OBSERVARE
Universidade Autónoma de Lisboa
e-ISSN: 1647-7251
VOL. 16, Nº. 2, TD4
Thematic Dossier
European Union Security Governance: from Integration to Strategic Autonomy
Abril 2026

JANUS.NET
e-journal of International Relations

POLÍTICA DE GESTÃO DE DADOS DA UNIÃO EUROPEIA: AMEAÇAS E DESAFIOS À SEGURANÇA DIGITAL

ANTÓNIO PEDRO BOGAS BARROSO
pedrobogasbarroso@gmail.com
Aspirante a Oficial Aluno no Mestrado Integrado na Especialidade de Piloto Aviador. Centro de Investigação da Academia da Força Aérea, Academia da Força Aérea, Instituto Universitário Militar (Portugal). ORCID: 0009-0007-0836-1061

ÉLIA CHAMBEL
eliachambel@gmail.com
Oficial da PSP (Portugal). Doutora em Relações Internacionais, Mestre em Ciência Política e Relações Internacionais e Licenciada em Ciências Policiais. Docente em várias instituições com destaque para o Instituto Superior de Ciências Policiais e Segurança Interna. ORCID: 0009-0005-8616-7470

TIAGO LUÍS CARVALHO
tiagoluiscarvalho13@gmail.com
Professor na Academia da Força Aérea (Portugal). Doutorado em Relações Internacionais e Pós-Graduado em Direito da União Europeia. Investigador do Instituto do Oriente, Instituto Superior de Ciências Sociais e Políticas, Universidade de Lisboa e do Centro de Investigação da Academia da Força Aérea, Academia da Força Aérea, Instituto Universitário Militar (Portugal). ORCID: 0000-0003-3486-9794

Resumo

Os dados pessoais são um ativo de grande valor. A disputa pelo controlo de dados tornou-se uma competição global, em que o acesso e o domínio sobre esses recursos oferecem vantagens económicas, estratégicas e geopolíticas substanciais. O papel estratégico dos dados é especialmente relevante para a União Europeia, que procura equilibrar o incentivo à inovação com a preservação dos seus valores democráticos e da sua soberania digital. Neste contexto, é imperativo assegurar políticas de gestão de dados claras e robustas, assegurando não apenas a privacidade, mas também protejam contra abusos de terceiros, garantindo assim a soberania e a segurança de Estados e cidadãos. Para abordar a complexa dinâmica digital, o presente estudo centra-se na análise das legislações adotadas pela União Europeia no domínio da gestão de dados entre 2016 e 2024. Procura-se, igualmente, compreender as possíveis consequências de uma gestão inadequada dos dados num cenário global marcado pela interdependência digital e por disputas geopolíticas, considerando o caso de Portugal e das suas Forças Armadas. Este estudo adota uma abordagem metodológica qualitativa, baseada na análise documental e em entrevistas semiestruturadas. Para delimitar o estudo, formulou-se a seguinte pergunta de partida: "Qual o impacto das políticas de gestão de dados da União Europeia na sua segurança digital?". Para reduzir a amplitude do tema, derivaram-se duas perguntas: (1) "Quais os fatores que afetam a segurança digital da União Europeia?"; e (2) "Estas políticas afetam as Forças Armadas Portuguesas?". Os resultados indicam que as políticas de gestão de dados da União Europeia influenciaram diretamente a sua segurança digital e promoveram uma abordagem ética e inovadora que protege os direitos dos cidadãos e a democracia. No entanto, para enfrentar as rápidas mudanças tecnológicas e as crescentes

ameaças, é necessário reforçar a colaboração internacional, investir em tecnologias emergentes e promover a literacia, assegurando um ambiente digital resiliente e inclusivo.

Palavras-chave

Governação de dados, Dados Pessoais, Política de Gestão de Dados, Segurança Digital, União Europeia.

Abstract

Personal data is a highly valuable asset. The competition for data control has become a global rivalry in which access to, and dominance over, these resources result in significant economic, strategic, and geopolitical advantages. The strategic role of data is particularly relevant for the European Union, which seeks to balance incentives for innovation with the preservation of its democratic values and digital sovereignty. In this context, it must ensure clear and robust data management policies that safeguard not only privacy but also provide protection against third-party abuses, thereby guaranteeing the sovereignty and security of its Member States and citizens. To address the complexity of the digital environment, this study focuses on the analysis of the European Union legislation on data management between 2016 and 2024. It also seeks to understand the potential consequences of inadequate data management in an international environment marked by digital interdependence and geopolitical disputes, using the case of Portugal and its Armed Forces. This study adopts a qualitative methodological approach, combining documentary analysis and semi-structured interviews. The guiding research question is: "What is the impact of European Union data management policies on its digital security?". To narrow the scope, two sub-questions were derived: (1) "Which factors affect the European Union's digital security?"; and (2) "Do these policies affect the Portuguese Armed Forces?". The results indicate that European Union data management policies have directly influenced its digital security and have promoted an ethical and innovation-driven approach that protects citizens' rights and democracy. However, to respond to rapid technological change and growing threats, it is necessary to strengthen international cooperation, invest in emerging technologies, and promote literacy, ensuring a resilient and inclusive digital environment.

Keywords

Data governance, Personal data, Data management policy, Digital security, European Union.

Como citar este artigo
Barroso, António Pedro Bogas, Chambel, Élia & Carvalho, Tiago Luís (2026). Política de Gestão de Dados da União Europeia: Ameaças e Desafios à Segurança Digital. *Janus.net, e-journal of international relations*. Thematic Dossier - European Union Security Governance: from Integration to Strategic Autonomy, VOL. 16, Nº. 2, TD4, Abril 2026, pp. 23-41. https://doi.org/10.26619/1647-7251.DT03226.2

Artigo submetido a 23 de novembro de 2025 e aceite para publicação a 18 de fevereiro de 2026.

POLÍTICA DE GESTÃO DE DADOS DA UNIÃO EUROPEIA: AMEAÇAS E DESAFIOS À SEGURANÇA DIGITAL

ANTÓNIO PEDRO BOGAS BARROSO

ÉLIA CHAMBEL

TIAGO LUÍS CARVALHO

Introdução

Este estudo insere-se na disciplina das Relações Internacionais e propõe uma análise aprofundada das dinâmicas contemporâneas relacionadas com a gestão de dados na era digital. Centra-se na importância crescente atribuída às políticas de gestão e proteção de dados pela União Europeia e por outros atores globais. Com a expansão da livre circulação de informação e do surgimento de desafios em torno da segurança digital, estas políticas tornam-se um elemento crucial para garantir privacidade, defesa e soberania no cenário internacional (British Academy & Royal Society, 2017).

