociais, técnicas e jurídicas adequadas à proteção das infraestruturas críticas num ecossistema digital em rápida mutação.

3. Estratégias Europeias para a Soberania Digital

3.1 Autonomia Estratégica e Soberania Digital

Inicialmente centrada na defesa, o conceito de autonomia estratégica da União Europeia foi alargado posteriormente às áreas económicas e tecnológicas, como por exemplo, a cadeias de abastecimento tecnológicas, acesso a matérias-primas (criação da Aliança Europeia para as Matérias-Primas) e proteção a infraestruturas críticas. A Estratégia Global da UE de 2016 é um marco importante na formulação da política externa e de segurança da UE, ao introduzir explicitamente o conceito de autonomia estratégica e associar a autonomia à capacidade de decisão e ação própria num sistema internacional cada vez mais multipolar e competitivo. (European External Action Service, 2016). A autonomia estratégica emerge num contexto internacional onde potências como a China ameaçam a economia da Europa e é neste cenário que o conceito surge como uma forma de manter a sua relevância global e reforçar a sua capacidade de ação. Além disso, a pandemia revelou fragilidades da Europa, como a interdependência global assimétrica e revelou vulnerabilidades nas áreas de ciência, tecnologia, dados, comércio e investimento que são cada vez mais relevantes para o contexto geopolítico atual. É com base nisto, que a União Europeia encara a transformação digital para salvaguardar os seus interesses estratégicos. (Borrell, 2020)

Recentemente, o conceito de soberania digital tem aumentado o seu destaque como uma forma da UE se afirmar no sistema internacional e reforçar a sua autonomia estratégica no domínio digital.

A atual preocupação da Europa com a soberania digital surgiu num contexto mais amplo de insegurança global e da necessidade de proteger os seus cidadãos. Crises como a financeira de 2009, a agressão russa à Ucrânia em 2015, a crise migratória e a imprevisibilidade da administração Trump levaram a União Europeia a repensar a sua posição estratégica e a defender uma maior autonomia, especialmente na área da defesa e da economia. Além disso, a influência crescente económica da China e o papel da empresa chinesa Huawei nas redes 5G levantaram preocupações adicionais. A pandemia da COVID-19, como mencionada previamente, reforçou a importância de garantir cadeias de abastecimento seguras e reforçar o controlo sobre recursos essenciais. Ao mesmo tempo, ficou evidente o papel central da digitalização na vida quotidiana e na resposta a crises, o que aumentou a consciência sobre questões de privacidade e a necessidade de investir na inteligência artificial, gestão de dados e plataformas digitais europeias. Um dos motivos das fragilidades da Europa na área digital deve-se à existência de diferentes leis e regulamentos nacionais que dificultam a criação de um mercado único. Esta fragmentação impede que empresas tecnológicas europeias cresçam a nível global, como fizeram a Google ou o Facebook. Além disso, muitas *startups* têm dificuldade em obter financiamento e acabam por se mudar para os Estados Unidos ou ser compradas por empresas americanas. Embora os líderes europeus reconheçam estas falhas internas, também criticam o domínio agressivo de empresas como a Google, Apple, Facebook e Amazon (Burwell & Propp, 2020).

A Comissão Europeia tem defendido a necessidade de soberania digital como forma de garantir autonomia estratégica e proteger os dados, infraestruturas e normas europeias. A soberania digital para a UE é vista como a capacidade de estabelecer as suas próprias regras no mundo digital. Ainda assim, levanta-se o debate sobre se esta estratégia é protecionista. Enquanto alguns líderes defendem que se trata apenas de criar alternativas tecnológicas europeias, outros admitem dar prioridade a empresas da UE, o que pode significar discriminação contra empresas estrangeiras. Dentro da própria Comissão Europeia existem posições diferentes sobre até que ponto esta autonomia digital deve ir. A Alemanha e outros países europeus começaram a restringir o uso de tecnologias estrangeiras em nome da soberania digital, como no caso do cancelamento de contratos com empresas americanas. A questão mais controversa tem sido o uso de equipamentos da Huawei nas redes 5G. Os EUA pressionaram os aliados europeus a excluir a empresa chinesa por motivos de segurança, mas países como o Reino Unido, França e Países Baixos optaram por uma abordagem intermédia. A Comissão

Europeia recomendou precauções semelhantes, mas sem impor regras. As decisões europeias são influenciadas pelos custos mais baixos da Huawei e pela sua presença pré-existente nas redes, mesmo que isso entre em conflito com os objetivos de autonomia digital da UE. (Burwell & Propp, 2020).

Apesar de ter avanços digitais relevantes, a UE continua a ter limitações e investimentos reduzidos em comparação aos EUA e a China, tanto em investimento privado em IA, como atração de talento, registo de patentes e adoção dessas tecnologias por empresas e cidadãos. Além disso, a China é líder no acesso e recolha de dados, algo essencial para a IA, e tem também avançado com o desenvolvimento de infraestruturas como supercomputadores. Os EUA continuam à frente em áreas como a computação quântica, *blockchain* e *Internet of Things* (IoT).

Devido à falta de consenso e estabelecimento de uma definição clara da soberania digital, em 2020, a Comissão Europeia definiu que a soberania digital envolve a proteção e resiliência dos dados, infraestruturas, redes e comunicações. No ano seguinte, apresentou a comunicação "2030 Digital Compass: the European way for the Digital Decade" com objetivos e metas gerais a serem alcançados até 2030, nomeadamente: 80% da população com competências digitais básicas e formar 20 milhões de especialistas em tecnologias da informação e da comunicação; expandir a conectividade Gigabit e 5G; fortalecer a produção de semicondutores avançados e implementar 10.000 nós de computação segura; 100% dos serviços essenciais disponíveis online, incluindo identidade digital europeia e acesso a registos médicos eletrónicos; incentivar a adoção de IA, computação em nuvem e *big data* por 75% das empresas e apoiar *start-ups.* (Comissão Europeia, 2021).

A Década Digital reforça a Bússola Digital ao implementar mecanismos de acompanhamento (sistema de monitorização, relatórios anuais, entre outros) como forma de atingir os objetivos estabelecidos pela Bússola Digital (Comissão Europeia, s.d.).

Ao limitar a influência de atores externos e ao promover o desenvolvimento de capacidades internas, a UE procura garantir maior controlo sobre o seu futuro digital. Esta estratégia passa tanto pela criação de novas políticas como pela adaptação de instrumentos

existentes de forma a demonstrar que a soberania digital é atualmente uma dimensão essencial para a autonomia estratégica europeia.

3.2. Principais Políticas e Regulamentos

Analisemos as principais estratégias (ilustradas na tabela 1) que a UE desenvolveu para o reforço da sua soberania digital.