O estudo oferece uma contextualização que destaca o papel cada vez mais importante do mundo digital nos conflitos atuais, onde este se caracteriza como um espaço essencial para a obtenção de vantagens militares, comerciais e estratégicas. O aumento exponencial das ameaças cibernéticas coloca a proteção de dados no centro das preocupações estatais, evidenciando a necessidade de estratégias integradas e de cooperação em cibersegurança para mitigar os riscos associados (Sambaluk & Spafford, 2020).

O domínio digital tem uma utilização crescente e os indivíduos dependem dele para realizar as tarefas quotidianas expondo os seus dados pessoais. Destaca-se o exemplo das finanças digitais (Rodima-Taylor, 2024). Os indivíduos devem possuir um conhecimento mínimo acerca dos seus direitos e deveres de modo a proteger a sua vida pública e privada, os dados mais frequentemente recolhidos estão diretamente ligados à segurança e à saúde, o que pode tornar-se uma preocupação não só para o indivíduo, mas também para o Estado (Kazemi *et al.*, 2023).

O aumento de ataques a bases de dados evidencia a sua importância como meio para conseguir um ambiente estável e resiliente. São exemplos destes ataques, os incidentes

que afetaram a Biostar 2 e a Air Europa em 2019 e 2023 respetivamente, que tiveram um grande impacto ao serem alvos de ciberataques, tendo sido roubados diversos dados pessoais, desde métodos de pagamento até dados biométricos. Uma gestão de dados eficaz é central para a soberania digital e possui uma influência direta nas relações entre Estados (Hummel *et al.*, 2021).

A tecnologia tem avançado a um nível sem precedentes nestes últimos anos e devido a este fator surgiu a necessidade da cibersegurança como meio de salvaguardar não só dos direitos humanos, mas também do bom funcionamento desta estrutura digital. O desenvolvimento deste domínio levou à criação de várias entidades, como a Agência da União Europeia para a Cibersegurança (ENISA) e o Centro Europeu de Cibercrime (EC3) da Europol, com o objetivo de proteger os cidadãos contra atos terroristas e garantir que não ocorram roubos de bases de dados garantindo a privacidade, segurança e o cumprimento das normas (Kazemi *et al.*, 2023).

Para garantir um desenvolvimento seguro da sociedade, é essencial que as bases de dados não sejam corrompidas ou manipuladas de forma ilícita, o que implica que se observem os três pilares da cibersegurança: confidencialidade, integridade e disponibilidade. O cumprimento destes três pontos é essencial para garantir que não existem falhas e de forma a criar um ambiente digital resiliente e íntegro (Kumar & Bhatia, 2020).

Neste quadro, a gestão de dados na União Europeia apresenta-se como uma problemática multidimensional, cuja análise requer uma articulação rigorosa entre diferentes níveis de análise. Assim, as secções seguintes explicam as opções metodológicas adotadas (secção 2) e enquadram, de modo sistemático, a literatura científica (secção 3), as políticas europeias relevantes (secção 4) e os riscos e ameaças associados (secção 5), preparando a análise do caso português (secção 6). A sétima secção expõe as conclusões, as recomendações e as limitações desta investigação.

Metodologia

Este estudo tem como objeto as políticas de gestão de dados da União Europeia. Procede-se também à identificação das ameaças neste campo, incluindo o impacto da má gestão de dados, de modo a compreender as políticas e reforçar a resiliência digital da União Europeia. Como limite temporal, definiu-se o período entre 2016 e 2024, que correspondem, respetivamente, às datas de aprovação do Regulamento Geral sobre a Proteção de Dados (RGPD) e do *European Union Cyber Solidarity Act* – duas legislações estruturantes no que respeita, respetivamente, à governação de dados e à segurança digital.

De modo a delinear o estudo foi formulada a seguinte pergunta de partida:

- PP- Qual o impacto das políticas de gestão de dados da União Europeia na sua segurança digital?

- Podemos derivar duas perguntas que ajudam não só a responder à mesma, mas também a diminuir a amplitude do tema, nomeadamente:

- PD1- Quais os fatores que afetam a segurança digital da União Europeia?

- PD2- Estas políticas afetam as Forças Armadas Portuguesas?

Privilegiando fontes primárias, este estudo procurou construir uma base sólida, que sustenta uma análise crítica e reflexiva para compreender as implicações, desafios e dinâmicas da gestão de dados (Booth et al., 2003). Adotou-se uma abordagem metodológica qualitativa, baseada na análise documental e em entrevistas semiestruturadas, para investigar a gestão de dados no contexto das Relações Internacionais e da era digital. A metodologia utilizada promove uma análise multidimensional, integrando diferentes perspetivas e experiências proporcionadas pelas entrevistas realizadas, o que enriquece a compreensão do tema e favorece o debate académico (Bryman, 2012).

O estudo incluiu entrevistas semiestruturadas a três profissionais de diferentes áreas: o Capitão Carlos Bernardino, que abordou o desenvolvimento tecnológico e a modernização da Força Aérea; Marco António Ribeiro dos Santos Costa, que explorou os desafios legislativos relacionados com a gestão de dados; e Luís Manuel da Silva Fernandes Santos, que destacou os impactos das políticas de segurança e proteção de dados nas práticas empresariais. Estas entrevistas complementaram a análise documental, proporcionando uma visão mais ampla acerca do tema.

Revisão de literatura

O ciberespaço surgiu como um domínio estratégico essencial para os Estados, exercendo uma grande influência na cibersegurança, ciberdefesa e na governação global. No livro *Cyberpolitics in International Relations* (Choucri, 2012), o ciberespaço é analisado a partir de diversas perspetivas teóricas das Relações Internacionais. Sob a perspetiva do realismo, é destacado como um campo de conflito interestatal, onde Estados competem com ciberataques, espionagem e desenvolvimento tecnológico, elevando a defesa digital ao nível da defesa militar tradicional. O liberalismo foca-se na cooperação internacional e na criação de normas globais para mitigar ameaças, enquanto o construtivismo analisa o ciberespaço como uma construção social, moldada por narrativas, ideologias e práticas, onde atores não estatais desempenham um papel crucial neste ambiente, influenciando significativamente a sua governação.