Tabela 1: Regulamentos e Ano de Adoção/Aplicação

Regulamentos/Políticas	Data de Adoção/Aplicação
Regulamento Geral sobre a Proteção de Dados (RGPD)	Adotado: 2016 Aplicação: 2018
Regulamento dos Mercados Digitais (DMA)	Aprovado:2022 Aplicação: 2023
Regulamento dos Serviços Digitais (DSA)	Aprovado: outubro 2022 Aplicação: 2024
Regulamento Europeu dos Circuitos Integrados (Chips Act)	Aprovado: julho 2023 Aplicação: 2023
Regulamento da Inteligência Artificial (AI Act)	Aprovado: maio 2024 Aplicação completa: entre 2025 e 2026
Estratégia para os dados (Data Act)	Adotado: 2024
Gaia-X	Lançamento: 2019 Aplicação faseada: desde 2021

- Regulamento Geral sobre a Proteção de Dados (RGPD)

É um regulamento que estabelece normas rigorosas de gestão e proteção de dados dos cidadãos europeus. Esta política reforça o controlo do mercado interno com sanções financeiras. Além do seu impacto interno, o RGPD tem uma dimensão externa importante. Casos como Schrems I e II demonstram como os tribunais europeus invalidaram acordos de

transferência de dados entre a UE e os EUA, como o "Safe Harbour" e o "Privacy Shield", por considerarem que não garantiam proteção adequada pelas autoridades norte-americanas. Em 2023, a CE estabeleceu um novo acordo com os EUA chamado o EU-US *Data Privacy Framework*, que procura limitar a vigilância excessiva das autoridades americanas. Além disso, a partir desse ano, a aplicação do RGPD intensificou-se com um aumento significativo de multas, entre elas contra o TikTok, de 530 milhões de euros, e Uber, de 290 milhões de euros. (Broeders et. Al, 2023; Reuters, 2025; Lomas, 2024)

- Regulamento dos Mercados Digitais (RMD)

Tem como objetivo a imposição de regras específicas às grandes plataformas digitais que atuam como controladores de acesso como empresas *Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft*. Na prática, isso significa que vão ter de permitir, por exemplo, que outros serviços consigam funcionar em conjunto com os seus, sempre que for necessário. As empresas que usam essas plataformas também devem poder aceder aos dados que geram enquanto usam esses serviços. Além disso, quem faz publicidade nestas plataformas tem de receber ferramentas e informações suficientes para poder confirmar por si próprio se os anúncios estão a funcionar bem. Os mesmos, têm de poder promover os seus produtos e fechar vendas diretamente com os clientes, mesmo fora da plataforma dos controladores de acesso se for essa a preferência do consumidor. Simultaneamente, estas plataformas têm restrições consideradas práticas abusivas, como por exemplo, dar destaque aos seus próprios produtos ou serviços em detrimento dos de outras empresas que usam a mesma plataforma. Também não podem impedir os consumidores de visitar ou comprar noutras lojas online. Se houver aplicações pré-instaladas nos dispositivos, os utilizadores poderão apagá-las se não as quiserem. Além de que estas empresas não podem continuar a seguir os utilizadores fora da sua plataforma principal para fazer publicidade direcionada, a menos que tenham recebido um consentimento claro e explícito. O regulamento beneficia não só pequenas empresas, pois oferece melhores condições de acesso ao mercado digital, mas também aos consumidores ao garantir uma maior variedade de serviços e preços mais competitivos. (Comissão Europeia, 2023b)

- Regulamento dos Serviços Digitais (RSD)

O principal objetivo do RSD é combater conteúdos ilegais, práticas prejudiciais e a desinformação. Além de proteger melhor os direitos dos utilizadores, este regulamento cria

regras mais justas para as plataformas digitais, ajudando especialmente as pequenas e médias empresas na competitividade. Aplica-se a vários tipos de prestadores de serviços online, como redes sociais, mercados digitais, lojas de aplicações, plataformas de alojamento ou de partilha de conteúdos. As regras variam consoante o tipo, o papel e a dimensão da plataforma, ou seja, maiores plataformas e motores de busca estão sujeitos a obrigações mais rigorosas devido ao maior impacto de divulgação de conteúdos ilegais. Todas as plataformas que operem no mercado europeu, mesmo que estejam fora da UE, têm de cumprir estas regras. (Parlamento Europeu, 2021)

- Regulamento Europeu dos Circuitos Integrados (*European Chips Act*)

É um regulamento que visa a reforçar a competitividade da UE no setor dos semicondutores que são essenciais para as cadeias de valor industriais e para a transição digital e ecológica. A UE desenvolveu esta estratégia devido à escassez global recente de semicondutores (aumentada pelas tensões geopolíticas) que expôs a dependência da Europa de um número reduzido de fornecedores externos. O regulamento assenta em três pilares: promoção da inovação e desenvolvimento tecnológico através desta iniciativa; fomentar um ambiente propício ao investimento de fábricas na Europa; criar um sistema de cooperação entre a Comissão Europeia, os Estados-Membros e os principais envolvidos. A estratégia tem como objetivo expandir a capacidade de produção com a meta de atingir 20% da quota de mercado global até 2030 e fortalecer as competências europeias em investigação, design, fabrico e embalagem de circuitos avançados. Além disso, promove parcerias internacionais, estabelece mecanismos para responder a crises e desenvolve infraestruturas de ensaio e certificação e apoia startups e Pequenas Médias Empresas (PME). (Comissão Europeia, s.d.)

- Regulamento da Inteligência Artificial (*AI Act*)

Estabelece regras para o uso de IA baseado no nível de risco (categorias como inaceitável, elevado, limitado e mínimo) e garante a segurança, transparência e proteção dos direitos fundamentais assentes nos valores da UE. Além de regulamentar a tecnologia, tem como objetivo incentivar a inovação e investimento ao apoiar startups e PMEs para o desenvolvimento de soluções, além de apostar nas parcerias público-privadas, centros de excelência e polos de inovação. Com base nisto, tem como objetivo tornar-se líder mundial na IA baseado em valores de inclusão e sustentabilidade (Parlamento Europeu, 2023).

- Estratégia Europeia para os Dados (*Data Act*)

Desenvolvimento de um mercado único de dados com o objetivo de permitir a circulação segura e eficiente de dados entre setores e países. Para isso, pretende assegurar que o acesso e uso dos dados seja feito de forma justa, transparente e em conformidade com as normas europeias, como o RGPD. Ao definir regras claras sobre quem pode aceder e utilizar os dados de dispositivos conectados e em que condições isso pode acontecer, pretende-se reduzir assimetrias de poder e evitar que empresas com maior domínio do mercado imponham cláusulas contratuais abusivas. Além disso, o regulamento facilita o acesso a dados privados por parte de entidades públicas, sempre que tal seja necessário para responder a situações de interesse público, como catástrofes naturais ou emergências sanitárias. Outro ponto relevante é o incentivo à concorrência no setor da computação em nuvem, através da simplificação dos processos de mudança entre prestadores de serviços de forma a evitar os bloqueios contratuais. A proposta inclui ainda uma revisão das regras de proteção de bases de dados. Na prática, espera-se que o *Data Act* estimule a inovação e a criação de novos modelos de negócio baseados na utilização de dados. Para os consumidores, isso poderá traduzir-se numa maior liberdade de escolha, por exemplo ao decidir onde reparar os seus produtos inteligentes, o que favorece preços mais competitivos. Para as empresas, o acesso mais facilitado e estruturado de dados poderá permitir melhorias significativas na eficiência de processos, nomeadamente na indústria e na agricultura, onde os dados em tempo real podem ser usados para otimizar cadeias de produção, logística e gestão de recursos naturais. (European Commission, 2024)

- Gaia -X

Em 2019, França e Alemanha lançaram este projeto para conectar provedores de serviços de cloud na Europa utilizando padrões abertos e normas comuns de privacidade e segurança. O objetivo é permitir que empresas e clientes possam movimentar dados industriais livremente dentro da Europa. Outros países da UE estão a ser convidados a participar, e a Comissão Europeia procura integrar essa iniciativa com a sua própria estratégia para uma infraestrutura de cloud federada. Essa preocupação com a proteção dos dados na Europa também reflete o receio em relação ao acesso dos governos estrangeiros, especialmente devido ao US CLOUD Act, que permite às autoridades americanas requisitar dados armazenados em empresas dos EUA. Para enfrentar isso, a UE está a negociar um acordo com os EUA para lidar com essas questões. Além disso, vários países europeus adotaram medidas de "data localization", que exigem que certos dados sensíveis, como informações de saúde ou financeiras sejam armazenados dentro do país. Embora algumas dessas medidas tenham

justificativas legítimas, como a supervisão regulatória, elas também podem ser usadas para proteger fornecedores locais de cloud mesmo que ofereçam serviços inferiores. A legislação europeia permite essa localização para dados pessoais, mas para dados não pessoais, que são essenciais para a indústria e a Internet das Coisas, a UE proibiu a exigência de armazenamento local com exceções de segurança pública. (Burwell & Propp, 2020). Gaia –X, apesar de não ser uma estratégia da UE e sim uma iniciativa colaborativa entre governos e empresas europeias, tem como finalidade o reforço da soberania digital da Europa.