Em *International Relations in the Cyber Age* (Choucri & Clark, 2018), os autores expandem esta análise, destacando desafios ao realismo diante da multiplicidade de atores não estatais. Sob a perspetiva liberal, reforçam a importância da governação partilhada, embora reconheçam a complexidade de regular um domínio sem fronteiras físicas claras. O construtivismo, por sua vez, destaca as narrativas sociais e a interdependência crescente entre sistemas digitais e sociais, apontando para a necessidade de estruturas de governação em constante evolução.

Shen (2022) destaca uma fragmentação na governação de dados, onde três principais atores – China, Estados Unidos e União Europeia – competem por influência. A União Europeia procura um equilíbrio entre privacidade e comércio digital, enquanto os Estados

Unidos priorizam o fluxo livre de dados para promover comércio e investigação. A China, por outro lado, regula rigorosamente os dados sob uma ótica de segurança nacional. Essa disputa geopolítica pelo controlo e pela regulamentação do ciberespaço reflete a crescente relevância dos dados como ferramenta estratégica no cenário internacional.

Aguerre *et al.* (2024) argumentam que a digitalização é um fenómeno transformativo global com impactos significativos que excedem o domínio digital, incrementando a urgência da cooperação e governação internacional. Por conseguinte, assinalam o crescimento no interesse e produção académicos sobre a governação digital. No entanto, destacam que se tratam de investigações essencialmente monodisciplinares com enquadramentos nacionais ou locais, existindo grandes lacunas na investigação supranacional, mais precisamente no plano regional e global. Este contexto reforça a necessidade de investigar as políticas de gestão de dados ao nível regional, através do caso da União Europeia. A incorporação complementar do caso de Portugal permite articular os dois níveis de análise, além de ser um caso pouco explorado pela literatura, em especial, considerando a dimensão das Forças Armadas.

Política de Gestão de Dados da União Europeia

A política de gestão de dados da União Europeia possui um impacto internacional, na medida em que influencia todos os membros do Espaço Europeu e estabelece regulamentos que afetam transações realizadas na região (Comissão Europeia, 2024a). Propostas pela Comissão Europeia com aconselhamento do Comité Europeu para a Proteção de Dados, podem ser alteradas conforme necessário, nomeadamente quando se encontra uma incompatibilidade, prevendo também o reconhecimento de países terceiros que cumprem as suas normas (Comissão Europeia, 2024a).

A Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados, criados em 2004 e 2018 respetivamente, asseguram a função de proteção de dados pessoais e atualizam as legislações existentes de acordo com os avanços políticos e tecnológicos. A Agência Europeia para a Segurança das Redes e da Informação (ENISA, 2023) reforça este esforço e oferece apoio técnico, monitorizando ameaças, promovendo a cooperação internacional com entidades como a Organização do Tratado do Atlântico Norte (OTAN) e agências dos Estados Unidos da América, além de coordenar estratégias para fortalecer infraestruturas digitais (ENISA, 2023). Iniciativas como o *European Union Chips Act* e o *Digital Europe Programme* destacam o compromisso da União Europeia em reduzir vulnerabilidades tecnológicas e estimular a inovação (Comissão Europeia, 2024c).

O aumento do fluxo de dados entre empresas públicas e privadas exige uma regulação eficiente, pois a troca de informações tornou-se essencial numa era de evolução tecnológica e globalização (Parlamento Europeu & Conselho da União Europeia, 2016). Regulamentos como o RGPD reforçam os direitos individuais, e estruturam o mercado interno da União Europeia, para além de implicarem um investimento em ciberdefesa, promovendo um tempo de reação a ciberataques mais ágil (Comissão Europeia, 2018).

O *European Union Cyber Solidarity Act* procura mitigar ameaças digitais com sistemas de alerta baseados em Inteligência Artificial (IA) para identificar e prevenir ataques cibernéticos, promovendo respostas coordenadas entre Estados-Membros (Comissão

Europeia, 2024b). Este sistema integra tecnologias avançadas e incentiva a colaboração entre setores público, privado e entre Estados de forma a fortalecer a resiliência coletiva.

Políticas europeias

O *Data Governance Act* da União Europeia estabelece um enquadramento estratégico para fortalecer a partilha segura e ética de dados e promove benefícios económicos e competitivos para as empresas e os cidadãos europeus (Parlamento Europeu & Conselho da União Europeia, 2022). Este regulamento é um pilar central da Estratégia Europeia para os Dados e tem como objetivo aumentar a confiança e a segurança nas transações, essenciais para setores como a saúde, a energia, o ambiente e a indústria (Parlamento Europeu & Conselho da União Europeia, 2022).

O regulamento garante que os dados sejam geridos de forma responsável, com transparência e proteção, sem prejuízo das leis nacionais. Facilita a reutilização de dados, protegendo dados sensíveis através de anonimização para além de assegurar a conformidade com as normas da União Europeia. Além disso, regula a atuação de intermediários, exigindo que estes garantam a privacidade, a integridade e a segurança das operações, e prevê mecanismos sancionatórios para práticas fraudulentas (Parlamento Europeu & Conselho da União Europeia, 2022).

Quanto à transferência internacional de dados, o regulamento impõe condições rigorosas para dados sensíveis, restringindo a partilha com países que não cumprem os requisitos da União Europeia. Estas regras visam assegurar transferências éticas e seguras, protegendo os interesses públicos (Parlamento Europeu & Conselho da União Europeia, 2022). Os Estados-Membros devem criar órgãos para apoiar a aplicação do regulamento, e promover a partilha responsável, respeitando a privacidade dos dados (Parlamento Europeu & Conselho da União Europeia, 2022).

A regulamentação proíbe acordos de exclusividade no armazenamento e análise de dados, exceto em casos de interesse geral devidamente justificados e limitados a 12 meses. Adicionalmente, estabelece sanções proporcionais à gravidade das violações, o que permite que cada Estado-Membro adapte as penalidades às suas realidades políticas e culturais (Parlamento Europeu & Conselho da União Europeia, 2022).

O regulamento prevê a criação do Comité Europeu da Inovação de Dados, que promove a partilha de conhecimento científico e tecnológico, facilitando colaborações internas e com países terceiros.

Esta revisão está prevista até 24 de setembro de 2025 para avaliar a sua eficácia e impacto na realidade europeia (Parlamento Europeu & Conselho da União Europeia, 2022).