3.3. Mecanismos de Financiamento

Neste contexto, a UE mobiliza vários mecanismos de financiamento para transformar as suas ambições digitais em ações concretas, sendo estes indispensáveis para atingir os objetivos da UE. Estas iniciativas têm como objetivo acelerar a inovação e infraestruturas digitais, certificando-se que a transformação é inclusiva e que aborde todos os setores da economia e sociedade. Estes programas estão inseridos no Quadro Financeiro Plurianual e no plano de recuperação NextGenerationEU de 2021 a 2027, nomeadamente:

- ➔ Programa Europa Digital (DIGITAL): Com um orçamento de 7,59 mil milhões de euros, apoia a implementação da supercomputação, inteligência artificial, cibersegurança e competências digitais avançadas e também contribui para a transformação digital da indústria, das PMEs e da administração pública. Além disso, quer também reduzir as desigualdades entre países. Entre as principais ações, destaca-se a criação de Espaços Europeus Comuns de Dados, infraestrutura de comunicação quântica segura e a promoção de serviços públicos digitais interoperáveis. É através dos *European Digital Innovation Hubs*, uma rede de cerca de 200 polos de inovação digital espalhados por toda a Europa, que o programa oferece apoio direto a empresas e entidades públicas no processo de transformação digital. Também se destaca o apoio à formação especializada em competências digitais e o investimento em cibersegurança, com medidas como os Centros de Operações de Segurança e o reforço da legislação europeia.

- ➔ Horizonte Europa: Financia a investigação e a inovação de modo a apoiar cientistas, investigadores e empresas. As áreas de foco deste programa são da saúde, ambiente, transição verde, tecnologia e investigação espacial e industrial, complementado o DIGITAL. Tem um orçamento total de 95,5 mil milhões de euros. É estruturado por

três pilares: 1º Ciência de excelência, 2º Desafios globais de competitividade da industria europeia, 3º Europa inovadora. Para este efeito, no segundo pilar, destaca-se "Digital, Indústria e Espaço" com 15,3 mil milhões de euros, que financia áreas como IA, computação de alto desempenho, *big data*, internet de nova geração e redes 6G. A digitalização também está presente nas áreas da saúde, mobilidade, clima e agricultura com o objetivo de fomentar soluções tecnológicas para esses setores. No terceiro pilar, o programa apoia a inovação de base tecnológica através do Conselho Europeu de Inovação e do Instituto Europeu de Inovação e Tecnologia, nomeadamente com o EIT Digital, que junta universidades, empresas e centros de investigação para impulsionar o empreendedorismo digital.

- ➔ Mecanismo Interligar a Europa (MIE) Digital: Faz parte da MIE cujo objetivo é apoiar a construção e o aprimoramento das infraestruturas da Europa. MIE Digital possui um orçamento de 2,06 mil milhões de euros cujas ações financiadas destacam-se a cobertura contínua com 5G ao longo dos principais eixos de transporte da UE, a instalação de cabos submarinos e redes backbone entre Estados-Membros e países terceiros, bem como o desenvolvimento de infraestruturas digitais associadas a projetos transfronteiriços de energia e transportes.

- ➔ InvestEU: É um instrumento que agrupa diferentes fundos europeus de modo a facilitar o acesso ao financiamento a empresas e projetos. Atrai investimento público e privado para iniciativas que ajudam na sustentabilidade da Europa, tendo como áreas de apoio à inovação e investigação, transição verde e digital (onde pelo menos 20% destina-se a prioridades digitais), inclusão social e formação e apoio a PME e empreendedores.

Apesar dos instrumentos DIGITAL e CEF Digital (Connecting Europe Facility) serem os que têm a área digital como foco principal, os outros apoiam a digitalização de modo parcial. Estes instrumentos não só permitem desenvolver capacidades tecnológicas avançadas, como também promover a adoção de tecnologias emergentes e a formação de competências digitais essenciais para garantir que a UE esteja preparada para enfrentar os desafios da transformação digital com autonomia estratégica e resiliência (Miron et. Al, 2024; Comissão Europeia, 2022; Comissão Europeia, 2023).

3.4. A digitalização como fator de resiliência

Como podemos verificar, o Regulamento Geral sobre a Proteção de Dados (RGPD), o Regulamento dos Mercados Digitais (RMD) e o Regulamento dos Serviços Digitais (RSD) representam uma transformação na forma como o digital é regulado na Europa. Enquanto o RGPD protege os dados dos utilizadores, o RMD garante regras de concorrência justa, e o RSD promove um ambiente online mais seguro e transparente. Neste sentido, os direitos dos cidadãos estão no centro da transformação digital. Por outro lado, o *AI Act* define os limites éticos da IA; o *Chips Act* assegura a produção de microchips; o *Data Act* foca-se nos dados dos cidadãos europeus e o Gaia-X é um projeto que junta empresas e governos para criar infraestruturas de armazenamento e partilha de dados da Europa. Embora estas estratégias sejam diferentes nos seus objetivos, contribuem para o desenvolvimento de uma Europa mais resiliente e inovadora. Estas políticas não só garantem a proteção dos cidadãos e empresas, controlam os seus ativos tecnológicos, promovem a coesão social, como também promovem a competitividade mundial de modo a ter uma adaptação flexível às mudanças digitais. Adicionalmente, estudos demonstram que a transformação digital melhora a capacidade das empresas de aprender com os problemas e de inovar para os resolver. Isso torna as organizações mais preparadas para lidar com mudanças inesperadas (Syaifuddin et al., 2024).

Em conclusão, a resiliência digital é crucial num mundo onde as ameaças cibernéticas estão cada vez mais sofisticadas e a dependência da tecnologia aumenta aceleradamente (LogAp, 2025). Neste sentido, torna-se claro que a soberania digital é essencial para a resiliência da União Europeia.

4. A Proteção Cibernética das Infraestruturas Críticas

4.1. Ameaças cibernéticas e casos relevantes na UE

A transformação digital provocou mudanças profundas no campo da cibersegurança. Com o surgimento da pandemia de COVID-19, muitas empresas foram obrigadas a adaptar-se rapidamente a novas formas de organização, recorrendo ao teletrabalho e tornando-se, consequentemente, mais dependentes da tecnologia. Esta rápida transição veio acompanhada

de um aumento das ameaças cibernéticas, que passaram a ter um impacto mais visível no funcionamento das infraestruturas críticas e, por consequência, no quotidiano das pessoas.

Em setembro de 2024, a Agência da União Europeia para a Cibersegurança (ENISA) publicou o relatório *ENISA Threat Landscape 2024*, no qual apresenta uma análise aprofundada das principais ameaças cibernéticas que incidem sobre o espaço da União Europeia. Este documento constitui um instrumento fundamental para a compreensão das tendências emergentes no domínio da cibersegurança, destacando um aumento notório na frequência e impacto dos ataques cibernéticos observados a partir da segunda metade de 2023. De acordo com a ENISA, este agravamento está fortemente associado à deterioração do panorama geopolítico, em particular no contexto da guerra na Ucrânia, que tem contribuído de forma significativa para a proliferação e evolução das ameaças no ciberespaço europeu (ENISA, 2024).

As infraestruturas críticas, nomeadamente as redes de energia, os sistemas de abastecimento de água, os serviços financeiros e os transportes, constituem elementos essenciais para o funcionamento eficaz da sociedade contemporânea. Qualquer ataque cibernético dirigido a estas estruturas pode provocar, de imediato, uma instabilidade profunda na vida quotidiana das pessoas. A proteção cibernética destes pilares fundamentais assume-se como uma prioridade incontornável no âmbito da União Europeia, onde a cooperação entre Estados-membros se revela indispensável para assegurar a resiliência e segurança do espaço europeu (ENISA, 2024).

Os principais ataques cibernéticos na União Europeia identificados no relatório da ENISA, incluem *ransomware*, *malware*, engenharia social, ataques à disponibilidade (DDoS), ameaças à integridade dos dados, manipulação da informação e ataques à cadeia de abastecimento, que comprometem fornecedores de software com o objetivo de afetar múltiplas organizações (ENISA, 2024).

Segundo o relatório, os ataques de ransomware registados são particularmente frequentes, utilizando técnicas de encriptação para bloquear o acesso a dados, exigindo resgates elevados em troca, com impactos severos especialmente nos setores da saúde e em outras infraestruturas críticas (ENISA, 2024). Também foi registado o uso de malware,

designadamente *trojans* e *spyware*, com o propósito de obter informação por via de espionagem. Face à evolução destas ameaças, o Parlamento Europeu reforçou a diretiva relativa à harmonização das medidas de proteção cibernética em toda a Europa, incidindo sobretudo nos setores essenciais (Parlamento Europeu, 2023). Simultaneamente, tem-se observado um crescimento do fenómeno conhecido como hacktivismo, que combina ativismo político com técnicas de *hacking*, expandindo-se particularmente em períodos próximos das eleições europeias (ENISA, 2024).

Na União Europeia, têm sido registados diversos casos de ataques cibernéticos. Segundo o Conselho Europeu, as ciberameaças evoluíram substancialmente, apresentando uma tendência de crescimento contínuo (Conselho Europeu, 2023). Os Estados-membros têm vindo a implementar estratégias de defesa e a reforçar a cibersegurança a fim de proteger infraestruturas críticas, assegurar a estabilidade económica e preservar a privacidade digital, aspetos fundamentais para garantir o seu funcionamento adequado. Conforme referido pelo Conselho Europeu, o crescimento contínuo das ciberameaças, impulsionado em grande parte pela evolução da inteligência artificial, tem vindo a elevar o custo económico associado à cibercriminalidade (idem). Estudos estatísticos indicam que 20% dos ataques cibernéticos dirigem-se a organizações da administração pública, seguidos pelos setores dos transportes (11%), financeiro (9%), infraestruturas digitais (9%), serviços às empresas (8%) e indústria transformadora (6%) (ENISA, 2024).

O ataque ao Serviço Nacional de Saúde da Irlanda, ocorrido em 2021, constitui um exemplo visível do impacto significativo que um ciberataque pode causar. Este ataque, do tipo *ransomware* atribuído ao grupo Conti, provocou a perda de dados nos sistemas informáticos do setor da saúde, resultando no cancelamento de consultas e tratamentos, cuja normalização demorou meses a ser restabelecida (ENISA, 2022). Para além disso, dados pessoais dos utentes foram divulgados na dark web, agravando as consequências do incidente.

Outro exemplo relevante ocorreu em 2019, quando a empresa norueguesa *Norsk Hydro*, do setor metalúrgico, foi alvo de um ataque ransomware (LockerGoga), que comprometeu a produção de alumínio. Este ataque gerou impactos importantes na Europa, causando interrupções em várias fábricas e prejuízos superiores a 60 milhões de euros. Na altura, a

empresa optou por divulgar publicamente o incidente e recusou-se a pagar o resgate exigido (ENISA, 2020).

Em 2021, foram registadas campanhas de espionagem digital dirigidas a instituições da União Europeia, atribuídas a grupos estatais que utilizaram técnicas de *phishing* para recolher dados confidenciais no setor da governação (ENISA, 2022). No ano anterior, em 2020, ocorreu o ataque ao *software Orion*, no âmbito do caso SolarWinds, que comprometeu a cadeia de abastecimento de vários setores, em particular da energia das instituições públicas. Este incidente motivou um reforço das políticas da UE relativas à verificação de fornecedores, dado o seu impacto não só na União Europeia, mas a nível global (Comissão Europeia, 2021). Ainda em 2020, a Agência Europeia de Medicamentos (EMA) foi alvo de um ataque cibernético que afetou o setor da saúde e da regulamentação farmacêutica, através de espionagem digital. As consequências incluíram o roubo de dados relativos às vacinas contra a COVID-19 e a manipulação de documentos com o objetivo de desacreditar o plano de vacinação (ENISA, 2021).

A Comissão Europeia alertou também para os riscos associados ao fornecimento de tecnologia 5G, cuja infraestrutura é crítica para setores essenciais como saúde, transportes e energia. O comprometimento das telecomunicações, base das infraestruturas críticas, pode afetar severamente estes setores (Comissão Europeia, 2020). Neste sentido, verifica-se que a dependência crescente de dispositivos IoT, muitos deles com segurança insuficiente, facilita a entrada e propagação de ciberataques (ENISA, 2024).

4.2. Medidas e organismos de cibersegurança

A transformação digital impôs a necessidade crescente de implementar medidas sólidas de cibersegurança, com vista a reforçar a proteção e a resiliência das infraestruturas digitais associadas a setores críticos. Essas medidas abrangem a avaliação de riscos, a implementação de controlos de segurança e a formação adequada dos recursos humanos.

Em 2016, a União Europeia adotou a diretiva relativa à Segurança das Redes e da Informação (SRI), conhecida também por NIS, que constituiu a sua primeira resposta legislativa estruturada para reforçar a cooperação entre os Estados-Membros neste domínio

(Diretiva (UE) 2016/1148). Esta diretiva estabeleceu obrigações específicas de segurança para os operadores de serviços essenciais nos setores críticos, como energia, transportes, saúde e finanças, estendendo também o seu âmbito aos prestadores de serviços digitais, incluindo mercados online, motores de busca e serviços de computação em nuvem.

Com a evolução dos ataques e como medida de reforço da segurança cibernética, a diretiva legislativa criada em 2016 foi revista e melhorada em 2022 pela UE, denominada SRI 2, entrando em vigor em 16 de janeiro de 2023. As novas regras estabelecidas procuram garantir um elevado nível de cibersegurança comum a todos os países da UE. A contínua evolução digital, acelerada pela pandemia de COVID-19, reforçou a urgência de intensificar as medidas de proteção para evitar ataques às infraestruturas críticas. De acordo com o Conselho Europeu, é imperativo assegurar a resiliência das redes 5G, essenciais para a rede digital como também para as infraestruturas críticas (energia, transportes, banca e saúde), indispensáveis à nossa sociedade (Conselho da União Europeia, 2023). Esta medida veio reforçar a gestão e a cooperação no que respeita aos riscos e incidentes cibernéticos em infraestruturas críticas. A Diretiva SRI 2 representa um marco, bem como uma referência para a gestão do risco e para a notificação obrigatória de incidentes em todos os setores abrangidos. O seu objetivo consiste em harmonizar as medidas de segurança entre os Estados-Membros, estabelecendo regras mínimas, mecanismos de cooperação, atualizando a lista de setores e atividades sujeitas a obrigações de cibersegurança e prevendo sanções em caso de incumprimento das orientações.