Em Portugal, segundo Costa (2024), a implementação do conceito de *data governance* ainda está em fase inicial e requer maior investimento em literacia digital e em mudanças de atitude. Bernardino (2024) reforça a necessidade de informar os cidadãos sobre seus direitos no âmbito da proteção de dados, o que promove a convergência e o alinhamento com os regulamentos da União Europeia.

O Regulamento Geral de Proteção de Dados (RGPD), adotado em 27 de abril de 2016 e em vigor desde 25 de maio de 2018, visa proteger os dados pessoais dos cidadãos da União Europeia, estabelece uma base comum para as legislações dos Estados-Membros e garante a liberdade, justiça e segurança na circulação de dados pessoais (Parlamento Europeu & Conselho da União Europeia, 2016). O regulamento aplica-se a todas as entidades que processam dados pessoais na União Europeia, mas exclui atividades relacionadas com a segurança e a política externa da União Europeia.

O RGPD define o tratamento de dados como um direito fundamental e regula a transparência e segurança na sua utilização. Dados sensíveis, como informações de saúde, origem racial, opiniões políticas e crenças religiosas, necessitam de proteção adicional e só podem ser processados com o consentimento explícito do titular ou em situações de interesse público (Parlamento Europeu & Conselho da União Europeia, 2016).

Os titulares de dados têm direitos garantidos, como acesso, retificação, apagamento, portabilidade e oposição ao tratamento dos seus dados. Empresas e entidades públicas devem assegurar que o tratamento de dados seja seguro, transparente e limitado ao necessário. Violações de segurança devem ser notificadas imediatamente às autoridades e aos titulares, com medidas de mitigação recomendadas (Parlamento Europeu & Conselho da União Europeia, 2016).

O regulamento também aborda a transferência internacional de dados, permitindo-a apenas sob condições específicas, como a existência de tratados ou consentimento do titular. Adicionalmente, incentiva os Estados-Membros a criar autoridades independentes para supervisionar o cumprimento do regulamento, com recursos adequados e proteção contra influências externas (Parlamento Europeu & Conselho da União Europeia, 2016).

O RGPD promove a liberdade de expressão, permitindo exceções para fins jornalísticos, literários e académicos, desde que conciliadas com a proteção de dados. Apesar de ser um marco na proteção de dados, conforme apontado por Costa (2024), ainda enfrenta desafios na sua implementação devido à falta de informação e de consciencialização por parte dos cidadãos, reforçando a necessidade de maior literacia sobre os direitos e deveres em relação aos dados pessoais.

Política de Gestão de Dados em Portugal

Em 2019, Portugal atualizou as suas políticas de gestão de dados com a Lei n.º 58/2019, alinhando-se ao RGPD de forma a proteger os dados pessoais dos cidadãos e garantir a circulação segura de informações, abrangendo tanto empresas públicas quanto privadas, dentro ou fora do território nacional (Lei n.º 58/2019, 2019). A Comissão Nacional de Proteção de Dados é a autoridade responsável por fiscalizar o cumprimento da lei, avaliar impactos e colaborar internacionalmente para um sistema de proteção atualizado e seguro. A *NATO Communications Academy,* inaugurada em 2019 em Oeiras, reforça a formação em cibersegurança e ciberdefesa, enquanto o Comando de Operações de Ciberdefesa reúne militares dos três ramos das Forças Armadas com o intuito de monitorizar o espaço digital e articular a segurança cibernética com órgãos como o *NATO Cyber Security Centre* (República Portuguesa, s.d.).

Segundo Costa (2024), embora Portugal siga as orientações da União Europeia, ainda apresenta deficiências, como falta de investimento na formação dos cidadãos e no aumento da literacia digital, o que cria vulnerabilidades. Projetos como o Gaia-X e iniciativas de digitalização previstas até 2030 visam melhorar a cibersegurança e promover a confiança entre empresas e clientes (Gaia-X, 2023; República Portuguesa, 2023). A Comissão Nacional de Proteção de Dados definiu uma série de medidas estratégicas para aprimorar a proteção de dados no país, incluindo o desenvolvimento de um Plano Nacional de Formação para promover a literacia digital, a criação de campanhas de boas práticas e de um canal prioritário *online* em parceria com Espanha de modo a facilitar a interação com os cidadãos (Comissão Nacional de Proteção de Dados, 2024). Além disso, procura fortalecer a cooperação nacional e internacional, estabelecendo protocolos robustos entre entidades públicas e privadas e incentivar a confiança mútua entre cidadãos e instituições.

A modernização e reorganização interna da Comissão Nacional de Proteção de Dados também são prioritárias, com melhorias na gestão de recursos humanos, aumento das sanções para violações de dados e aprimoramento da eficiência nas operações. Estas medidas visam consolidar a proteção de dados, fortalecer a cibersegurança e assegurar uma abordagem resiliente e integrada frente aos desafios digitais emergentes.

Ameaças e desafios à segurança digital da União Europeia

A ENISA e outras autoridades nacionais reportam um aumento nas tentativas de furto e violação de dados, destacando a atuação de agentes não estatais, como hackers organizados e ativistas cibernéticos, que representam um grande desafio à cibersegurança devido à sua natureza descentralizada, dificultando a sua identificação e o rastreamento (ENISA, 2023). Estes agentes ameaçam sistemas críticos e processos democráticos, como demonstra o ataque do grupo "*Fancy Bear*" em 2021 contra instituições governamentais europeias (Starks, 2021). A interferência em sistemas eleitorais é especialmente preocupante, pois compromete a confiança pública e a integridade das democracias, tornando essencial o fortalecimento de protocolos de segurança (ENISA, 2023).

Para enfrentar estes desafios, a União Europeia tem adotado medidas para aumentar a sua resiliência e autossuficiência, como o *European Union Chips Act*, que tem como objetivo atrair empresas tecnológicas para o território europeu, reduzindo dependências externas (Comissão Europeia, 2024c). A Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados desempenham um papel crucial na promoção de boas práticas, literacia digital e uma cultura de responsabilidade na proteção de dados (Comissão Europeia, 2024d). A União Europeia também colabora internacionalmente e investe no desenvolvimento de tecnologias de cibersegurança para limitar a influência de agentes não estatais e proteger infraestruturas e processos democráticos.

Potencial de dados furtados

O aumento exponencial de cibercrimes, impulsionado por novas tecnologias, tem colocado em risco dados sensíveis de indivíduos e organizações. Pequenas e médias empresas são frequentemente alvos devido à sua menor capacidade de investir em cibersegurança. Técnicas como *ransomware* e *phishing* destacam-se pela eficácia em explorar vulnerabilidades para extorsão financeira e roubo de dados. Esses ataques comprometem informações pessoais, financeiras e corporativas, que consequentemente causam danos à reputação, perdas financeiras e desconfiança pública, tornando a recuperação um processo longo (Europol, 2024; Macnish *et al.*, 2019).