Para garantir a implementação eficaz da Diretiva SRI 2, foi criada a Rede Europeia de Organizações de Coordenação de Cibercrises (EU-CyCLONe), com o objetivo de coordenar a resposta a incidentes e crises de cibersegurança de grande escala (ENISA, 2024). A proteção das infraestruturas críticas face a ameaças cibernéticas exige uma atuação articulada ao nível da prevenção, deteção e resposta. A missão da EU-CyCLONe consiste em facilitar a coordenação entre os Estados-Membros a nível político e estratégico durante situações de crise, promovendo a partilha de informação, boas práticas e decisões rápidas e coordenadas. Esta rede coopera também com outras entidades relevantes, como a ENISA (Agência da União Europeia para a Cibersegurança), a CSIRTs Network (Computer security Incident Response Team Network), a Europol e a Comissão Europeia. O organismo ENISA tem como principais responsabilidades apoiar os Estados-Membros na implementação de políticas eficazes de cibersegurança, incluindo a aplicação da Diretiva SRI 2 (ENISA, 2024). A agência desenvolve

relatórios regulares sobre ameaças e tendências cibernéticas (ENISA *Threat Landscape*) e promove a formação de profissionais através de programas específicos e exercícios de simulação a nível europeu, como o *Cyber Europe*. Para além disso, a ENISA assume ainda um papel central na certificação da segurança digital, através do Quadro Europeu de Certificação em Cibersegurança. A CSIRTs *Network*, ao contrário da EU-CyCLONe que atua a nível político-estratégico, foca-se na cooperação técnica entre os Estados-Membros. A sua missão passa por reforçar a troca de informações em tempo real sobre incidentes e ameaças significativas, assegurando uma resposta mais eficaz a nível técnico-operacional (ENISA, 2024).

Em Portugal, o Centro Nacional de Cibersegurança (CNCS) é a entidade responsável pela coordenação da cibersegurança a nível nacional (CNCS, 2024). O seu objetivo é garantir a resiliência das infraestruturas críticas e dos serviços essenciais, supervisionando a implementação da Diretiva SRI 2 junto dos operadores dos setores como energia, saúde e transportes, bem como dos prestadores de serviços digitais. Entre as suas iniciativas destacam-se o Exercício Ciber Perseu (simulação nacional de cibercrises), a Escola Nacional de Cibersegurança (formação de especialistas em segurança digital) e o Observatório de Cibersegurança (recolha e análise de dados sobre o estado da cibersegurança em Portugal) (CNCS, 2024).

4.3. Impacto das tecnologias emergentes

As tecnologias emergentes, como a Inteligência Artificial (IA), a Internet das Coisas (IoT), a computação quântica e o 5G transformaram profundamente a gestão das infraestruturas críticas. Estas inovações permitiram melhorar significativamente a eficiência e a rapidez da gestão das infraestruturas, no entanto, também introduziram novos riscos e desafios no domínio da cibersegurança. A IA, por exemplo, permite detetar ameaças através de sistemas avançados de análise, mas pode igualmente ser utilizada como instrumento de ataque (Ekonomista, 2024; CISO Advisor, 2024). A IoT, embora beneficie setores como a energia, a saúde e os transportes ao possibilitar o controlo remoto e a monitorização em tempo real, expõe-se a vulnerabilidades quando não acompanhada de medidas de segurança robustas (EPS Programming, 2023). A tecnologia 5G, ao expandir a largura de banda e potenciar a conectividade, aumenta igualmente a superfície de ataque cibernético (Kaspersky, n.d.; CompuLab, 2024a). Por fim, a computação

quântica, apesar do seu potencial revolucionário ao nível da encriptação e do processamento de dados, pode vir a representar uma ameaça à segurança de dados caso seja explorada para fins maliciosos (CompuLab, 2024b; MIT Technology Review Portugal, 2024).

5. Desafios e Caminhos Futuros

5.1 Barreiras técnicas, políticas e operacionais

A necessidade de encontrar soluções para os dilemas impostos pelos desafios emergentes abordados ao longo deste trabalho é urgente. As novas tecnologias são uma área complexa onde, quando nos apercebemos das suas consequências e de que forma regulá-las, outras mais avançadas já foram postas em prática. Sendo assim, a União Europeia encontra muitas barreiras para a proteção legal e técnica de suas infra-estruturas face às tecnologias disruptivas. Simultaneamente, abordagens demasiado reducionistas ou exageradas podem resultar em políticas desajustadas à realidade (Valeriano, Maness, 2018, p. 262), o que torna importante a procura pelo equilíbrio entre estas perspetivas.

Primeiramente, é necessário compreender que as ações integradas da União Europeia devem estar inseridas num quadro legal, que por si só é difícil de ser definido, pois envolve os interesses de uma multiplicidade de atores, não só estatais como também privados. Algumas questões a serem debatidas no âmbito jurídico são a adequação de modelos tradicionais de controlo governamental, a possibilidade de aplicar jurisdições atuais a meios digitais, e como resolver possíveis conflitos entre legislações internacionais (Bechara et al, 2021. p. 360).

A União Europeia, no seu Plano para a Cibersegurança e Estratégias Nacionais, reconhece a complexidade de conciliar a soberania com poderes centrais e responsabilidades. O ciberespaço, enquanto domínio de operação, é passível de ser submetido às leis dos conflitos armados, levantando questões relevantes no âmbito da ciberdefesa, especialmente no que toca às ameaças híbridas e às suas relações com os atores civis e militares. Adicionalmente, deve-se refletir sobre o papel da União Europeia na criação das ciber normas. Acima de tudo, coloca-se em questão a possibilidade da criação destas normas num espaço digital transfronteiriço que desafia lógicas soberanas e implica o envolvimento de milhares de atores com perspetivas

diferentes, que dificilmente concordariam com a imposição de normas universais para o ciberespaço e as novas tecnologias.

Para além da necessidade de cooperação nas políticas digitais e para as tecnologias disruptivas, alguns outros campos políticos intersectam-se com estes desafios e tornam ainda mais complexa a sua resolução. Por exemplo, agendas transnacionais como a corrupção, a lavagem de dinheiro e o crime organizado, estão intimamente ligadas à agenda da cibersegurança, e, por isso, uma abordagem completa para a regulação deste tópico deve também ter em consideração algumas conexões não óbvias.

Outro desafio imposto à resiliência digital da União Europeia é a atuação no ciberespaço de atores não-estatais. Os Estados, ao mesmo tempo que dificilmente reconhecem autoridades acima deles próprios, também compreendem a necessidade de participação estratégica em organismos internacionais que coordenam políticas comuns. Isto faz com que estejam dispostos a adotar regulações coordenadas no âmbito digital, que impõem certos limites a estas atividades. Contudo, os atores privados ou não-tradicionais com quem lidam não têm necessariamente de respeitar políticas de regulação, entre outras, o que causa uma assimetria de poder e torna mais complexa a capacidade de reação dos Estados às novas ameaças digitais.

5.2 Reflexões para reforçar a soberania e a resiliência digital

Ao longo da história, algumas estratégias foram delineadas para tentar reforçar a soberania e a resiliência da União Europeia. Porém, a maioria apresentou falhas estruturais, visto que concentravam os esforços em criar planos de ação que complementavam leis locais já existentes, mas não reforçavam mecanismos de diálogo constante entre os países, um dos fatores considerados mais importantes para a ciberdefesa (Bechara, Schuch, 2021). Esta troca de comunicação poderia favorecer, por exemplo, a partilha de informações e a aquisição de conhecimento sobre determinadas investigações, de maneira a elevar o nível técnico de discussão sem necessidade de repetir trabalhos. Para isto, é necessário manter uma relação de confiança e políticas equitativas, de forma que mais países membros sintam-se integrados ao diálogo e queiram aderir a possíveis políticas conjuntas.

A estrutura supranacional da União Europeia já facilita esta relação estratégica. Contudo, o processo para aumentar a resiliência digital não pode ser feito abruptamente sem encontrar alguma resistência dos Estados, pois eventuais propostas de defesa devem contar com o facto de que cada membro deseja regular as políticas aplicadas de acordo com seus contextos políticos, económicos e sociais. Com isso em consideração, cabe à União Europeia fomentar uma cultura de cibersegurança comum, para que estas práticas se infiltrem nas estruturas dos Estados como prioritárias, e de maneira a elevar o debate sobre o tópico. Isto é válido não só numa perspetiva técnica, mas como um assunto que deve constar em todos os níveis da sociedade: desde a educação básica à superior, aos diversos níveis de diálogo governamental. Visto serem desafios emergentes que afetam também a sociedade civil, é fundamental que esta apoie e exija dos seus governantes a implementação de políticas eficazes de cibersegurança e defesa.

Para além da sociedade civil, a União Europeia deve cada vez mais fortalecer a sua resiliência digital também em sintonia com o setor privado. Apesar deste representar um desafio, como visto no subtópico anterior, não deixa de ser indispensável para o desenvolvimento de novas e atuais políticas de cibersegurança. Um bom exemplo a ser fortalecido são as Parcerias Público-Privadas (PPPs) entre empresas e autoridades estatais, consideradas boas ferramentas de cooperação (Bechara, Schuch, 2021). No domínio da cibersegurança, estas parcerias podem compartilhar informações, desenvolver tecnologias de defesa, realizar gestões de crise conjuntas e colaborar para a proteção de infraestruturas críticas. Além disso, se bem implementadas, podem ser grandes aliadas na concretização de alguns objetivos da estratégia de cibersegurança da União Europeia, como a redução do cibercrime, o reforço das capacidades industriais de ciberdefesa e a inclusão mais abrangente deste tópico na Política Comum de Segurança e Defesa (PCSD).

5.3. Perspetivas para a segurança digital na UE

A partir da presidência de Ursula Von der Leyen na Comissão Europeia, a União Europeia deixou claro que a "soberania digital" seria uma das prioridades da governação europeia em relação às novas tecnologias para os próximos anos (Bellanova et al, 2022). Com isto, tem sido crescente o desejo em controlar, ou supervisionar, as ferramentas digitais europeias, em oposição a uma abordagem mais flexível que abre espaço para o controlo de

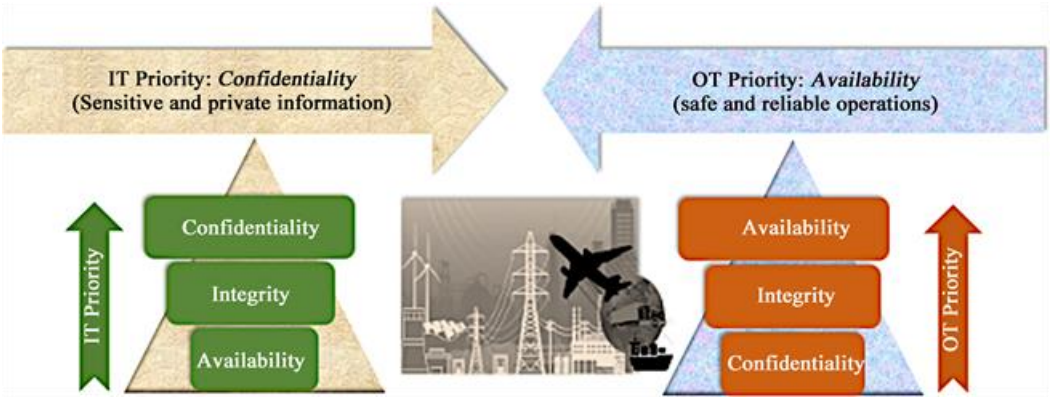
atores não estatais. Sendo assim, a Comissão Europeia tem-se apoiado neste desejo pela soberania digital, ao desenvolver as capacidades de resiliência europeias, o que incluiu diminuir a dependência de alguns serviços e atores externos, como: operadores de serviços e infraestruturas (Madiega, 2020) e fontes de recursos naturais necessários para operar serviços de cibersegurança (DeCarlo, Goodman, 2022).

Outro conceito que continuará a ser fortemente avançado nos próximos anos são as "ameaças híbridas", no sentido em que há uma sobreposição das ameaças *cyber* e as ameaças físicas, e o ciberespaço pode ser um meio através do qual atores hostis ataquem a União Europeia, por exemplo através da desinformação ou de danos a infraestruturas críticas de comunicação. Este é o caso na atual guerra na Ucrânia, na qual, segundo o CERT-EU (*Computer Emergency Response Team for the EU Institutions, Bodies and Agencies*), foram detetadas atividades *cyber* russas contra países europeus (CERT-EU, 2023, p. 3). As ameaças híbridas na forma de ciberataques também são cada vez mais preocupantes mediante a utilização das tecnologias emergentes de Inteligência Artificial, que impulsionam as capacidades ofensivas de ataques de engenharia social, do phishing, e da identificação de vulnerabilidades na cibersegurança (CERT-EU, 2023, p. 4). Por isso, a União Europeia também pretende avançar políticas de regulação e gestão da Inteligência Artificial, sendo um exemplo o AI Act.

As ameaças híbridas também representam um risco para outras infraestruturas críticas além das de comunicação, como os setores hospitalares, energéticos e de administração pública, que, cada vez mais digitalizados, são vulneráveis a possíveis ataques cibernéticos. Contudo, é comum que a proteção das Tecnologias Operacionais (OT) seja menos valorizada que a proteção das Tecnologias de Informação (IT). Esta é uma situação que deve ser revista pelos sistemas de segurança da União Europeia, visto que danos realizados através do espaço ciber a infraestruturas críticas podem ocasionar consequências muito graves, como afetar o funcionamento de geradores, transformadores, redes elétricas em geral, distribuição de gás, e até mesmo a integridade física da população. Diferentemente da proteção às IT, cujo um dos focos principais é garantir a confidencialidade do sistema e a proteção de dados, as OT também exigem um cuidado reforçado em suas infraestruturas materiais, de modo a garantir que as operações físicas decorram de maneira segura. A cibersegurança possui um papel imprescindível nesta proteção, e a União Europeia deve reforçar a capacidade dos Estados

Membros preverem vulnerabilidades e ameaças em suas infraestruturas críticas a partir das Tecnologias de Informação

Figura 2: Prioridades das Tecnologias de Informação e Tecnologias Operacionais (Roshanaei, 2021).



Finalmente, outra ferramenta para a cibersegurança que a União Europeia pretende reforçar é o seu papel como exportadora de normas e princípios que valorizam a cibersegurança, de modo a promover esta visão globalmente e, por conseguinte, aumentar a sua proteção contra ciberataques (Carrapico, Farrand, 2024, p . 153). Neste âmbito, é interessante analisar a ciber-diplomacia realizada pela União, que busca promover *standards* comuns para a cibersegurança e tornar-se uma liderança global estabelecida neste assunto, com base em valores democráticos do Estado de direito e nos direitos individuais. Para isso, é de esperar que a União Europeia insista em demonstrar a ligação da cibersegurança com outras políticas digitais, aumentar sua participação em mecanismos multilaterais que discutem este assunto, e continuar a expandir suas relações bilaterais e regionais, o que pode até mesmo ter *spillover effects* no aprofundamento da integração europeia.

6. Conclusão

6.1 Síntese da análise

Ao longo deste trabalho, foi possível acompanhar como os conceitos de soberania digital e cibersegurança deixaram de estar confinados a círculos técnicos ou especializados,

passando a ocupar um lugar central no debate político europeu. A transformação digital alterou não apenas os modos de organização socioeconómica, mas também as próprias categorias com que pensamos a autonomia e segurança.