Os dados biométricos, cada vez mais usados como substitutos de palavras-passe tradicionais, também enfrentam desafios significativos. Por serem únicos e imutáveis, o seu comprometimento pode gerar riscos permanentes para os indivíduos, além de levantar preocupações sobre privacidade, consentimento e uso indevido por empresas em países sem um enquadramento regulatório claro (Natgunanathan *et al.*, 2016).

Outro risco crescente é a desinformação, utilizada para manipular a opinião pública e apoiar interesses políticos ou geopolíticos, como no conflito entre Rússia e Ucrânia. A disseminação deliberada de informações falsas afeta setores críticos, como saúde e democracia, o que exige ações coordenadas para mitigar os seus efeitos (ENISA, 2023).

Casos como o ataque à plataforma *Biostar 2*, que teve como consequência o furto de dados biométricos de mais de um milhão de utilizadores, evidenciam a fragilidade das infraestruturas digitais. Apesar de cumprir formalmente o RGPD, a resposta da empresa responsável levantou críticas sobre a eficácia das práticas de conformidade e destacou a necessidade de medidas mais rigorosas, como criptografia e arquiteturas descentralizadas, além de uma supervisão regulatória mais robusta (Trend Micro, 2019; Suprema, 2022). Esses incidentes realçam a urgência de fortalecer práticas de segurança cibernética e proteção de dados frente aos desafios da era digital.

A guerra Rússia-Ucrânia intensificou a preocupação com a segurança e a defesa na Europa, promovendo um aumento significativo nos investimentos nestes setores (Euronews, 2023). Desde o início do conflito, a União Europeia tem sido alvo de ciberataques com o intuito de aceder a bases de dados estratégicas, obter informações militares e lançar campanhas de desinformação que comprometem a coesão social e política (Duguin & Pavlova, 2023). Estes ataques demonstram o uso dos dados como armas estratégicas num conflito que transcende fronteiras físicas, evidenciando a interconexão das infraestruturas cibernéticas globais e os impactos transnacionais destas operações.

Em resposta, a União Europeia tem adotado medidas para proteger suas infraestruturas digitais, incluindo o *European Union Cyber Solidarity Act*, que reforça a prontidão e a capacidade de resposta contra ameaças cibernéticas, visando assegurar a integridade de os seus sistemas e mitigar os riscos globais decorrentes do conflito (Comissão Europeia, 2024b).

Impacto na Confiança e Reputação

A gestão de dados é crucial nas relações internacionais, garantindo direitos fundamentais como acesso, retificação e eliminação de dados, assegurados pelo RGPD, para que os cidadãos tenham controlo sobre as suas informações pessoais. No entanto, a confiança pública nos governos pode ser comprometida por fatores como burocracia excessiva e experiências negativas com serviços públicos. Reduzir barreiras e simplificar processos é essencial para melhorar a perceção dos cidadãos e promover confiança nas instituições (Hitlin & Shutava, 2022).

A transição para o *e-government* traz benefícios como redução de custos e maior eficiência dos serviços públicos, mas também enfrenta desafios relacionados com cibersegurança e à confiança nas novas tecnologias. A falta de atualização e segurança pode gerar desconfiança dos cidadãos em partilhar dados pessoais e realizar transações digitais, atrasando o avanço dessas soluções. Para garantir o sucesso do *e-government,* é necessário investimento contínuo em segurança, transparência e campanhas de educação para que os cidadãos compreendam e confiem nos serviços digitais (Horsburgh et al., 2011).

Durante a pandemia de COVID-19, o *e-government* demonstrou sua importância ao permitir acesso seguro e remoto a serviços públicos, reduzindo a necessidade de deslocamentos e interação física. Este contexto evidenciou como a confiança entre cidadãos e governos é vital para a aceitação de soluções digitais e destacou a necessidade de campanhas educativas e transparência para fomentar essa confiança (Martinus & Seth, 2023). A liderança responsável e transparente é essencial para reconquistar e manter a confiança pública, promovendo o uso eficiente de recursos e alinhando as soluções digitais aos interesses da sociedade (P. Hiltin et N. Shutava, 2022).

Atores não estatais

A segurança contemporânea enfrenta riscos crescentes de atores não estatais e movimentos internos, que emergem de forma descentralizada e espontânea, facilitados pela rápida partilha de informações no meio digital. Estes atores incluem terroristas recrutados através das redes sociais, hackers organizados e ativistas cibernéticos, que visam desestabilizar sistemas críticos, interferir em processos eleitorais e procuram obter acesso a dados sensíveis. Exemplos como o ataque do grupo "Fancy Bear" em 2021 evidenciam a complexidade de rastrear e mitigar essas ameaças, que comprometem a confiança pública e a integridade das instituições democráticas (Starks, 2021).

A espionagem digital também é um grande risco, intensificado pelo conflito Rússia-Ucrânia. A Letónia reportou várias atividades de espionagem relacionadas com serviços russos e chineses, com ataques visando identificar vulnerabilidades e sabotar bases de dados europeias. Além disso, campanhas de desinformação, especialmente em plataformas como Telegram, têm sido usadas para manipular perceções públicas e influenciar decisões políticas, tornando-se um elemento central da guerra híbrida (*Latvian State Security Service*, 2024).

A União Europeia reconhece estes desafios, tem investido em novas tecnologias de cibersegurança e tem estabelecido parcerias internacionais para proteger infraestruturas críticas e processos democráticos, reforçando a sua capacidade de resposta a ameaças cibernéticas e híbridas (ENISA, 2023).

Gestão de dados relacionada com os conflitos internacionais

A gestão de dados desempenha um papel central nas relações internacionais, especialmente no campo das *cyberpolitics*, que emergiram como uma resposta ao acesso generalizado à internet. Este ramo aborda questões cruciais como propriedade de bases de dados, regulação de crimes no espaço digital e implementação de políticas de segurança. Ao contrário das limitações físicas que tradicionalmente definem políticas territoriais, os recursos digitais possuem uma natureza intangível, o que faz com que a informação possa permanecer indefinidamente na rede ou desaparecer com um único ataque (Krieger, 2014). A União Europeia, por meio de suas diretrizes e regulações, procura moldar o futuro digital e estabelecer-se como líder no espaço cibernético, influenciando diretamente a soberania e as relações internacionais dos Estados-Membros (Salbu, 2001).

Os dados, são reconhecidos como um recurso valioso, pois são ferramentas poderosas que podem moldar perceções e comportamentos. Através de práticas de segmentação e personalização de conteúdo digital, é possível manipular ideologias e influenciar decisões. Este poder, frequentemente concentrado em grandes empresas tecnológicas, representa um desafio tanto para a segurança dos indivíduos quanto para a integridade das democracias (Zwitter, 2015). Ao mesmo tempo, a governação de dados tornou-se uma prioridade estratégica para governos e organizações internacionais, como a União Europeia, que busca regular o espaço digital para proteger os seus cidadãos, enquanto enfrenta uma rápida evolução tecnológica e conflitos geopolíticos que afetam diretamente sua capacidade de resposta (Zwitter, 2015).

A ascensão da China como líder em tecnologia e vigilância global representa um desafio significativo para a União Europeia. Empresas chinesas, como Huawei e Tencent, têm sido acusadas de facilitar a recolha de dados pessoais para o governo chinês, o que levanta preocupações sobre privacidade e manipulação de informações (Zhao, 2022). Além disso, o uso de tecnologias como a inteligência artificial, muitas vezes alimentadas por grandes volumes de dados recolhidos de forma pouco transparente, incrementa a desconfiança. A falta de regulamentos rigorosos na China permitiu ao país acumular vastas bases de dados que alimentam tanto seu desenvolvimento tecnológico quanto sua capacidade de influência global, colocando-o em competição direta com os Estados Unidos e a União Europeia, especialmente em setores como defesa e indústria (Zhao, 2022).

Estas ameaças não são limitadas a estados-nação. Grupos não estatais, como hackers organizados e ativistas cibernéticos, também representam um risco crescente, operando de forma descentralizada e com alcance global. O ataque do grupo "*Killnet*" à Lituânia em 2022 e o aumento dos ciberataques a países da OTAN desde o início do conflito Rússia-Ucrânia ilustram a crescente sofisticação dessas ameaças (Al Jazeera, 2022). A

espionagem digital também se intensificou, com ações atribuídas a agentes chineses e russos, que exploram vulnerabilidades em infraestruturas críticas e promovem campanhas de desinformação para moldar perceções públicas e influenciar decisões políticas (*Latvian State Security Service*, 2024).

Nesse contexto, a União Europeia tem investido em medidas como o *European Union Cyber Solidarity Act* e em parcerias estratégicas para enfrentar esses desafios. As Parcerias Público-Privadas são um componente fundamental dessa estratégia, permitindo a colaboração entre os setores público e privado para melhorar a resiliência digital, promover inovação e garantir a segurança dos dados. Essas parcerias dependem por vezes de *outsourcing*, o que oferece flexibilidade para adaptar abordagens às necessidades específicas de cada contexto, combinando a experiência técnica do setor privado com a capacidade de regulamentação do setor público (ENISA, 2017).

A colaboração internacional também desempenha um papel crucial na resposta a ciberameaças globais. A União Europeia trabalha em estreita cooperação com órgãos como a OTAN e a Agência de Cibersegurança dos Estados Unidos para fortalecer as suas capacidades de deteção, resposta e mitigação de incidentes cibernéticos. Essa cooperação promove a troca de melhores práticas, harmonização de normas e desenvolvimento de ferramentas conjuntas que aumentam a interoperabilidade e eficácia das soluções implementadas (*European Cybersecurity Competence* Centre, s. d.). Josep Borrell, nnum discurso, destacou que "as ciberameaças não têm fronteiras", enfatizando a necessidade de uma abordagem coordenada e integrada para garantir a segurança no ambiente digital.

O rápido crescimento das ciberameaças, combinado com a crescente dependência de infraestruturas digitais, sublinha a importância de políticas robustas de gestão de dados e da cibersegurança. A União Europeia continua a enfrentar desafios complexos no cenário geopolítico e digital, mas suas iniciativas, como a regulação do espaço digital e o fortalecimento de parcerias estratégicas, demonstram um compromisso em proteger seus cidadãos e promover um futuro digital seguro e confiável.

Política de gestão de dados em Portugal e nas Forças Armadas

Este capítulo analisa as implicações da implementação de regulamentos de cibersegurança em Portugal, com foco nas Forças Armadas e nos setores público e privado. Apesar de um aumento previsto de 15% no investimento em cibersegurança em 2024, visando atualizar infraestruturas, implementar novas tecnologias e fortalecer a resiliência contra ameaças emergentes, persistem desafios significativos, como a falta de recursos humanos qualificados e de uma cultura de cibersegurança (*Security Magazine*, 2024).

Segundo Costa (2024), Portugal adota os regulamentos da União Europeia de forma reativa e limitada, sem um desenvolvimento local ou iniciativas próprias, o que prejudica a construção de uma infraestrutura robusta de segurança. A falta de profissionais especializados agrava a dificuldade de monitorizar e responder a incidentes, enquanto a ausência de campanhas educativas e de sensibilização deixa os cidadãos vulneráveis a

riscos digitais, como mencionado por Santos (2024). A falta de consciencialização pública contribui para práticas inseguras, aumentando a exposição a ameaças.

O Centro Nacional de Cibersegurança (2022) aponta que pequenas e médias empresas enfrentam desafios ainda maiores devido a restrições financeiras e falta de conhecimento especializado. Apenas uma fração dessas empresas dispõe de certificações de segurança, e os orçamentos destinados à cibersegurança são frequentemente insuficientes, tornando-as alvos fáceis para ciberataques. Assim, a ausência de alinhamento com as melhores práticas internacionais aumenta a vulnerabilidade dessas organizações, destacando a necessidade de estratégias nacionais mais proativas e integradas.

A gestão de dados nas Forças Armadas Portuguesas é estratégica frente à rápida evolução tecnológica e às crescentes ameaças no ciberespaço. Com a transformação digital, o governo português tem investido em infraestruturas tecnológicas e em políticas de cibersegurança para cumprir compromissos com a União Europeia e a OTAN. Iniciativas como a criação da *NATO Communications and Information Academy* em Oeiras reforçam a capacitação em cibersegurança e a colaboração internacional (Nunes, 2020).