A União Europeia tem procurado afirmar-se neste novo cenário através de um conjunto articulado de estratégias que combinam tanto legislação e investimento, como estrutura institucional preparada para tal. Ferramentas como o RGPD, o AI Act ou o Digital Services Act não são apenas instrumentos regulatórios, representam também tentativas conscientes de moldar um modelo europeu num espaço digital muitas vezes dominado por lógicas e valores externos. Ainda assim, percebemos que a resposta não pode assentar unicamente em normas jurídicas, a execução e a inovação continuam a depender de recursos materiais, de competências humanas e de uma visão partilhada entre os vários atores envolvidos.

A proteção das infraestruturas críticas revelou-se, nesse sentido, uma área especialmente sensível. Os casos analisados demonstraram que as ameaças cibernéticas não são apenas potenciais, são frequentes e cada vez mais sofisticadas, difíceis de prever e com consequências reais. Mais do que uma questão tecnológica, estamos perante uma vulnerabilidade transversal que coloca à prova a capacidade de articulação entre Estados-Membros, agências europeias, setor privado e sociedade civil.

A abordagem aos desafios e caminhos futuros destacou precisamente essa complexidade. O digital é hoje um domínio simultaneamente técnico, político, económico e simbólico. Falar de soberania digital na UE é reconhecer tensões profundas entre a necessidade de independência estratégica e a interdependência inevitável num mundo globalizado e tecnologicamente assimétrico. O que se evidencia, acima de tudo, é que a União Europeia está ainda num processo de construção neste novo território.

6.2 Considerações finais e reflexões futuras

Pretende-se que este trabalho não seja apenas uma descrição das estratégias da União Europeia para o digital, mas a consciência de que a construção da soberania digital exige escolhas difíceis, coerência política e compromisso a longo prazo. Há avanços reais, sobretudo no plano normativo, mas há também zonas de desajuste entre o que está previsto e o que é executado na prática.

Um dos pontos que se tornou particularmente claro é a necessidade de tornar esta transição digital mais equilibrada dentro da própria União. A disparidade de meios entre Estados-Membros compromete a eficácia das medidas comuns e fragiliza a segurança do conjunto. A utilização inteligente de instrumentos como o Fundo Europeu de Desenvolvimento Regional pode fazer a diferença, não apenas pelo financiamento de infraestruturas, mas pela possibilidade de gerar competências, atrair investimento tecnológico local e consolidar capacidades institucionais onde elas são mais frágeis.

Ao longo da investigação, ficou evidente que a resposta à complexidade digital não pode depender apenas de grandes planos ou de estruturas técnicas sofisticadas. Muitas das falhas que ameaçam a cibersegurança resultam da descoordenação entre níveis de decisão ou da falta de formação adequada em setores estratégicos. A resposta precisa, por isso, de ser pensada de forma integrada não apenas do topo para a base, mas através de circuitos de comunicação e responsabilidade mais ágeis e consistentes.

A inovação deve ser encarada não como fim em si mesma, mas como um meio para antecipar riscos, melhorar respostas e reforçar a autonomia da UE. Modelos de deteção precoce, interoperabilidade real entre sistemas públicos e privados, e avaliação contínua das vulnerabilidades são caminhos possíveis que merecem ser pensados mais seriamente. Mas tudo isso exige clareza de objetivos, vontade política e capacidade de coordenação institucional.

Outro ponto que não pode ser ignorado é o da proximidade com os cidadãos. O discurso sobre o digital continua a ser pouco acessível e distante da realidade de grande parte da população. Esta distância contribui para a sua passividade, e, em última análise, para a fragilidade da própria soberania que se pretende construir. É necessário que a política digital europeia seja também um projeto comunicável e partilhável não apenas por quem a concebe, mas por quem dela depende.

É neste ponto que o nosso trabalho encontra a sua linha de chegada: a soberania digital europeia não se esgota na proteção de sistemas, mas passa pela capacidade de transformar o digital num espaço seguro, partilhado e verdadeiramente europeu. Isso implica investimento, mas também visão e sobretudo, disposição para reconhecer que o digital é, hoje, um terreno

político em disputa, e que a forma como a UE responde a essa disputa definirá o seu papel no mundo.

Bibliografia

Alcaraz, C., Zeadally, S. (2014). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8(4), 53-66.

Bechara, F., Schuch, S. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, 28(29), 359-374.

Bedingfield, W. (2020). Europe Has a Plan to Break Google and Amazon's Cloud Dominance. *Wired UK* https://www.wired.co.uk/article/europe-gaia-x-cloud-amazon-google

Borrell, J. (2020). *Os motivos pelos quais a autonomia estratégica europeia é importante* |

EEAS. European Union External Action.

https://www.eeas.europa.eu/eeas/os-motivos-pelos-quais-autonomia-estrat%C3%A9gica-europeia-%C3%A9-importante_pti

Briggs, B. (2019). Hackers Hit Norsk Hydro with Ransomware. The Company Responded with Transparency. *Microsoft News*. https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

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. *JCMS Journal of Common Market Studies*, *61*(5), 1261–1280. https://doi.org/10.1111/jcms.13462

Burwell, F. G., & Propp, K. (2020). *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?* Atlantic Council. http://www.jstor.org/stable/resrep26697

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43–62.

Celeste, E. (2021). Digital Sovereignty in the EU: Challenges and Future Perspectives. *School of Law & Government, Dublin City University*.

Centro Nacional de Cibersegurança (CNCS). (2023). Relatório Tecnologias Emergentes, https://www.cncs.gov.pt/docs/rel-tecemer2023-observ-cncs.pdf

Centro Nacional de Cibersegurança (CNCS). (2024). Exercício Nacional de Cibersegurança. https://www.cncs.gov.pt/pt/exercicio-nacional-ciberseguranca/

Centro Nacional de Cibersegurança (CNCS). (2024). Observatório de Cibersegurança. https://www.cncs.gov.pt/pt/observatorio/

CERT-EU. (2023). Russia's War on Ukraine: One Year of Cyber Operations – 24 February 2022–24 February 2023. *CERT-EU*. https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Christou, G. (2014). Cybersecurity in the European Union: Resilience and adaptability in governance policy. *Palgrave Macmillan.*

CISCO Systems. (2010). Cybersecurity: Everyone's Responsibility. https://www.nist.gov/system/files/documents/2017/01/25/kparra_cybersecurity-responsibility.pdf

Comissão Europeia. (2022). *A guide to EU funding opportunities to digitalise businesses*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/guide-eu-funding-opportunities-digitalise-businesses

Comissão Europeia. (2020 janeiro 23). Cibersegurança das redes 5G – Caixa de ferramentas da UE para medidas de mitigação de riscos. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

Comissão Europeia. (2025). A Estratégia para a Cibersegurança. https://digital-strategy.ec.europa.eu/pt/policies/cybersecurity-strategy

Comissão Europeia (s.d.). Europe's digital decade: 2030 targets https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

Comissão Europeia. (2023). *O Programa Europa Digital | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/pt/activities/digital-programme

Comissão Europeia. (n.d.). *Regulamento Circuitos Integrados*. Commission.europa.eu. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_pt

CompuLab. (2024). Cibersegurança Quântica: Qual a ameaça à segurança dos dados?. https://www.compulab.pt/blog/ciberseguranca-quantica-o-impacto-da-computacao-quantica-na-criptografia-e-na-protecao-de-dados/

CompuLab. (2024). Impacto do 5G na Cibersegurança: Novas Oportunidades e Riscos. https://www.compulab.pt/blog/o-impacto-do-5g-na-ciberseguranca-novas-oportunidades-e-riscos/

Conselho da União Europeia. (2025, maio 27). Como está a UE a reforçar a sua cibersegurança. https://www.consilium.europa.eu/pt/policies/cybersecurity/.

Conselho da União Europeia. "Como a UE está a reforçar a sua cibersegurança." https://www.consilium.europa.eu/en/policies/cybersecurity/.