Apesar dos avanços, desafios persistem. A escassez de recursos humanos especializados compromete a capacidade de resposta a ciberameaças, exigindo medidas como a criação de um quadro especial para profissionais de ciberdefesa e incentivos para a retenção de talentos. Propõe-se também o estabelecimento de uma reserva nacional de especialistas para garantir respostas rápidas em situações críticas (Nunes, 2020).

A segurança dos sistemas de informação militares é prioritária, mas a dependência de tecnologias desatualizadas e a utilização de dispositivos não seguros representam vulnerabilidades. Segundo Bernardino (2024), é crucial atualizar equipamentos e garantir que sistemas internos sejam protegidos para evitar compromissos de rede. Além disso, a Estratégia Nacional de Segurança do Ciberespaço destaca a necessidade de alinhar iniciativas nacionais e internacionais para garantir uma abordagem coesa e integrada (ENISA, 2023).

A formação também tem sido foco, com disciplinas de ciberdefesa introduzidas em cursos militares, que proporcionam conhecimentos essenciais sobre segurança da informação. Contudo, o país ainda está no início desse processo, e esforços contínuos são necessários para construir uma ciberdefesa nacional resiliente, que garanta a soberania digital e o cumprimento de compromissos internacionais (Nunes, 2020).

Conclusões

O espaço digital tornou-se um domínio essencial, influenciando profundamente as relações sociais, económicas e políticas. Tal influência gera avanços significativos e também apresenta desafios complexos, como a privacidade e a proteção de dados. A União Europeia tem liderado esforços regulatórios, implementando políticas como o RGPD e o *Data Governance Act*, que promovem segurança, transparência e proteção de direitos fundamentais. No entanto, dificuldades de harmonização entre Estados-Membros, a influência de grandes corporações tecnológicas e a atuação de agentes não estatais, representam barreiras significativas a uma integração positiva de novas tecnologias.

Empresas privadas como *Google* e *TikTok* acumulam grandes volumes de dados pessoais e desafiam a soberania regulatória europeia, enquanto campanhas de desinformação e ciberataques ameaçam as democracias e a estabilidade digital. A União Europeia procura mitigar esses riscos ao estabelecer regulamentos robustos e mecanismos de supervisão eficazes, reforçando tanto a privacidade como a resiliência das infraestruturas digitais.

Em Portugal, as Forças Armadas têm avançado na cibersegurança, alinhando-se com as políticas europeias e da OTAN. A criação do Centro de Comando de Operações de Ciberdefesa e da *NATO Communications and Information Academy* em Oeiras reflete o compromisso nacional em fortalecer a defesa cibernética. Contudo, desafios como a escassez de recursos humanos especializados, a falta de atualização tecnológica e a necessidade de formação contínua limitam a eficácia dessas iniciativas. Propostas como a criação de uma reserva nacional de especialistas e parcerias público-privadas são essenciais para superar essas dificuldades.

Respondendo às questões formuladas no início do artigo, conclui-se que as políticas de gestão de dados da União Europeia influenciam diretamente a segurança digital, promovem uma abordagem ética e inovadora que protege os direitos dos cidadãos e sustenta a democracia. No entanto, para enfrentar as rápidas mudanças tecnológicas e as crescentes ameaças, é necessário reforçar a colaboração internacional, investir em tecnologias emergentes e promover a literacia digital, assegurando um ambiente digital seguro, resiliente e inclusivo.

Conclui-se igualmente que é imperativo que as Forças Armadas se desenvolvam de modo a abranger este mundo digital em transformação, observando-se já esse processo nas Forças Armadas Portuguesas. Futuras investigações centradas nas Forças Armadas, numa perspetiva comparativa entre Estados-Membros da União Europeia, permitiriam uma reflexão fundamentada sobre a cadência de adaptação a este novo campo para assegurar uma defesa e modernização proativas.

Este estudo apresenta limitações decorrentes da bibliografia disponível sobre o tema e da sua natureza volátil, uma vez que se trata de uma área de rápida evolução, na qual os fatores determinantes evoluem continuamente. Apesar destas limitações, é possível reconhecer a crescente importância desta temática a nível global, cuja influência se estende do indivíduo aos próprios Estados, criando desafios e oportunidades em todas as esferas da sociedade.

Referências

Aguerre, C., Campbell-Verduyn, M., & Scholte, J. A. (2024). Introduction: Polycentric perspectives on digital data governance (pp. 1–18). In C. Aguerre, M. Campbell-Verduyn, & J. A. Scholte (Eds.), *Global digital data governance: Polycentric perspectives* (pp. 1–18). Routledge.

Al Jazeera. (2022, 27 junho). *Russia hackers claim responsibility for cyber-attack on Lithuania*. https://www.aljazeera.com/news/2022/6/27/russia-hackers-claim-responsibility-for-cyber-attack-on-lithuania

Bernardino, C. (2024, 17 outubro). *Entrevista conduzida por A. Barroso* [Videoconferência; comunicação pessoal não recuperável].

Booth, W. C., Colomb, G. G., & Williams, J. M. (2003). *The Craft of Research* (2ª ed.). University of Chicago Press.

British Academy & Royal Society. (2017). *Data management and use: Governance in the 21st century*. https://royalsociety.org/news-resources/projects/data-governance/

Bryman, A. (2012). *Social Research Methods* (4ª ed.). Oxford University Press.

Centro Nacional de Cibersegurança. (2022). *Relatório Cibersegurança em Portugal: Sociedade 2022*. https://www.cncs.gov.pt/docs/rel-sociedade2022-observ-cncs.pdf

Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press.

Choucri, N., & Clark, D. (2018). *International relations in the cyber age: The co-evolution dilemma*. MIT Press.

Comissão Europeia. (2018). *Perguntas e Respostas – Regulamento Geral sobre a Proteção de Dados*. https://ec.europa.eu/commission/presscorner/api/files/document/print/pt/memo_18_387/MEMO_18_387_PT.pdf

Comissão Europeia. (2024a, setembro 24). *Políticas da UE em matéria de cibersegurança*. https://digital-strategy.ec.europa.eu/pt/policies/cybersecurity-policies

Comissão Europeia. (2024b, novembro 04). *Cyber Solidarity Act*. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

Comissão Europeia. (2024c, novembro 04). *European Chips Act*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_pt

Comissão Europeia. (2024d, dezembro 11). *Digital Europe Programme*. https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Comissão Nacional de Proteção de Dados. (2024). *Plano Anual de Atividades para o Ano de 2025*. https://www.cnpd.pt/media/1d5eggad/cnpd_plano-anual-de-atividades-2025.pdf

Costa, M. (2024, 11 setembro). *Entrevista conduzida por A. Barroso* [Presencial; comunicação pessoal não recuperável].

Duguin, S., & Pavlova, P. (2023). *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict*. European Parliament, Directorate-General for External Policies. https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2023)702594.

ENISA. (2017). *ENISA Public Private Partnerships (PPP): Cooperative models*. https://doi.org/10.2824/076734

ENISA. (2023). *ENISA Threat Landscape 2023: July 2022 to June 2023*. https://doi.org/10.2824/782573

Euronews. (2023, 30 novembro). *Record increase in EU military spending amid "demanding times"*. https://www.euronews.com/2023/11/30/record-increase-in-eu-military-spending-amid-demanding-times

European Cybersecurity Competence Centre. (s.d.). *European Cybersecurity Competence Centre*. Consultado em 30 de dezembro de 2024, em https://cybersecurity-centre.europa.eu/index_en

Europol. (2024). *European Union terrorism situation and trend report 2023*. Publications Office of the European Union. https://doi.org/10.2813/302117

Gaia-X. (2023). *A Federated Secure Data Infrastructure*. https://gaia-x.eu/about/

Hitlin, P., & Shutava, N. (2022). *Trust in Government: A Close Look at Public Perceptions of the Federal Government and Its Employees*. https://ourpublicservice.org/wp-content/uploads/2022/03/Trust-in-Government.pdf

Horsburgh, S., Goldfinch, S., & Gauld, R. (2011). Is Public Trust in Government Associated With Trust in E-Government? *Social Science Computer Review*, 29, 232–241. https://doi.org/10.1177/0894439310368130

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1). https://doi.org/10.1177/2053951720982012

Kazemi, A., Kalhornia Golkar, M., & Lajmiri, S. (2023). Origins of Cyber Security: Short Report. International Journal of Reliability, Risk and Safety: *Theory and Application*, 6(2), 77-83. https://doi.org/10.22034/ijrrs.2023.6.2.9

Krieger, J. (2014). *Explorations in Cyber International Relations*. Oxford University Press.

Kumar, R., & Bhatia, M. (2020). A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability. In *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 334-337). IEEE. https://doi.org/10.1109/GUCON48875.2020.9231255

Latvian State Security Service. (2024). *Annual Report for 2023*. https://vdd.gov.lv/en/news/press-releases/vdd-publishes-the-annual-report-on-its-activities-in-2023/

Lei n.º 58/2019, de 8 de agosto. (2019). https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Macnish, K., Fernandez-Inguanzo, A., & Kirichenko, A. (2019). Smart Information Systems in Cybersecurity: An Ethical Analysis. *ORBIT Journal*, 2(2). https://doi.org/10.29297

Martinus, M. & Seth F. (2023). *E-government and digital trust: Lessons from the COVID-19 pandemic.* ISEAS Yusof Ishak Institute. https://www.iseas.edu.sg/wp-content/uploads/2023/05/ISEAS_Perspective_2023_48.pdf

Natgunanathan, I., Mehmood, A., Xiang, Y., Beliakov, G., & Yearwood, J. (2016). Protection of Privacy in Biometric Data. *IEEE Access*, 4, 880-892 https://doi.org/10.1109/ACCESS.2016.2535120

Nunes, P. F. V. (2020). *A edificação da capacidade de ciberdefesa nacional: Contributos para a definição de uma estratégia militar para o ciberespaço*. Coleção "ARES", 36. Instituto Universitário Militar. https://www.ium.pt/pub/65

Parlamento Europeu, & Conselho da União Europeia. (2016). *Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados—RGPD)*. Eur-Lex. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679

Parlamento Europeu, & Conselho da União Europeia. (2022). *Regulamento (UE) 2022/868 (Data Governance Act)*. Eur-Lex. https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

República Portuguesa. (2023). *Avaliação da Potencial Económico da Transição Digital em Portugal*. https://portugaldigital.gov.pt/wp-content/uploads/2023/05/Portugal-Digital_Avaliacao-Transicao-Digital_Documento-Final_v20230330_VF.pdf

República Portuguesa. (s.d.). *Ministério da Defesa Nacional. Comando de Operações de Ciberdefesa—COCiber*. Consultado em 17 de novembro de 2024, em https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro/Paginas/default.aspx

Rodima-Taylor, D. (2024). Grassroots data activism and polycentric governance: Perspectives from the margins (pp. 68–87). In C. Aguerre, M. Campbell-Verduyn, & J. A. Scholte (Eds.), *Global digital data governance: Polycentric perspectives*. Routledge.

Salbu, S. R. (2001). *The European Union Data Privacy Directive and International Relations*. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/39802/wp418.pdf

Sambaluk, N. M., & Spafford, E. H. (2020). *Myths and realities of cyber warfare: Conflict in the digital realm*. Praeger.

Santos, L. M. S. F. (2024, 11 setembro). *Entrevista conduzida por A. Barroso* [Presencial; comunicação pessoal não recuperável].

Security Magazine. (2024, 30 outubro). *IDC prevê que investimento em cibersegurança atinja 250 milhões em Portugal até ao final do ano*. https://www.securitymagazine.pt/2024/10/30/idc-preve-que-investimento-em-ciberseguranca-atinja-250-milhoes-em-portugal-ate-ao-final-do-ano/

Shen, Y. (2022). Data governance in China's platform economy. China Economic Journal, 15(2), 202–215. https://doi.org/10.1080/17538963.2022.2068833

Starks, T. (2021, 01 julho). *US, UK accuse Russian military hackers of battering-ram password attacks against hundreds of targets*. CyberScoop. https://cyberscoop.com/russia-gru-brute-force-password-spray-nsa-cisa-fbi-uk/

Suprema. (2022, 23 maio). *Legal notice*. https://www.supremainc.com/en/util/legal-notice.asp

Trend Micro. (2019, agosto 15). *Over 27.8M records exposed in BioStar 2 data breach*. https://www.trendmicro.com/vinfo/us/security/news/online-privacy/over-27-8m-records-exposed-in-biostar-2-data-breach

Zhao, B. (2022). *China's Rising Data Power and the Global Impacts*. [Preprint]. ResearchGate. https://doi.org/10.13140/RG.2.2.27432.85762/1

Zwitter, A. (2015). Big Data and International Relations. *Ethics & International Affairs*, 29(4), 377-389. https://doi.org/10.1017/S0892679415000362