DeCarlo, S. Goodman, S. (2022). Russia, Palladium, and Semiconductors. *US International Trade Commission.*

Deibert, R. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy*, 30(1), 25–39.

EDRI. (2023). *EU Digital Decade - European Digital Rights (EDRi)*. European Digital Rights (EDRi). https://edri.org/our-work/missing-peoples-rights-in-the-eu-digital-decade/

Ekonomista. (2024). O Impacto da Inteligência Artificial na Cibersegurança. https://www.e-konomista.pt/o-impacto-da-inteligencia-artificial-na-ciberseguranca/

ENISA. (2023). ENISA Threat Landscape 2023. *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Commission (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 Final, Brussels, Belgium.

European Commission. (2020). Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/shaping-europes-digital-future.

European Commission. (2021). 2030 Digital Compass: The European Way for the Digital Decade. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0118

European Commission. (2024). *Data Act | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/data-act

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2018). Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats. *JOIN (2018) 16.*

European External Action Service (EEAS). (2016). Shared Vision, Common Action: A Stronger Europe – *A Global Strategy for the European Union's Foreign and Security Policy.* https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf

European Medicines Agency (EMA). (2021). Cyberattack on EMA – Update 5. https://www.ema.europa.eu/en/news/cyberattack-ema-update-5.

European Parliament. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). https://eur-lex.europa.eu/eli/dir/2022/2555/oj

European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, 33, 369-378.

Geraldes, S. (2019). A Estratégia de Cibersegurança da União Europeia: Catastrofista, Realista e/ou Otimista?. *IDN: Nação e Defesa*, 154, 91-108.

Gonçalves, E. (2024). IA, nova fronteira na proteção de infraestrutura crítica. *CISO Advisor*. https://www.cisoadvisor.com.br/security-room-posts/ia-nova-fronteira-na-protecao-de-infraestrutura-critica/

Goutam, R. (2015). Importance of Cyber Security. Department of Computer Science, University of Lucknow. *International Journal of Computer Applications*, 111(7), 14-17.

Hinsley, FH. (1986). Sovereignty, *Cambridge University Press.*

IRM. (2015). Amateyrs attack technology. Professional hackers target people. www.irmplc.com/issues/human- behaviour.

Kaspersky. (n.d.). 5G e cibersegurança: tudo o que você precisa saber. https://www.kaspersky.com.br/resource-center/threats/5g-pros-and-cons

Kitchen, M. (2023). Compreendendo os Riscos e Regulamentações da Segurança da Internet das Coisas. *EPS Programming*. https://www.epsprogramming.com/pt-br/blogue/compreendendo-os-riscos-e-regulamentacoes-da-seguranca-da-internet-das-coisas/

Latici, T. (2020). Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence. *European Parliamentary Research Service.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf

Lipson, H. (2002). Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. *Carnegie Mellon Software Engineering Institute, Special Report.*

Litvinski, O. (2018). Emerging Technology: Toward a Conceptual Definition International Journal of Trade. *Economics and Finance*, 9(6).

LogAP (2025). *Resiliência digital: o que é e como fortalecer sua estratégia.* https://logap.com.br/blog/resiliencia-digital

Lomas, N. (2024). *Uber fined $324M over EU drivers' data transfer breach.* TechCrunch. https://techcrunch.com/2024/08/26/uber-fined-324m-over-eu-driver-data-transfer-breach/

Luca Belli, Bruna Franqueira, Erica Bakonyi, Larissa Chen, Natalia Couto, Sofia Chang, Nina da Hora e Walter B. Gaspar (2023) Cibersegurança: uma visão sistémica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano – Rio de Janeiro : FGV Direito Rio, 2023.

Madiega, T. (2020). Digital Sovereignty for Europe. *European Parliamentary Research Service, European Parliament*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Miron, D., Ionel, E.S. & Belciu, A.C. (2024). An Analysis of the Digital Resilience Challenge for Implementing EU Programs and Instruments. Proceedings of the International Conference on Business Excellence, 18(1), 2024. 321-334. https://doi.org/10.2478/picbe-2024-0028

Motha, S. (2008). Sovereignty. *The New Oxford Companion to Law, Oxford University Press* https://www.oxfordreference.com/view/10.1093/acref/9780199290543.001.0001/acref-9780199290543-e-2052>

Nehme, Marcos. (2024). Cibersegurança na Computação Quântica: navegar o novo horizonte. *MIT Technology Review Portugal*.

https://www.mittechreview.pt/2024/computacao/ciberseguranca-computacao-quantica-novo-horizonte/

Observador. (2023). Empresa de transportes Barraqueiro alvo de ciberataque. https://observador.pt/2023/01/10/empresa-de-transportes-barraqueiro-alvo-de-ciberataque/

Parlamento Europeu. (2023). Lei da UE sobre IA: primeira regulamentação de inteligência artificial. Temas | Parlamento Europeu. https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial

Parlamento Europeu. (2021). *A Lei dos Mercados Digitais e da Lei dos Serviços Digitais da UE explicadas | Temas | Parlamento Europeu*. Www.europarl.europa.eu. https://www.europarl.europa.eu/topics/pt/article/20211209STO19124/a-lei-dos-mercados-digitais-e-da-lei-dos-servicos-digitais-da-ue-explicadas

Parlamento Europeu e Conselho da União Europeia. (2016). *Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação na União*. Jornal Oficial da União Europeia L 194. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.

Parlamento Europeu e Conselho da União Europeia. (2022). *Diretiva (UE) 2022/2555, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2)*. Jornal Oficial da União Europeia L 333, 80–152. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555.

Parlamento Europeu e Conselho da União Europeia. (2022) *Regulamento (UE) 2022/1925 Do Parlamento Europeu e do Conselho de 14 de setembro de 2022 relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais).* Jornal Oficial da União Europeia L 265/1 Regulation - 2022/1925 - EN - EUR-Lex

Pohle, J. (2020). Digital sovereignty. A new key concept of digital policy in Germany and Europe. *Konrad-Adenauer-Stiftung,* Berlin. https://www.kas.de/en/web/guest/single-title/-/content/digitale-souveraenitaet

Politico Europe. (2021). Cyberattack on EMA reveals vulnerabilities in EU agencies. https://www.politico.eu/article/ema-cyberattack-reveals-eu-vulnerabilities/

Público. (2022). Ataque informático paralisa serviços do Centro Hospitalar de Lisboa Ocidental. https://www.publico.pt/2022/08/26/sociedade/noticia/ataque-informatico-paralisa-servicos-centro-hospitalar-lisboa-ocidental-2018432

Reuters. (2025). TikTok fined 530 million euros by EU regulator over data protection. *Reuters*. https://www.reuters.com/sustainability/boards-policy-regulation/tiktok-fined-530-million-euros-by-eu-regulator-over-data-protection-2025-05-02/

Roshanaei, M. (2021). Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies. *Journal of Computer and Communications,* 9(8), 80-102.

Svantesson, D. (2014). Sovereignty in International Law: How the Internet (Maybe) Changed Everything, but Not for Long. *Masaryk University Journal of Law and Technology*, 8(1), 137-155.

Syaifuddin, S. N., Sumarwan, U., & Simanjuntak, M. (2024). The role of digital transformation in enhancing organizational resilience: Dynamic capabilities as mediators. *Journal of Innovation and Entrepreneurship,* 13(1). https://doi.org/10.1186/s13731-024-00405-4

TiSafe. (2024). Tendências de cibersegurança em infraestruturas críticas 2025. https://tisafe.com/tendencias-de-ciberseguranca-em-infraestruturas-criticas-2025/

United Nations Office on Drugs and Crime (UNODC). (2012). The use of the Internet for terrorist purposes. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf