NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTAMENTO DE
CIÊNCIAS SOCIAIS APLICADAS

RITA VASCONCELOS FARIA

Licenciada em Design de Comunicação - Artes gráficas

SALVAGUARDA DA PRIVACIDADE EM MEIO DIGITAL

RECURSO AO SELO DE USABILIDADE E ACESSIBILIDADE NO CONTEXTO DA ADMINISTRAÇÃO PÚBLICA PORTUGUESA

MESTRADO EM SOCIEDADE DIGITAL

Universidade NOVA de Lisboa
Setembro 2024

NOVA SCHOOL OF SCIENCE & TECHNOLOGY

DEPARTAMENTO DE
CIÊNCIAS SOCIAIS APLICADAS

SALVAGUARDA DA PRIVACIDADE EM MEIO DIGITAL

RECURSO AO SELO DE USABILIDADE E ACESSIBILIDADE NO CONTEXTO DA ADMINISTRAÇÃO PÚBLICA PORTUGUESA

RITA VASCONCELOS FARIA

Licenciada em Design de Comunicação - Artes gráficas

Orientador: Professor Doutor Davide Scarso
Professor Auxiliar do Departamento de Ciências Sociais Aplicadas
da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa.

Júri:

Presidente: Professora Doutora Paula Cristina Gonçalves Dias Urze
Professora Associada com Agregação do Departamento de Ciências Sociais Aplicadas da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa.

Arguente: Doutora Maria Luísa de Castro de Oliveira e Sousa
Investigadora do Departamento de Ciências Sociais Aplicadas da Faculdade de Ciências e Tecnologia da Universidade NOVA de Lisboa.

MESTRADO EM SOCIEDADE DIGITAL

Universidade NOVA de Lisboa
Setembro 2024

Salvaguarda da Privacidade em Meio Digital – Recurso ao Selo de Usabilidade e Acessibilidade no Contexto da Administração Pública Portuguesa

À memória de Helder Alves,
cuja amizade e ativismo são uma lembrança inspiradora.

AGRADECIMENTOS

Aos meus pais, pelo apoio incondicional e pela força que me deram ao longo desta etapa. Ao João, pelo incentivo que deu início a todo este processo, e juntamente com o Gonçalo, pela paciência e boa disposição constantes.

Aos professores, pelo tempo que nos dedicaram e pela proximidade que proporcionaram, enriquecendo-nos com as suas valiosas partilhas de conhecimento. Ao meu orientador, cujo contributo foi essencial para dar forma a esta dissertação. Aos colegas do mestrado, cuja amizade e cooperação foram fundamentais para superar as frustrações deste percurso.

À minha tia Ana Faria e à amiga Paula Pina, que generosamente se disponibilizaram para me apoiar neste trabalho, sempre que precisei.

Aos meus amigos, pela compreensão e por terem adiado encontros, permitindo que eu me dedicasse ao projeto.

RESUMO

Este estudo procura contribuir para um quadro mais robusto de proteção da privacidade em *sites* e aplicações móveis do setor público, analisando a privacidade digital no contexto da Administração Pública portuguesa. Explora o papel do Selo de Usabilidade e Acessibilidade como ferramenta para promover configurações que reforçam a salvaguarda da privacidade dos utilizadores de serviços digitais. A investigação apoia-se na estrutura de atributos de privacidade de Barth, Ionita e Hartel (2022), propondo um modelo de diagnóstico para avaliar as práticas de privacidade *online* das organizações. Este modelo resulta na criação de um formulário (Produto de Investigação 1) e de uma tabela de consulta (Produto de Investigação 2). Ambas as soluções têm como objetivo fomentar uma cultura de privacidade nas instituições, beneficiando os utilizadores e assegurando o respeito pelos seus direitos.

Palavras chave: Privacidade, Acessibilidade, Usabilidade, *User-Centered*, Serviços Digitais, Administração Pública Portuguesa

ABSTRACT

This study aims to contribute to a more robust privacy protection framework on public sector websites and mobile applications by analysing digital privacy in the context of the Portuguese Public Administration. It explores the role of the Usability and Accessibility Seal as a tool to promote configurations that reinforce the safeguarding of users digital privacy. The research is based on Barth, Ionita and Hartel's framework of privacy attributes (2022), proposing a diagnostic model to evaluate online privacy practices within organizations. This model results in the development of a form (Research Product 1) and a consultation table (Research Product 2). Both solutions aim to foster a culture of privacy in organisations, benefiting users and ensuring that their rights are respected.

Keywords: Privacy, Accessibility, Usability, User-Centred, Digital Services, Portuguese Public Administration

ÍNDICE

LISTA DE SIGLAS

AMA - Agência para a Modernização Administrativa
CNPD - Comissão Nacional de Proteção de Dados
DNP - Documento Normativo Produzido
EPD - Encarregado da Proteção de Dados
EUA - Estados Unidos
FIP - *Fair Information Practices*
HTML - *HyperText Markup Language* (Linguagem de Marcação de Hipertexto)[1]
INCM - Imprensa Nacional Casa da Moeda
IP - *Internet Protocol* (Protocolo de *Internet*)[2]
ISO - *International Organization for Standardization* (Organização Internacional de Normalização)
LGPD - Lei Geral de Proteção de Dados Pessoais (Brasil)
LUAP - Lista Unificada de Atributos de Privacidade
PET - *Privacy-Enhancing Technologies (*Princípios de Tratamento Justo de Informação)
PRR - Plano de Recuperação e Resiliência
RGPD - Regulamento Geral sobre a Proteção de Dados
SUA - Selo de Usabilidade e Acessibilidade
TIC - Tecnologias da Informação e Comunicação
UE - União Europeia
WCAG - *Web Content Accessibility Guidelines* (Diretrizes de Acessibilidade para Conteúdo da *Web*)

1 Linguagem de marcação utilizada para criar e estruturar páginas web. O HTML define a organização e o formato do conteúdo na *web*, permitindo a integração de textos, imagens, ligações, vídeos e outros elementos multimédia

2 Um IP é um conjunto de regras que ajuda os dispositivos eletrónicos a comunicarem-se na *Internet*, serve para direcionar os dados de um computador para outro, indicando para onde devem ir.

CAPÍTULO 1

INTRODUÇÃO

Contextualização e Importância do Tema

Na era digital, a privacidade tornou-se uma preocupação crescente para indivíduos e organizações. Com o aumento exponencial da utilização das tecnologias de informação e comunicação, a quantidade de dados pessoais recolhidos e processados atingiu níveis sem precedentes. Este panorama coloca a privacidade digital como um dos grandes desafios para as sociedades contemporâneas, exigindo uma abordagem sólida e estruturada para assegurar a proteção dos direitos dos utilizadores.

A implementação da transformação digital na Administração Pública tem vindo a ganhar maior relevância na estratégia das políticas públicas, alimentando uma narrativa que sublinha o potencial proporcionado pelas tecnologias digitais. Em particular, tem-se assistido a um foco crescente na utilização inteligente dos dados, que envolve a análise e interpretação de grandes volumes de informações para otimizar recursos, melhorar a tomada de decisões e formular políticas públicas mais eficazes, contribuindo assim para a melhoria do desempenho, eficiência e abrangência da Administração Pública. Portugal tem acompanhado a média europeia na modernização administrativa dos organismos do setor público[1], e, nesse sentido, a interação dos serviços públicos com a comunidade é, frequentemente, mediada pela sua presença *online*, nomeadamente através de *sites* e aplicações móveis.

A proteção dos dados pessoais e o respeito pela privacidade estão intrinsecamente ligados à utilização destes serviços digitais no contexto da Administração Pública. Desde a Convenção 108 do Conselho da Europa, em 1981, que a proteção dos direitos e liberdades dos indivíduos face ao crescente tratamento automatizado dos dados pessoais foi reconhecida internacionalmente como um fator de relevo[2]. A acompanhar a evolução das tecnologias de informação e comunicação, e como reflexo do amadurecimento dos debates associados, surgiu, mais recentemente, o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, instituído em 2016[3]. A partir de maio de 2018, a implementação deste regulamento tornou-se obrigatória em todos os Estados-Membros, tendo, por conseguinte, um impacto significativo na forma como as entidades devem gerir os dados pessoais. As organizações afetadas passaram a ter de respeitar princípios específicos de proteção de dados no tratamento e recolha dos mesmos, como garantia da privacidade dos utilizadores. A abordagem *privacy by design* representou um marco importante nesse contexto: proposta em 2009 por Ann Cavoukian, na Conferência Internacional de Comissários para a Proteção de Dados e Privacidade, uma organização de alcance global nesta matéria, que ainda hoje se reúne (desde 2019, designada por Assembleia Mundial da Privacidade).

Paralelamente, a «acessibilidade digital» tem sido outra frente relevante no contexto da modernização dos serviços públicos. Este termo refere-se ao princípio fundamental de proporcionar a todos os utilizadores virtuais uma igualdade de «oportunidade de uso, de forma amigável, digna e segura»[4],

1 República Portuguesa. 2021. «Resolução do Conselho de Ministros n.º 131/2021».

2 Conselho da Europa. 2018. «Convenção para a Proteção das Pessoas quanto ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108+)» Versão em português Conselho da Europa.

3 União Europeia. 2016. «Regulamento Geral sobre a Proteção de Dados».

4 Instituto Nacional para a Reabilitação. 2020. «Acessibilidade Digital» www.inr.pt .

permitindo que qualquer utilizador interaja com conteúdos digitais, independentemente de recorrer a diferentes estratégias de adaptação ou tecnologias de apoio. De acordo com a Diretiva 2016/2102 do Parlamento Europeu e do Conselho da União Europeia, os serviços digitais devem ser acessíveis a todos os utilizadores, incluindo aqueles com deficiência[5]. Portugal já havia despertado para este tema, legislando sobre o assunto ao longo das últimas duas décadas: em 1999, 2007, 2012 e 2018, com a transposição dessa diretiva pelo Decreto-Lei n.º 83/2018, refletindo o compromisso nas interações com os serviços públicos digitais[6]. Este processo evidencia que práticas digitais consideradas inacessíveis são discriminatórias, uma vez que limitam ou impedem determinados cidadãos de participar plenamente na sociedade.

A criação, em 2019, do «Selo de Usabilidade e Acessibilidade» (SUA) pela Agência para a Modernização Administrativa (AMA) e pelo Instituto Nacional para a Reabilitação[7] reforçou o empenho em proporcionar experiências positivas nas vertentes digitais dos serviços públicos, uma vez que este Selo certifica a conformidade com as melhores práticas de acessibilidade e usabilidade em *sites* e aplicações móveis. A «usabilidade» refere-se a uma disciplina de *design* de produto que fornece orientações para que a utilização de um produto seja, simultaneamente, eficaz e satisfatória para o seu utilizador. Esta área técnica complementa a acessibilidade, aplicando-se transversalmente no ambiente digital: inclui especificidades das interações dos utilizadores com aplicações ou interfaces, tais como a criação de uma experiência de navegação fluida ou a minimização das frustrações de quem os utiliza.

Problema de Investigação

O problema central que orienta esta investigação é a efetiva adequação das políticas e mecanismos de proteção da privacidade em meio digital, especialmente no contexto da Administração Pública portuguesa.

A pergunta geral de pesquisa inicial foi: 'A privacidade individual é adequadamente salvaguardada no ecossistema digital?' (Q1). Esta questão evoluiu para: 'As políticas de privacidade e outros mecanismos em vigor demonstram conformidade com uma abordagem centrada no utilizador para a proteção da privacidade?' (Q2A). A reformulação foi fundamentada na análise do conceito de *privacy by design* e seus princípios, que destacam a importância de uma abordagem proativa e centrada no utilizador. E fez surgir duas questões derivadas que orientaram a investigação para aspetos mais específicos: 'De que maneiras podemos observar e avaliar a conformidade das políticas de privacidade com uma abordagem centrada no utilizador?' (Q2B); e: 'Como podemos verificar a conformidade com a proteção da privacidade centrada no utilizador, na realidade portuguesa?' (Q2C).

Para responder à questão Q2B, foram procurados métodos e indicadores que avaliassem a conformidade das políticas de privacidade. Identificou-se que as formas de visualização e comunicação das políticas de privacidade, como painéis de controlo, certificações, rótulos, *pop-ups* e ícones de privacidade, servem como indicadores da sua eficácia. A «Lista Unificada de Atributos de Privacidade» de Susanne Barth, Dan Ionita e Pieter Hartel forneceu um quadro qualitativo para medir a importância atribuída a diferentes práticas de privacidade[8]. Adicionalmente, nesta fase emergiu a interrogação acerca do papel da conformidade e da intervenção do utilizador na eficácia das políticas de privacidade, expressa na questão: 'A conformidade para a proteção da privacidade está dependente da intervenção do utilizador ou os agentes responsáveis pelo desenvolvimento dos sistemas de informação sal-

5 União Europeia. 2016. «Diretiva (UE) 2016/2102 relativa à acessibilidade dos sítios web e das aplicações móveis de organismos do setor público».

6 República Portuguesa. 2018. «Decreto-Lei n.º 83/2018».

7 Portal ePortugal. 2019. «Foi lançado o Kit do Selo de Usabilidade e Acessibilidade».

8 Susanne Barth, Dan Ionita e Pieter Hartel. 2022. «Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines». ACM Computing Surveys 55, n.º 3.

vaguardam *a priori* a proteção da privacidade, independentemente da intervenção do utilizador?' (Q3).

Procurando respostas para a questão Q2C, foi identificada a Administração Pública portuguesa como um setor chave devido ao seu compromisso com serviços centrados no cidadão. A plataforma Mosaico da AMA[9] forneceu informações relevantes. Inicialmente, explorou-se o Selo de Maturidade Digital[10], mas a sua operacionalização revelou lacunas. Em contraste, o Selo de Usabilidade e Acessibilidade apresentou uma metodologia robusta que poderia ser adaptada para a privacidade *online*. Isso levou à formulação da questão: 'É possível realizar um diagnóstico da privacidade *online*, de modo semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4A) e suas questões operacionais, Q4B e Q4C, sobre ferramentas automáticas e manuais para diagnóstico da privacidade *online*.

Finalmente, o desenvolvimento da formulação do problema resultou na questão: 'O Selo de Usabilidade e Acessibilidade pode, ou não, contribuir para uma configuração mais robusta na salvaguarda da privacidade digital do utilizador?' (Q5).

Conseguimos observar os caminhos da interrogação de partida à questão principal, que originou o modelo de análise, representados na 'Figura 1.2 - Percurso da Pesquisa à Questão Central', no fim deste capítulo.

Objetivos da pesquisa

O objetivo principal deste trabalho, por conseguinte, é analisar se a aplicação dos princípios de acessibilidade e usabilidade, conjuntamente formalizada na certificação do SUA, pode promover a proteção da privacidade em *sites* e aplicações móveis da Administração Pública portuguesa.

Esta hipótese é refletida no Produto de Investigação 1 (PI1), projetado como ferramenta operacional, na forma de um formulário *online*, que permita às organizações extrair dados para um diagnóstico das suas práticas de privacidade *online*. Durante a fase de verificação de PI1, constatou-se que os indicadores desenvolvidos não atingiram completamente a finalidade da ferramenta e, devido à dificuldade em realizar a recolha e a análise de dados diretamente a partir do formulário PI1, emergiu como uma continuidade necessária o Produto de Investigação 2 (PI2), uma tabela de consulta derivada de PI1 que serve para verificação dos mesmos conteúdos de PI1 sem a necessidade de recolha ativa de dados. A tabela serve como uma ferramenta acessível para profissionais e especialistas envolvidos na conceção, desenvolvimento, e implementação de políticas de privacidade em projetos digitais, incluindo *sites* e aplicações móveis.

Desenho de investigação

A nossa investigação adotou uma abordagem metodológica mista, combinando análise qualitativa adiante enunciada, com um tratamento quantitativo de dados. Inicialmente, a pesquisa seguiu um método qualitativo para explorar as dimensões da privacidade digital, o que proporcionou uma formulação clara do problema e das hipóteses de trabalho, com base na revisão da literatura, bem como, a construção de um quadro teórico para guiar a recolha de dados para análise estatística, que por sua vez conduziu ao desenvolvimento de PI1, centrado na avaliação das características de privacidade digital. Este método quantitativo aplicado à verificação da experiência foi projetado para ser realizado por meio de recolha de dados via PI1, embora essa fase tenha sido ajustada com a observação preliminar do

9 A plataforma Mosaico foi desenvolvida pela Agência para a Modernização Administrativa (AMA) e visa apoiar as equipas da Administração Pública no desenho e desenvolvimento de serviços públicos digitais.

10 Os Selos de Maturidade Digital foram criados com o objetivo de certificar a maturidade digital das organizações em várias dimensões, concretamente: a da sustentabilidade, a da cibersegurança, a da acessibilidade e a da privacidade e proteção de dados pessoais.

fenómeno estudado, através de testes, o que fez incorporar no trabalho, novamente, com a proposta de utilização da tabela de consulta, PI2, um modo qualitativo.

Relevância e Originalidade do Estudo

O tema da salvaguarda da privacidade *online* diz respeito a todos os cidadãos utilizadores de serviços públicos digitais, na medida em que devem ver respeitados os seus direitos fundamentais, mesmo considerando que, na maior parte das vezes, não existe uma consciência ativa acerca destes assuntos, exceto quando ocorre algum acontecimento prejudicial. No nosso caso, desenvolvemos um particular interesse pelo tema da privacidade no decorrer do curso em que esta dissertação se insere, o Mestrado em Sociedade Digital, incentivado pela possibilidade de vir a desempenhar profissionalmente funções enquanto *designer* de *interfaces* visuais (*User interface*) e da experiência do utilizador (*User experience*). A tabela PI2, desenvolvida como parte deste trabalho, serve como uma ferramenta acessível para profissionais e especialistas envolvidos na conceção, desenvolvimento, e implementação de políticas de privacidade em projetos digitais, incluindo *sites* e aplicações móveis, tais como engenheiros de *software*, gestores de projetos digitais, consultores de privacidade, advogados de *compliance*, *designers* de *UX/UI*, responsáveis pela proteção de dados e Encarregados de Proteção de dados (ou *Data Protection Officers*). É importante notar, que este último é uma figura obrigatória para as entidades públicas desde a Lei 58/2019 que veio adaptar o RGPD à legislação portuguesa[11]. O facto de pensar a confluência de áreas, por si distintas, apresenta benefícios que permitirão poupar esforços no aperfeiçoamento da infraestrutura digital que decorre na Administração Pública, ao garantir que as práticas de privacidade estejam intrinsecamente ligadas à usabilidade e acessibilidade dos serviços oferecidos.

A privacidade digital é um campo dinâmico e em constante evolução, a capacidade das organizações em defini-la é testada à medida que novas tecnologias emergem e se tornam parte integrante da vida quotidiana. Este estudo tem como objetivo contribuir para a compreensão mais aprofundada dos desafios envolvidos na salvaguarda da privacidade em ambientes digitais.

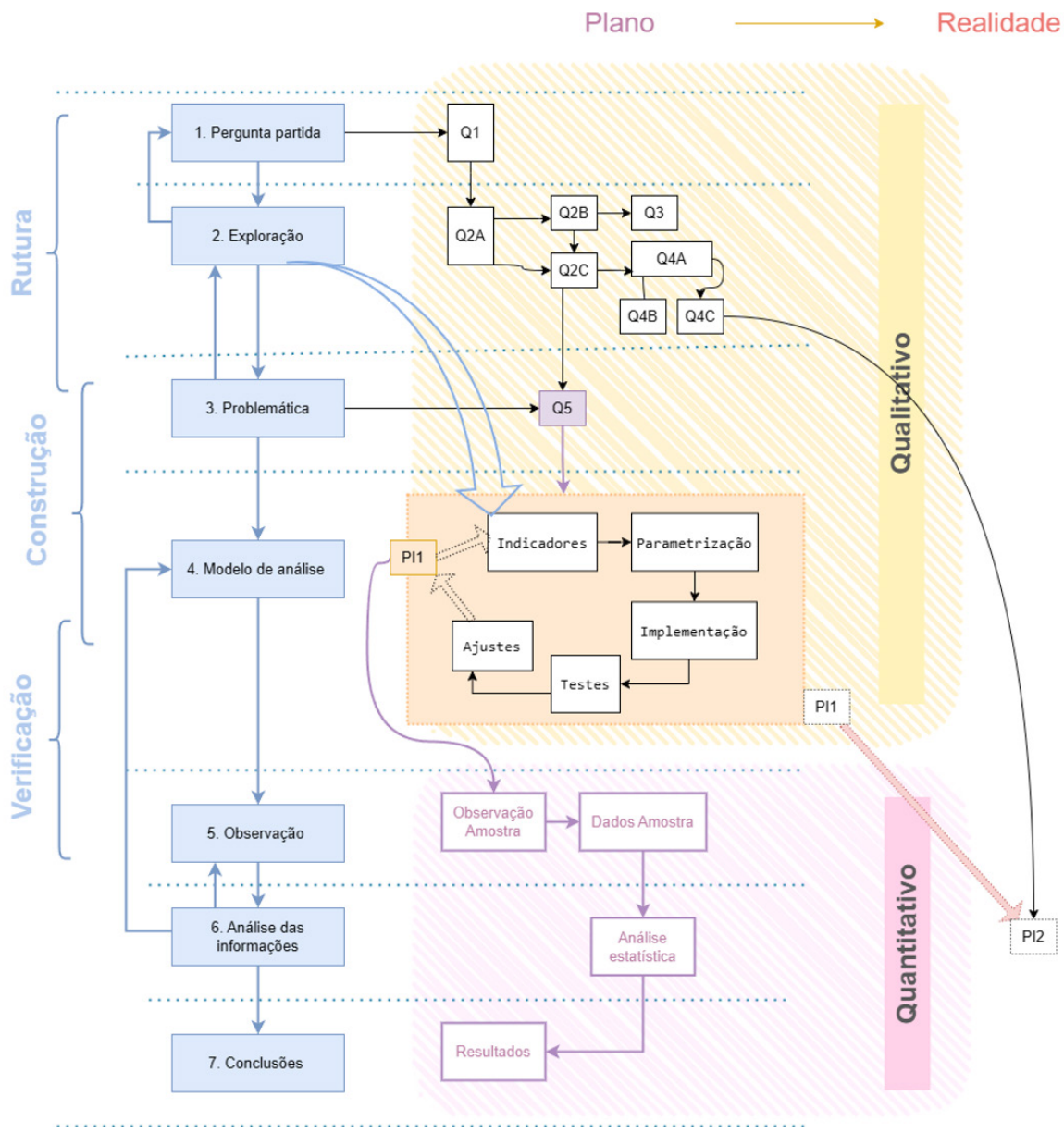
As próximas páginas decorrem numa estrutura composta por três partes principais: o capítulo 2, intitulado 'Enquadramento teórico', situa o contexto do estudo, relacionando o estado da arte à problemática que quisemos investigar; no capítulo 3, denominado 'Trabalho Empírico', descrevemos a metodologia geral adotada na pesquisa e os instrumentos utilizados, bem como o debate obtido a partir dos resultados; e por fim, no capítulo 4, chamado 'Conclusão', apresentamos os resultados organizados conforme as questões levantadas e a forma como estas foram satisfeitas face ao que foi previsto, e deixamos a sugestão de algumas explorações subsequentes do que foi feito.

Cada uma das três parcelas do roteiro da dissertação organiza-se em várias secções, descritas sucintamente no início de cada capítulo. Vamos de seguida passar à compreensão do tema da privacidade digital através do conhecimento existente.

A figura 1.1 ilustra o processo de investigação e as metodologias propostas.

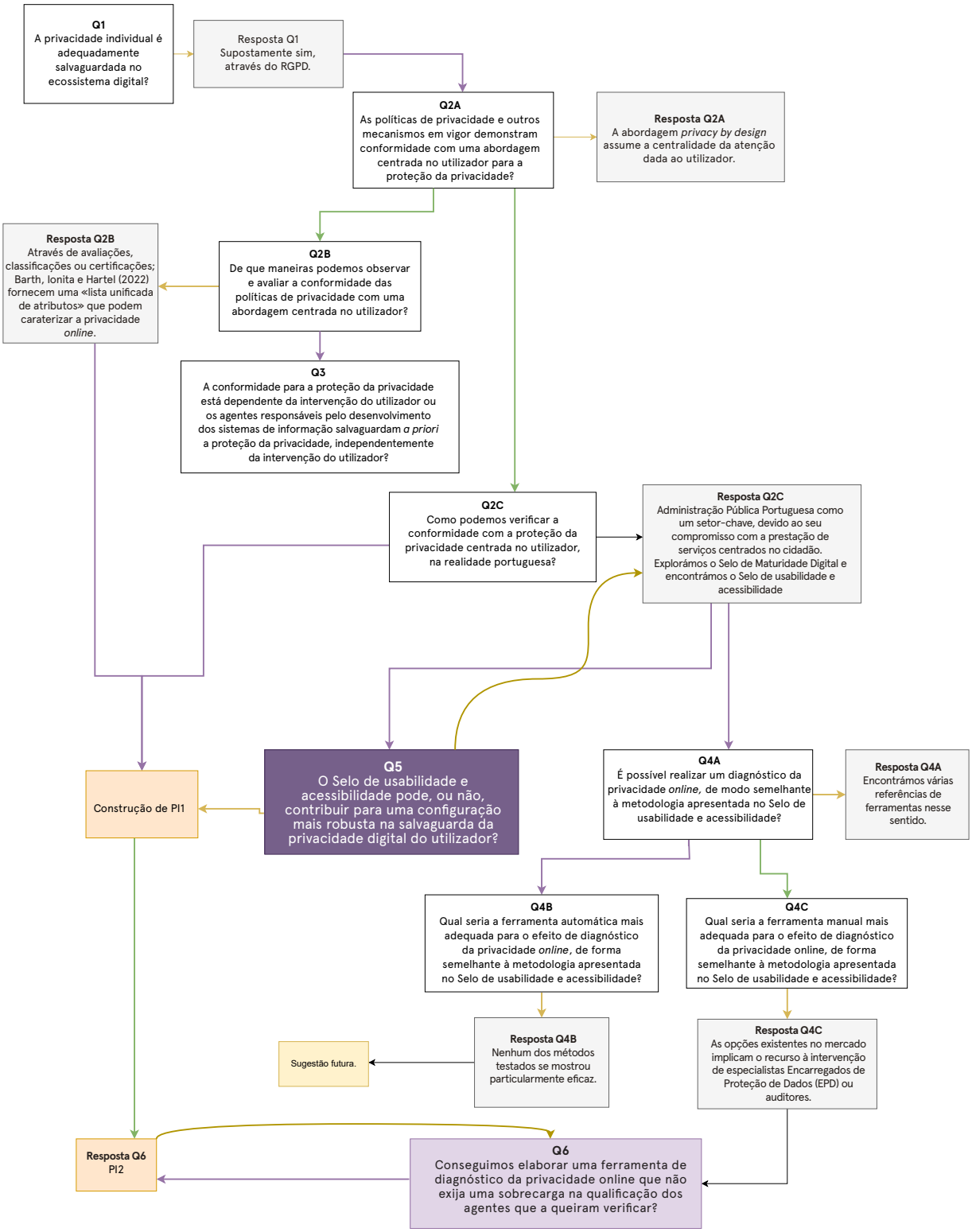
11 República Portuguesa. 2019. «Lei n.º 58/2019».

Figura 1.1 - Procedimento da investigação e metodologias programadas



Fonte: Rita V. Faria adaptado de «Os três actos e as sete etapas do procedimento metodológico de uma investigação científica» apresentados no *Manual de Investigação em Ciências Sociais* por Luc van Campenhoudt, Jacques Marquet e Raymond Quivy. 2019.

Figura 1.2 - Percurso da Pesquisa à Questão Central



CAPÍTULO 2

ENQUADRAMENTO TEÓRICO

Neste capítulo fazemos o enquadramento teórico em três partes.

Na primeira, 'Ecossistema digital no início do século XXI', começamos por contextualizar concisamente o assunto em que se insere a privacidade digital – iniciamos na secção 'Da *Internet* ao *Big Data*', continuamos em '*Big Data* e a cultura algorítmica' e prosseguimos para 'Desafios e implicações de uma economia digital baseada em dados'. Em seguida introduzimos o tema da 'Proteção da privacidade' deixando nota dos principais cenários do panorama internacional em 'Principais panoramas continentais na relação com a privacidade'; depois fazemos um enquadramento específico das 'Políticas de privacidade', das suas origens em 'Precursores da proteção da privacidade', que nos fornecem um ponto de partida para a exploração mais sistemática do problema, e abordamos o 'Papel do Encarregado da Proteção de Dados na promoção de uma cultura de privacidade nas organizações'. Posteriormente, em 'Estudos sobre as políticas de privacidade' investigamos o ângulo que nos parece o mais interessante e o mais pertinente para abordar o problema da privacidade digital (segundo a ótica *privacy by design*, com uma lógica centrada no utilizador) compreendendo melhor a especificidade das políticas de privacidade, nomeadamente quanto aos seus formatos de apresentação, descritos em 'Formatos de políticas de privacidade' e os elementos básicos que caracterizam as políticas de privacidade, em 'Fundamentos da privacidade *online*', ficando a conhecer a «Lista Unificada de Atributos de Privacidade» de Barth, Ionita e Hartel (2022).

Na segunda parte, a problemática é trazida para o contexto português. Primeiro situando-nos genericamente na 'Conjuntura digital da Administração Pública nacional' quanto à relevância da questão dos diagnósticos e avaliações contínuas. Desta delimitação descrevemos uma fonte de informação útil para o desenho da metodologia do trabalho empírico em 'Mosaico, modelo comum de Portugal', através do qual conhecemos as certificações dos 'Selos de Maturidade Digital' e do 'Selo de Usabilidade e Acessibilidade', que deixamos descritos. Depois percorremos brevemente os contornos específicos dos temas da 'Inclusão e acessibilidade digital', bem como o da 'Usabilidade'.

Na terceira parte, 'Síntese das questões de investigação', assinalamos a sequência das perguntas formuladas que nos permitiu apurar a hipótese explorada no capítulo seguinte.

2.1 ECOSSISTEMA DIGITAL NO INÍCIO DO SÉCULO XXI

2.1.1 DA INTERNET AO *BIG DATA*

A expansão da *Internet* facilitou o acesso e a partilha de informações, tornando-se uma infraestrutura essencial para a comunicação e para a troca de dados à escala global. A expressão «sociedade em rede» descreve uma forma de organização social caracterizada pela multiplicidade de vínculos horizontais, distribuídos ao longo das redes de comunicação, as «conexões». A maneira dinâmica e descentralizada como a informação flui nesta rede permitiu maior diversidade de atores na participação e acesso a informações, por contraste com estruturas tradicionais como os meios de comunicação social, onde a informação pode ser mais estática e centralmente controlada. Estes «fluxos de comunicação»

moldam de tal forma o poder e a dinâmica social, que o capitalismo contemporâneo é em boa parte impulsionado pela produção, distribuição e acumulação de informações[1].

As conexões decorrentes da utilização da *Internet* têm sido um catalisador de transformações profundas na configuração da economia contemporânea. Anteriormente à ascensão das plataformas *online*, como a Google, a Amazon ou a Meta, o modelo de negócios predominante baseava-se em transações convencionais, tais como a compra e venda de produtos ou de prestação de serviços. O modelo centrava-se em publicidade contextual, onde os anúncios eram exibidos com base na recorrência de palavras-chave pesquisadas pelos utilizadores. Em 2000, a Google lançou o serviço publicitário AdWords que permitiu às empresas comprarem anúncios com base em palavras-chave específicas. Esta mudança marcou o início da rentabilização direta do mecanismo de busca da Google e viria a desencadear um novo paradigma dos modelos de negócios das plataformas digitais, focado nos lucros permitidos pela recolha e comércio de dados, onde a informação sobre utilizadores, e seus comportamentos, se tornou um ativo-chave[2].

As empresas reconheceram potencial nos dados originados pelos utilizadores. Não apenas como um subproduto das interações *online*, mas como uma valiosa fonte de informação sobre o comportamento humano. As redes sociais aumentaram a quantidade de dados produzidos, o que facilitou ulteriormente a publicidade direcionada e as análises de mercado[3].

Simultaneamente, a maior quantidade de informação produzida requisitou meios adicionais para armazenar, analisar e compreender os dados disponíveis. Genericamente, o termo *Big Data* refere-se a essa capacidade de recolher e armazenar quantidades massivas de dados para análise, através de técnicas de computação avançadas, conferindo valor económico aos conhecimentos extraídos, embora a expressão *Big Data* seja extensamente discutida na literatura de várias disciplinas e a sua definição possa variar consoante o âmbito da sua aplicação[4].

Estamos hoje familiarizados com inúmeros produtos gratuitos, outrora opcionais, e que hoje constituem ferramentas básicas que participam no trabalho e na vida social de todos. Todas essas aplicações gratuitas têm na retaguarda uma quantidade enorme de dados, acerca dos utilizadores e dos seus comportamentos, que são usados para criar os perfis que os anunciantes pagam para ter acesso. O modelo de negócio da publicidade é um motor económico da tecnologia. Durante séculos, o acesso à informação cumpriu um papel importante no desenvolvimento e crescimento da civilização. Contudo, a transformação impulsionada pelo aumento da capacidade de armazenamento combinada com capacidades computacionais cada vez mais rápidas e eficientes, resultou em desenvolvimentos paralelos que trouxeram novas proporções à gestão e interpretação de dados no século XXI, nomeadamente a partir da década de 2010, contribuindo para a acumulação do *Big Data*.

2.1.1.1 *BIG DATA* E A CULTURA ALGORÍTMICA

Para uma compreensão cabal acerca do que é o *Big Data*, torna-se útil percebermos as dimensões que orientam o seu potencial em diversos campos de investigação. As propriedades fundamentais que moldam a eficácia e a aplicabilidade do *Big Data* em diferentes contextos, são comumente conhecidas como «os V's do *Big Data*»[5]. Entre essas dimensões, destacam-se: 1) «o valor», que ressalta a importân-

1 Manuel Castells. 2007. *A Era da Informação: Economia, Sociedade e Cultura.*

2 Robert Graham. 2017. «Google and Advertising: Digital Capitalism in the Context of Post-Fordism, the Reification of Language, and the Rise of Fake News».

3 Giuseppe Aceto, Valerio Persico e Antonio Pescapé. 2019. «A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges».

4 Saswat Sarangi e Pankaj Sharma. 2020. *Big Data: A Beginner's Introduction.*

5 Hafiz Suliman Munawar et al. 2022. «Big Data in Construction: Current Applications and Future Opportunities».

cia de extrair insights valiosos e significativos; 2) «o volume», referindo-se à escala maciça de dados; 3) «a velocidade», que destaca a necessidade de processamento rápido e análise em tempo real; 4) «a variedade», abrangendo diferentes tipos de dados estruturados e não estruturados; 5) «a veracidade», indicando a fiabilidade e precisão dos dados; 6) «a volatilidade», considerando a instabilidade temporal dos dados; 7) «a validade», garantindo a autenticidade e integridade das informações; 8) «a variabilidade», reconhecendo a diversidade nos padrões de dados; 9) «a vulnerabilidade», alertando para possíveis riscos e ameaças à segurança; 10) e, por fim, «a visualização», reforçando a importância de representar dados de maneira acessível e compreensível. O foco desta dissertação incide principalmente sobre estas duas últimas dimensões, nomeadamente a vulnerabilidade e a visualização dos dados.

Entre as etapas implicadas no *Big Data* estão abrangidas a recolha, o armazenamento, a classificação e o refinamento de dados. Muitas vezes os dados apresentam-se num formato não estruturado, o que significa que é difícil identificar padrões, a menos que sejam classificados e tornados mais estruturados. Para os poder compreender e interpretar, os conjuntos de dados devem primeiro ser tornados gerenciáveis, conforme salientado por Saswat Sarangi e Pankaj Sharma. Estes autores descrevem o processo típico da análise de dados como um ciclo, que permite encontrar pontos de referência «significativos e acionáveis», comparando-o ao encontrar «da agulha num palheiro»[6]. Este ciclo compreende a conversão inicial de dados não estruturados em dados estruturados, seguida pela sua análise para obter perspetivas acionáveis, de modelos de previsão que permitam antecipar eventos futuros, continuando até à avaliação dos resultados obtidos e, por fim, proporcionar adaptações em processos, com base nas conclusões extraídas[7].

As técnicas que melhor demonstram as capacidades no processamento de *Big Data* podem ser definidas em seis categorias[8]: 1) aprendizagem automática (*machine learning*) e técnicas de mineração de dados *(data mining)*[9]; 2) computação em nuvem; 3) análise de redes semânticas/extração de dados da *web (web scraping)*; 4) técnicas de visualização; 5) técnicas matemáticas e estatísticas e; 6) técnicas de otimização. A base que permite a aplicação destas técnicas avançadas de *Big Data* são os algoritmos. Um algoritmo é uma sequência de instruções lógicas, expressas numa «linguagem de programação de alto nível», que resolve problemas ou executa tarefas determinadas, funcionando como uma «máquina calculadora abstrata» que contém a fórmula de uma lei aplicável (função). Quando vários algoritmos interdependentes são combinados, formam um programa de computador (*software*), que instrui componentes de *hardware (*componentes microeletrónicos) a interagir com *software* para executar funções específicas[10]. Por sua vez, o que permite a aprendizagem automática é a capacidade de os algoritmos, enquanto conjunto de passos e de etapas na resolução de um problema ou na realização de uma tarefa, se poderem adaptar aos dados de que dispõe, reprogramarem-se a si mesmos e aperfeiçoarem-se, descobrindo e aplicando fórmulas mais eficazes.

A quantidade de informações, organizadas e não organizadas, que compõem os conjuntos de dados digitais é tão extensa que a sua gestão eficiente exigiu novas formas de especialização em áreas como as tecnologias da informação e comunicação, análise de dados ou estratégia empresarial. Ao longo do tempo, a análise de dados transitou do escrutínio das características inerentes aos conjuntos de dados em relação às tecnologias vigentes, para tecnologias projetadas com vista à extração de valor

6 Sarangi e Sharma. 2020.

7 Ibid.

8 Azlinah Mohamed et al. 2020. «The State of the Art and Taxonomy of Big Data Analytics: View from New Big Data Framework».

9 «Mineração de dados» consiste na prática de analisar enormes conjuntos de dados para gerar nova informação.

10 Paulo Nuno Vicente. 2023. *Os Algoritmos e Nós*.

económico a partir de volumes muito grandes e variados de dados. Este desenvolvimento possibilitou mecanismos de captura, análise e descoberta em alta velocidade[11].

Viktor Mayer-Schönberger e Kenneth Cukier sustentam que a sociedade moderna está a passar por uma significativa transformação com a crescente influência do *Big Data*, impulsionada pela capacidade de identificar padrões e relações anteriormente não reconhecidos, remodelando assim a compreensão da informação na vida social contemporânea[12]. Quase todos os setores da sociedade e da economia foram atingidos por este fenómeno, e muitas definições convencionais da forma como vivemos, são moldadas pelas perceções desenvolvidas a partir do *Big Data*. Áreas como a ciência, a indústria ou os serviços públicos, beneficiam do conhecimento útil extraído a partir de grandes e complexos conjuntos de dados, através de técnicas e ferramentas avançadas de análise de dados que detetam inferências no conhecimento. Concretamente, é através de algoritmos analíticos, serviços, ferramentas de programação ou aplicações inteligentes e expansíveis, que se encontram padrões e tendências[13], tornando um conhecimento escondido em visível.

A Inteligência Artificial é um campo de investigação e desenvolvimento que apareceu oficialmente em 1956 com o objetivo de simular aspetos da aprendizagem e outras características da inteligência humana em máquinas. Ao longo do tempo, a ambição em atingir uma «inteligência computacional» capaz de equivaler a uma «inteligência natural» passou por várias fases, incluindo: uma primeira geração focada no raciocínio lógico e na modelação do funcionamento do cérebro humano (as redes neuronais artificiais); uma segunda geração, desenvolvida entre as décadas de 1970 e 1980, dedicada a inteligências específicas e à criação de programas baseados na codificação do conhecimento especializado (sistemas especialistas, ou periciais); e uma terceira geração, que é a atual, «baseada na resolução de problemas específicos e caracterizada pelo recurso intensivo a enormes conjuntos de dados digitais (*big data*) e à aprendizagem automática»[14]. Estes três caminhos coexistem hoje em dia, desenvolvendo modos próprios de criar e aplicar algoritmos.

Em menos de vinte anos, os sistemas algorítmicos mudaram de um estado latente para uma presença cada vez mais participativa no mundo económico, laboral e da vida quotidiana, impulsionando uma transformação digital em diversos setores. Esta era, designada «Quarta Revolução Industrial – a primeira a ser anunciada antes de acontecer»[15], é notavelmente marcada pela conectividade e análise de dados em tempo real. Inclui uma profusão de tecnologias como a Inteligência Artificial, a robótica, a *Internet* das Coisas (*Internet of Things*), os veículos autónomos, a impressão 3D, a nanotecnologia, a computação quântica, entre outras.

Reconhece-se que hoje, graças à circulação de dados e a algoritmos de aprendizagem automática, desfrutamos de serviços e benefícios sem precedentes. Mas as arquiteturas de informação, desenvolvidas por engenheiros, por vezes acabam por ter usos não previstos que impactam a sociedade. Assinalamos de seguida algumas novas ameaças emergentes.

2.1.2 DESAFIOS E IMPLICAÇÕES DE UMA ECONOMIA DIGITAL BASEADA EM DADOS

Neste cenário contemporâneo em que se evidencia uma notável transição da *Internet*, originalmente concebida como uma ferramenta de comunicação e acesso à informação, para um modelo de negócios centrado na exploração do *Big Data*, emergiu a noção de «capitalismo de vigilância», cunhada

11 Aceto, Persico e Pescapé. 2019.

12 Viktor Mayer-Schönberger e Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work, and Think.*

13 Marozzo e Talia. 2023. «Perspectives on Big Data, Cloud-Based Data Analysis and Machine Learning Systems».

14 Vicente. 2023.

15 Ibid.

por Shoshana Zuboff. Na sua conceção, a autora destaca-o como uma «nova ordem económica»[16]. A forma dominante de capitalismo na atual «sociedade da informação», segundo a qual, a economia global se move na direção de uma nova lógica de acumulação, que se apropria da experiência humana como matéria-prima gratuita para a previsão comportamental. O capital incorporado no mercado é, neste caso, a informação extraída em larga escala pelas empresas. Enquanto a vigilância implícita no conceito se refere à ocultação dos mecanismos de captação e de transformação da experiência humana privada, mecanismos esses que alimentam os sistemas de produção e de valorização do capital. Zuboff defende que este modelo económico ameaça a privacidade individual, ao criar uma desigualdade social entre os grupos económicos e os utilizadores, que pode mesmo comprometer a autonomia e liberdade destes últimos. Para Zuboff não teria de ser necessariamente assim (tradução nossa):

> Na altura, a Google tinha muitas outras opções em cima da mesa para abrir caminho à rentabilização muitas outras opções. Essas opções teriam exigido um período mais longo de exploração, tentativa e erro, e eventual institucionalização. Mas eles encontraram este modelo, e funcionou, e nunca mais olharam para trás…[17].

Couldry e Mejias consideram a questão da vigilância digital como marcada por uma permissividade alarmante, destacando que o custo da conectividade através de aplicações, plataformas e objetos inteligentes é elevado e merece ser contestado. Não apenas porque a interferência proveniente da tradução constante das nossas vidas em dados digitais se estende a muitos aspetos da vida privada. Nomeadamente através do controlo de formas de conhecimento, de meios de produção e até de possibilidades de participação política. Como, por se tratar de um processo que permite adquirir (a partir das ligações digitais) e transferir por meios obscuros, grandes quantidades de dados pessoais a empresas, frequentemente provenientes de países mais desenvolvidos, que os utilizam para gerar lucro. Factos que ecoam a dinâmicas semelhantes às do colonialismo, com práticas históricas de exploração de recursos em regiões colonizadas, daí apelidando de «colonialismo de dados» a extração e monetização de dados, pois não traz benefícios equitativos para as comunidades de origem e perpetua as relações desiguais de poder[18].

Neste sentido, Sarangi e Sharma sustentam que a democratização do acesso ao *Big Data*, é um desafio importante para os governos e decisores políticos, para que os benefícios não fiquem circunscritos a um determinado setor da sociedade ou da economia. Sobretudo porque as grandes empresas tecnológicas procuram atingir o sucesso segundo a lógica de «o vencedor leva tudo», açambarcando os recursos e ganhos, e deixando poucas vantagens para os concorrentes. Tornando-se, então, crítico «empreender esforços sinceros para reduzir a desigualdade criada entre ricos e pobres no que diz respeito à capacidade de aceder e analisar dados»[19]. Ao mesmo tempo, é igualmente necessário repensar os processos pelos quais os próprios Estados nacionais podem participar competitivamente e contrabalançar o poder acumulado pelas grandes empresas tecnológicas.

Para Evgeny Morozov, segundo Hernandez V. Eichenberger, o desafio maior não estará tão centrado na questão de vigilância em si, mas sim nas consequências políticas do capitalismo de vigilância[20]. Para

16 Shoshana Zuboff. 2020. *A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira de poder*.

17 Shoshana Zuboff et al. 2019. «Surveillance Capitalism: An Interview with Shoshana Zuboff». Tradução nossa.

18 Nick Couldry e Ulises A. Mejias. 2019. «Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject».

19 Sarangi e Sharma. 2020.

20 Hernandez Vivan Eichenberger. 2020. «Resenha de "Big Tech: A Ascensão Dos Dados e a Morte Da Política" de Evgeny Morozov».

este autor os algoritmos não são capazes de narrar historicamente toda a realidade vivida, pois simplificam a complexidade da vida social. Morozov argumenta que o controlo massivo de dados por grandes empresas tecnológicas pode moldar e influenciar as decisões políticas e sociais de maneira preocupante, exigindo a atenção urgente para a regulamentação e proteção da democracia. Tendo em conta que «a acumulação de dados digitais relativos a comunidades humanas e o seu processamento por recurso a algoritmos é uma forma de poder»[21], compreende-se facilmente a ideia de que a mercantilização de muitos aspetos da vida privada limite o debate público e intervenção cidadã.

Outro desafio para as democracias, ampliado pelo efeito do *Big Data*, é a desinformação. O capitalismo digital e as plataformas tecnológicas têm contribuído significativamente para a disseminação de informação e a formação em ambientes *online* de «bolhas de filtro» ou «câmaras de ressonância»[22]. As empresas tecnológicas dominantes exploram a manipulação algorítmica dos dados e a segmentação de audiência para direcionar campanhas de desinformação e promover interesses comerciais e políticos[23] criando um ambiente propício à reafirmação de posições não abertas ao diálogo crítico, em que os utilizadores são expostos apenas a informações que reforçam as suas opiniões políticas, protegidos pela informação previamente filtrada e permanecendo isolados de outros utilizadores com convicções opostas (câmaras de ressonância) e no limite, atingindo uma radicalização política[24]. A *Internet* permitiu que desaparecessem as limitações de espaço e tempo disponíveis para a comunicação do pensamento, e Helena Martins Barreto sustenta que as plataformas digitais têm emergido como agentes centrais numa nova estrutura de mediação social, utilizando dados, publicidade e circulação mediada de conteúdos para influenciar a disseminação de informações[25]. O capitalismo de vigilância articula-se com esta economia política de desinformação, através do tráfego de dados obtidos pela subjugação voluntária a um contante escrutínio algorítmico[26]. Para Morozov, as *fake news*, *per si*, não são o problema, já que estas são fruto do capitalismo digital contemporâneo e argumenta que a solução para a desinformação é repensar o capitalismo digital, numa realidade em que a publicidade não tenha tanta influência sob as vidas dos cidadãos e que estes tenham maior poder de decisão[27].

Uma forma significativa de desinformação é a difusão de *deepfakes*[28] facilitada pelo funcionamento dos novos modelos de Inteligência Artificial generativa. São um novo formato de informação que depende de grandes volumes de dados na medida em que é necessário um vasto conjunto destes para treinar modelos que consigam replicar padrões específicos de movimento, expressões faciais, voz e outras características pessoais. Maria Pawelec reconhece um potencial ameaçador das *deepfakes* por afetar os governos em algumas «funções democráticas de núcleo»[29], desempenhadas através de práticas e ações sociais como o sistema de voto, a representação ou a escolha. As *deepfakes* fragilizam a base factual da deliberação ao suscitar a dúvida sobre o que se vê e se ouve, e podem contribuir

21 Vicente. 2023.

22 Seth Flaxman, Sharad Goel e Justin M. Rao. 2016. «Filter Bubbles, Echo Chambers, and Online News Consumption».

23 Thiago Henrique de Jesus Silva. 2024. «A Desinformação como Instrumento de Dominação Capitalista».

24 Eliana Sanches de Frias. 2022. «Inteligência artificial, desinformação e populismo digital: Como as plataformas digitais impulsionam os movimentos de extrema direita».

25 Helena Martins do Rêgo Barreto. 2024. «Desinformação em meio à crise do capitalismo e à configuração de uma nova estrutura de mediação social».

26 Julian Affonso de Faria e Cláudio Márcio Magalhães. 2021. «O Capitalismo de Vigilância e a Política da Desinformação».

27 Mayara Mayumi Sataka e Matheus Felipe Silva. 2021. «Big Tech. A ascensão dos dados e a morte da política».

28 Vídeos e audios sintéticos gerados por Inteligência Artificial que parecem extremamente reais e podem enganar as pessoas.

29 Maria Pawelec. 2022. «Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions».

para decisões enviesadas. Por instalarem a dúvida quanto aos factos partilhados e à sua verdade, não só enfraquecem a sua certeza como contribuem para a queda da confiança baseada na informação.[30]

O cibercrime representa outra vertente das preocupações relevantes de uma economia assente em grandes volumes de dados, trazendo ameaças que afetam o ciberespaço. Genericamente, refere-se ao conjunto de atividades ilegais realizadas por meio de tecnologias digitais e redes de comunicação. Em Portugal, de acordo com o Relatório sobre Riscos e Conflitos do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (2024), as práticas de cibercrime que no último ano afetaram tanto indivíduos quanto organizações, incluíram: 1) a utilização de *software* malicioso que impede o acesso a dados ou dispositivos da vítima, exigindo um resgate para desbloqueio (*ransomware*), habitualmente pago em criptomoedas; 2) técnicas de engenharia social para enganar os recetores de *emails* (*phishing*), de mensagens de texto (*smishing*) ou de chamadas telefónicas (*vishing*) para obtenção de credenciais confidenciais; 3) uma variedade de burlas e esquemas fraudulentos, para enganar funcionários ou outras pessoas e obter transferências de dinheiro e informações sensíveis; 4) o comprometimento de contas, que consiste na tentativa de aceder de forma não autorizada a contas de utilizador, muitas vezes através de tentativas automatizadas; 5) e a exploração de vulnerabilidades que consiste em aproveitar falhas de segurança em *software* e sistemas para causar danos ou obter acesso não autorizado.

Em suma, a transição para uma economia digital impulsionada pelo *Big Data* trouxe enormes oportunidades, mas também desafios sem precedentes, como o aumento da vigilância, do cibercrime e da desinformação. Este novo modelo de economia, ao apropriar-se da privacidade e da experiência humana para fins comerciais, ameaça direitos fundamentais como a autonomia individual e a liberdade. A crescente desigualdade no acesso e controlo de dados, aliada à manipulação algorítmica, reforça a necessidade de repensar e continuar a regulamentar este cenário. O professor e investigador em Media Digitais, Paulo Nuno Vicente, assinala a perceção pública de que a próxima década trará desenvolvimentos importantes na «maturação cívica de uma literacia relativa à Inteligência Artificial e tecnologias relacionadas, a qual não se esgota na compreensão técnica acerca do funcionamento interno dos sistemas algorítmicos, mas inclui decisivamente considerações abrangentes, informadas e críticas sobre questões sociais, culturais, socioeconómicas e políticas decorrentes»[31].

Através da referência a estes debates, procurámos ilustrar como a privacidade é um dos elementos trazidos à superfície, na interseção das relações de poder que a tecnologia envolve. Foi em torno deste tema que a nossa pesquisa se articulou, examinando um pouco mais acerca das formas pelas quais, possivelmente, a privacidade individual é salvaguardada, dado o conhecimento prévio e experiência concreta enquanto utilizadores comuns do ecossistema digital.

2.1.3 PROTEÇÃO DA PRIVACIDADE

A relação entre a privacidade e a sociedade sempre existiu, «as pessoas exercem a privacidade por meio de preferências e práticas acerca de informação pessoal que são específicas dos contextos sociais e que mudam ao longo do tempo»[32]. Três principais fatores impulsionadores, da era da informação, podem afetar a privacidade:

30 As *deepfakes* não são necessariamente produzidas com um fim nefasto. Podem surgir como ferramentas úteis para a educação, ser desenvolvidas para servir um negócio, ou simplesmente resultar sem nenhuma destas intenções. Chris Umé, autor de um dos maiores sucessos de *deepfakes* – Deepfake Tom Cruise no Tik Tok – afirmou que o objetivo por trás do seu trabalho é «entreter as pessoas e mostrar o que é possível fazer (com as redes neurais artificiais), aumentar a consciencialização e indicar onde isto vai dar» (How synthetic media, or deepfakes, could soon change our world, 2021).

31 Vicente. 2023.

32 Whalstrom et al. citado por Vinícius Camargo Andrade et al. 2022. «Privacy by Design and Software Engineering: A Systematic Literature Review».

as mudanças tecnológicas, as mudanças sociais e as descontinuidades nas circunstâncias[33]. Estes fatores, individualmente e em conjunto, alteram e expandem-se a uma velocidade sem precedentes, modificando os termos da nossa compreensão sobre o mundo em geral, e para a nossa privacidade, em particular.[34] Por serem tão significativas e causadoras de inquietude, é compreensível que as mudanças decorrentes da variação destes fatores decisivos, profundamente interligados, conduzam ao surgimento de novos direitos, como de resto aconteceu em várias ocasiões ao longo da História. Sendo então o próprio direito à privacidade, um direito social altamente contextual[35].

Importa salientar que praticamente todas as informações têm o potencial de assumir uma natureza pessoal, englobando diversos domínios, tais como biográficos, biológicos, genealógicos, históricos, transacionais, locacionais, relacionais, computacionais, vocacionais ou de reputação. Uma grande parte dos dados que compõem a «força vital da nova economia»[36] é identificável, ou seja, relaciona-se com qualquer informação associada a uma pessoa reconhecível. A possibilidade de identificação pode ocorrer de forma direta ou indireta, abrangendo informações que, isoladamente, não identificam uma pessoa, mas que, quando combinadas ou usadas com outras informações, podem conduzir à sua identificação. Daí serem entendidos como «dados pessoais» *(personal data*) ou, dependendo da abordagem específica adotada por determinada lei ou regulamentação, encontra-se também o termo sinónimo «informações de identificação pessoal» (P*ersonally Identifiable Information*).

Embora dados isolados possam parecer inócuos, a sua combinação pode revelar padrões e informações que, de outra forma, permaneceriam ocultos. O cruzamento de dados permite uma análise mais aprofundada e uma compreensão mais alargada do fenómeno em estudo. Um exemplo paradigmático ocorreu nos Estados Unidos, quando uma cadeia de lojas, através da análise dos hábitos de compra dos seus clientes, conseguiu prever a gravidez de uma jovem adolescente antes da sua família o saber, enviando-lhe publicidade relacionada com produtos para bebés. Este tipo de prática demonstra como o cruzamento de dados aparentemente irrelevantes — como a compra de produtos específicos — pode gerar conclusões sobre aspetos privados da vida de um indivíduo.

De igual modo, técnicas como o *browser fingerprinting* utilizam informações triviais, como o tipo de navegador, o sistema operativo ou o idioma do utilizador, para criar uma impressão digital única que permite a sua identificação. Já a análise de metadados, como o horário de envio de uma mensagem ou a localização de uma chamada, pode revelar padrões comportamentais, independentemente do conteúdo da comunicação. Os *pixels* de monitorização são outro exemplo: monitorizam acções como a abertura de *e-mails* e, quando combinados com outros dados, permitem a construção de perfis detalhados. Estes exemplos demonstram como a combinação de dados aparentemente inofensivos pode comprometer a privacidade, ao permitir a identificação ou o seguimento de indivíduos de forma inesperada e, muitas vezes, sem o seu consentimento explícito.

33 James Waldo Herbert S. Lin e Lawrence H. Cox. 2010. «Engaging Privacy and Information Technology in a Digital Age».

34 Podemos pensar na pandemia Covid-19 como um exemplo de situação onde as normas de privacidade foram temporariamente ajustadas: não só se verificou o desenvolvimento e a implementação rápida de uma profusão de tecnologias, como o comportamento social sofreu alterações em prol da saúde pública; governos e organizações implementaram medidas que, em tempos normais, poderiam ser vistas como invasivas, mas que foram aceites devido à emergência global e à necessidade de transpor as consequências da crise sanitária.

35 Sobre as principais vertentes dos direitos fundamentais adaptados às exigências e ameaças sentidas pelas pessoas no universo digital ouça-se o podcast da série «Da Capa à Contracapa» realizado pela Fundação Francisco Manuel dos Santos, moderado pelo jornalista José Pedro Frazão «Como garantir direitos fundamentais na Era Digital?» (16 Janeiro 2024)

36 Ann Cavoukian e Michelle Chibba. 2018. «Start with Privacy by Design in All Big Data Applications».

Complementarmente, dados sensíveis são informações pessoais que requerem proteção especial devido ao seu potencial discriminatório e impacto nos direitos fundamentais[37]. A União Europeia considera sensíveis várias categorias de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como os dados genéticos, os dados biométricos tratados unicamente para identificar uma pessoa de forma inequívoca, os dados relativos à saúde, ou dados relativos à vida sexual ou orientação sexual de uma pessoa[38]. A nível global, a maioria dos países segue o modelo europeu para classificar os dados sensíveis, com divergências em torno da inclusão dos registos criminais; embora os dados de saúde sejam os mais amplamente classificados como sensíveis em termos legais, na prática, os dados financeiros são os mais violados em casos de roubo ou fuga de informação, refletindo o seu alto valor comercial e a crescente utilização em transações fraudulentas[39]. Adicionalmente, o conceito de dados sensíveis pode estar em evolução, decorrente dos avanços tecnológicos, que alegadamente converte mais dados em potencialmente sensíveis[40].

Pode ser tentador reutilizar dados recolhidos num contexto específico para um propósito diferente do qual foram obtidos, e essa vontade pode acontecer tanto na investigação científica académica como no desenvolvimento de produtos comerciais ou na elaboração de perfis individuais[41]. Mas tal situação desvenda um possível conflito entre os interesses pessoais dos titulares dos dados e os interesses de investigadores, ou os interesses de intervenientes empresariais que procuram obter a propriedade intelectual sobre a informação, ou do interesse público que pode alegar a defesa do proveito das informações para benefícios sociais do progresso científico.

A forma de resolver estas tensões através do direito, assenta muito na vontade de equilibrar o avanço tecnológico com a proteção dos direitos individuais, garantindo que as pessoas mantenham o controle sobre as suas informações num ambiente digital em constante evolução. De resto, esta preocupação não surge hoje. O direito fundamental à autodeterminação informativa, derivado de uma decisão de 1983 do Tribunal Constitucional Alemão, constitui uma das primeiras abordagens legais à proteção da privacidade. Em termos simples, concedeu às pessoas, em vez dos governos, o poder de decidir o destino das suas informações pessoais.

Além disso, a privacidade da informação abrange tanto a forma como a informação é protegida e acedida, mas também os modos pelos quais é recolhida e utilizada. Portanto a abrangência do direito engloba o controlo do indivíduo sobre a recolha, utilização e divulgação, por parte de terceiros, das suas informações pessoais. E, de certa forma, a proliferação das aplicações de *Big Data* e outras tecnologias de comunicação de informações vieram alterar a noção de informação pessoal, pois nem sempre as pessoas se apercebem da interferência na sua esfera privada, como consequência do que partilham.

Por outro lado, reconhecemos que a privacidade é controlada de forma pervasiva por entidades que não são o próprio indivíduo produtor de dados. Alguns pensadores contemporâneos adicionam mesmo a ideia de que a privacidade está a morrer ou está, já, efetivamente, morta[42]. Esta alusão à erosão da esfera privada provocada por uma nova economia de dados pode ser compreendida se restrin-

37 Caitlin Sampaio Mulholland. 2018. «Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)».

38 União Europeia. 2016. «Regulamento (UE) 2016/679».

39 Min Wang e Zuosu Jiang. 2017. «The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World».

40 Paul Quinn e Gianclaudio Malgieri. 2021. «The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework».

41 Nissenbaum citado por Bart Jacobs e Jean Popma. 2019. «Medical Research, Big Data and the Need for Privacy by Design».

42 Ann Cavoukian, Scott Taylor e Martin E. Abrams. 2010. «Privacy by Design: Essential for Organizational Accountability and Strong Business Practices».

girmos a definição de privacidade ao direito de o indivíduo aceder e controlar os seus dados pessoais no que diz respeito à recolha, utilização e transferência dos mesmos.

2.1.3.1 PRINCIPAIS PANORAMAS CONTINENTAIS NA RELAÇÃO COM A PRIVACIDADE

Ainda antes de desenvolvermos o tema da privacidade digital no contexto português, abordamos brevemente as diferenças na forma de versar sobre este tema entre a União Europeia (UE), os Estados Unidos (EUA), a China e outros blocos emergentes, como a Ásia-Pacífico e a América Latina, por refletirem contextos culturais, políticos e económicos distintos que moldam políticas de proteção de dados e de privacidade também diferentes em cada região.

É reconhecido que a União Europeia tem liderado a proteção da privacidade digital, promovendo um quadro normativo robusto que procura equilibrar a inovação tecnológica com a proteção dos direitos individuais, sublinhando a importância da privacidade como um direito humano essencial[43]. A adoção do Regulamento Geral sobre a Proteção de Dados (RGPD) em 2018, que iremos especificar mais à frente, consolidou a UE como referência mundial em matéria de proteção de dados.

Nos Estados Unidos, a privacidade digital tem sido tratada de uma forma menos centralizada e menos regulada do que na UE[44]. De um modo geral, a abordagem americana tende a privilegiar a inovação e o crescimento económico, priorizando a flexibilidade e a autonomia das empresas no uso de dados[45], a autorregulação das empresas assenta em leis que variam conforme o setor. Mesmo depois do escândalo *Cambridge Analytica* e da interferência estrangeira nas eleições presidenciais de 2016, a ação política e governamental dos Estados Unidos ainda necessita de articular melhor a forma como as plataformas digitais operam em conformidade com os direitos humanos e os princípios democráticos fundamentais[46]. Os investigadores Achyuth, Putman e Fisher concluíram que a privacidade dos dados nos Estados Unidos está na sua fase inicial, necessitando de uma revisão premente, apontando a Lei de Privacidade do Consumidor da Califórnia (*California Consumer Privacy Act*) como uma das legislações mais próxima das normas europeias, embora numa escala muito menor[47].

Por seu lado, a China tem vindo a priorizar uma harmonia social e coletiva vinculada a objetivos económicos do Estado, propondo um controverso sistema de crédito social que expande o controlo estatal sobre os dados e os comportamentos individuais. Este sistema tem vindo a ser implementado em modo experimental desde 2014 e revela uma grande espectativa: que seja um dos projetos de reforma social e económica mais substanciais da História nacional, capaz de impulsionar o desenvolvimento contínuo da China na era da informação[48]. Se o sistema de crédito social da China é uma resposta pró-ativa que combina arquiteturas de vigilância e tecnologias de Inteligência Artificial para fins políticos (controlo do Estado e o planeamento económico), o RGPD da Europa, pelo contrário, é uma resposta reativa, que afirma a privacidade individual e impõe limites à utilização de dados pessoais pelas empresas[49]. A China, que inicialmente teve uma abordagem próxima dos EUA, convergiu

43 Polonca Kovac e Grega Rudolf. 2022. «Social Aspects of Democratic Safeguards in Privacy Rights: A Qualitative Study of the European Union and China».

44 Ruben de Bruin. 2022. «A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence».

45 Ibid.

46 (Guilherme E. Trevisan, Odisséia Aparecida P. Fontana e Silvia Ozelame R. Moschetta. 2022. «Resolução de conflitos interinstitucionais nas relações entre usuários e plataformas digitais».

47 Achyuth Rachur, Jonathan Putman e Clifford Fisher. 2022. «What did the digital age mean for privacy in the United States?».

48 Brett Aho e Roberta Duffield. 2020. «Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China».

49 Ibid.

recentemente com as regras da UE em alguns aspetos que visam proteger os direitos dos utilizadores, nomeadamente através da sua Lei da Cibersegurança e da Especificação da Segurança das Informações Pessoais. Estas «caraterísticas chinesas, como o aumento paradoxal - mas paralelo - da vigilância estatal e da privacidade dos consumidores e o princípio da ciber-soberania com impacto na proteção dos dados pessoais, compõem agora a abordagem da China»[50].

Além destes três grandes blocos, outras regiões emergentes têm vindo a ajustar as suas legislações em relação à privacidade digital, equilibrando estas preocupações com a necessidade de inovação tecnológica. Na América Latina, por exemplo, o impacto do RGPD tem sido notório, e desde a sua entrada em vigor em 2018, muitos países têm alterado as suas leis emulando os padrões europeus, a este fenómeno designa-se «Efeito Bruxelas», que demonstra a capacidade de a União Europeia influenciar regulamentações globais[51]. Contudo, o pesquisador Renan Canaan defende que, no caso do Brasil, a replicação acrítica do RGPD na Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD) favoreceu as empresas europeias em detrimento das firmas brasileiras: apesar de ter constituído uma oportunidade para combater monopólios de dados e fomentar a inovação, trouxe incertezas jurídicas que podem travar o desenvolvimento tecnológico dos empresários brasileiros[52]. Pelo que, se deve avaliar se a reprodução de regimes de proteção de dados, ou outros, é adequada ou «se não é apenas mais uma faceta do projeto de dominação expansionista dos países europeus sobre o Sul Global»[53].

No contexto da região da Ásia-Pacífico observa-se uma diversidade de abordagens à legislação sobre proteção de dados. Também na sequência da introdução do RGPD em 2018, a Austrália, a Indonésia, a Índia, a Malásia, o Japão, Singapura e a Tailândia estão atualmente numa nova fase de investigação sobre a regulamentação adicional necessária neste domínio[54]. Enquanto alguns países estão a adotar princípios semelhantes aos do RGPD, outros mantêm influências mais próximas dos modelos dos EUA, favorecendo a autorregulação[55]. Tal como na UE, a Austrália, tem leis de proteção de dados e de privacidade em vigor desde a década de 1980, mas noutros países da Ásia Central, do Sudeste Asiático e da Ásia Oriental, estas leis são um fenómeno recente, por exemplo: em Singapura, Malásia e Japão estabeleceram leis de proteção de dados que, embora diferentes entre si, não têm mais de uma década[56]. O Japão, tem implementado uma legislação de proteção de dados semelhante aos princípios vigentes no RGPD, o que facilitou um acordo de certificação de adequação mútua com a UE, em 2019, permitindo concretizar a livre circulação transfronteiriça de dados pessoais entre estas duas economias[57]. Embora Índia e Indonésia estejam a desenvolver leis específicas de proteção de dados, estão juntamente com a Tailândia menos avançados no domínio da legislação de proteção de dados, podendo estabelecer as

50 Emmanuel Pernot-Leplay. 2020. «China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?».

51 Arturo J. Carrillo e Matías Jackson. 2022. «Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America».

52 Renan Gadoni Canaan. 2022. «Estímulo à inovação através de regulamentações para a proteção de dados pessoais: o impacto da replicação da GDPR na LGPD».

53 Ibid.

54 Robert Walters, Leon Trakman e Bruno Zeller. 2019. «Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approache».

55 Graham Greenleaf. 2019. «Global Data Privacy Laws 2019: 132 National Laws & Many Bills».

56 Walters, Trakman e Zeller. 2019.

57 Masao Horibe. 2020. «The Realization of Mutual Adequacy Recognition Between Japan and the EU and Issues Raised in the Process».

suas referências internas ou seguindo a UE e outros países como a Austrália e Singapura, para obterem orientação. Já Singapura implementou um modelo favorável às empresas[58].

No conjunto todos estes países estão a adaptar-se a uma realidade global onde a proteção da privacidade se torna central para o comércio internacional e para as relações digitais entre Estados. A abordagem europeia, dentro da qual Portugal se insere, é, portanto, caracterizada por uma regulação centrada na salvaguarda das liberdades individuais e no controlo do uso de dados por parte de empresas e governos.

2.1.3.2 POLÍTICAS DE PRIVACIDADE

No contexto *online*, uma política de privacidade é uma declaração formal que descreve a posição de uma entidade, seja um serviço, empresa ou organização, no que diz respeito à forma como recolhem, utilizam, armazenam e partilham dados e informações pessoalmente identificáveis[59]. Com o propósito de informar os visitantes, a publicação de políticas de privacidade em sites coloca os utilizadores a par dos seus direitos à privacidade e das formas como podem exercê-los. As políticas de privacidade são, pelo menos em teoria, um mecanismo dedicado a divulgar práticas de processamento de dados[60] que reflete as regulamentações de privacidade, à luz das preocupações de proteção do consumidor.

As obrigações legais relacionadas com a necessidade de fornecer políticas de privacidade, que abrangem as entidades que processam dados de utilizadores podem variar entre regiões. Nos países com leis de proteção de dados mais robustas, como os da UE, essa obrigação é clara. Em 2016 entrou em vigor em toda a UE o Regulamento Geral de Proteção de Dados, sendo que as organizações foram obrigadas a atuar em conformidade a partir de 25 de maio de 2018. Este regulamento introduziu uma legislação significativa, uma vez que estabeleceu um quadro unificado que concede aos consumidores um maior controlo sobre os seus dados pessoais. Adicionalmente, destaca-se o aumento da responsabilidade das organizações e a imposição de sanções substanciais em caso de não conformidade, conforme estabelecido no artigo 83º do RGPD, que prevê a aplicação de multas até 10 milhões de euros ou 2% das receitas anuais a nível mundial do exercício financeiro anterior[61].

Além disso, o RGPD alargou o âmbito geográfico, passando a incluir organizações com presença na UE, bem como aquelas localizadas fora dela, desde que envolvidas no tratamento de dados pessoais de cidadãos europeus. Com este alcance extraterritorial, que tenta contornar qualquer tentativa de evasão regulatória, o RGPD introduziu uma série de características regulamentares relevantes, nomeadamente o consentimento válido, específico e informado, dependente de ação afirmativa do utilizador.

Outra mudança significativa trazida pelo RGPD é o estabelecimento do princípio da responsabilização, que transfere o ónus da prova para as organizações que recolhem e utilizam dados, exigindo especificamente que sejam capazes de demonstrar o consentimento e a conformidade com o RGPD[62]. Este fator de concordância legal veio moldar bastante a forma como as organizações passaram a definir os seus comunicados acerca privacidade, isto é, as suas políticas de privacidade.

O RGPD veio ainda estipular a obrigação para as organizações informarem os indivíduos acerca de como processam os dados pessoais, em formato conciso, transparente e de fácil acesso. Isto inclui quer os casos em que os dados são recolhidos diretamente do titular dos dados, quer de terceiros. Foi esta mudança, aliás, que despertou a nossa atenção para a problemática da privacidade, na medida

58 Walters, Trakman e Zeller. 2019.

59 Abraham Mhaidli et al. 2023. «Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities».

60 Benjamin Fabian, Tatiana Ermakova e Tino Lentz. 2017. «Large-scale readability analysis of privacy policies».

61 Grace Fox, Theo Lynn e Pierangelo Rosati. 2022. «Enhancing consumer perceptions of privacy and trust: a GDPR label perspective».

62 Ibid.

em que, enquanto utilizadores regulares de serviços *online* partilhamos da perceção geral de que estes procedimentos são rápidos, mas não necessariamente evidentes para o cidadão. Como a questão de partida ainda se encontrava neste ponto pouco apurada, preferimos não a estipular imediatamente. Em associação com esta etapa, investigámos um pouco mais sobre a base de entendimento prevista legalmente para este assunto.

2.1.3.3 PRECURSORES DA PROTEÇÃO DA PRIVACIDADE

O RGPD, a par de outras leis e regulamentos, menciona a importância da utilização dos princípios de «*privacy by design*», que consiste numa atitude substancialmente proativa na tutela da privacidade. A origem do conceito *privacy by design* remonta a uma reflexão acerca da privacidade oriunda da tecnologia, por volta do final da década de 1990, de acordo com a qual a conformidade para a proteção de privacidade tendia a identificar-se somente após as violações de privacidade terem ocorrido[63]. Nesse sentido, a então Comissária de Privacidade de Ontário, Ann Cavoukian, defendeu a necessidade de integrar a defesa da privacidade nas aplicações digitais desde o início, isto é, desde o momento em que é desenhada e concebida determinada tecnologia e não apenas como preocupação posterior.

Na altura em que foi proposta publicamente, em 2009, esta abordagem foi bem recebida: por ocasião do encontro intitulado «Privacy by Design: The Definitive Workshop» co-organizado pelo escritório de Cavoukian – Comissária para a Informação e Privacidade de Ontário – e pela Autoridade de Direito, Informação e Tecnologia de Israel, reunindo notáveis profissionais em privacidade, líderes empresariais, especialistas em tecnologias de informação e investigadores académicos, para debater de que forma as ameaças à privacidade vindouras poderiam ser melhor resolvidas, a necessidade de uma nova forma de pensar a privacidade já se fazia sentir de modo mais evidente, face à explosão do volume de informações pessoais recolhidas, à medida que a tecnologia da informação se tornou cada vez mais interligada. Este foi um momento importante que proporcionou a aceitação e a cunhagem deste conceito fundador, traduzido como «privacidade desde a conceção» e é sobre esta perspetiva que se desenrola a principal orientação que demos à investigação neste trabalho.

Privacidade desde a conceção

Embora inicialmente a privacidade desde a conceção fosse referida enquanto conceito técnico, viria a evoluir para um modelo conceptual, orientador na «construção de um programa completo de privacidade»[64], incluído nos processos de negócios. A premissa da privacidade desde a conceção tem as suas raízes mais remotas nas *Fair Information Practices* (FIP), um «código de práticas justas de informação» apresentado no início da década de 1970. Este conjunto de diretrizes éticas para a recolha, utilização, armazenamento e divulgação de informações pessoais, visava proteger a privacidade dos dados pessoais em sistemas de manutenção de registos, e foi apresentado num relatório do Comité consultivo do Governo dos EUA (especificamente o Departamento de saúde, educação e bem-estar) para resolver a falta de proteção legal. Segundo a legislação da altura, a privacidade de uma pessoa estaria mal protegida contra práticas arbitrárias ou abusivas de manutenção de registos[65]. Conforme consta no documento oficial, os cinco princípios básicos, com efeito jurídico, em que se baseava a proposta, orientam para o seguinte (tradução nossa):

63 Cavoukian, Taylor e Abrams. 2010.

64 Ibid.

65 Robert Gellman. 2022. «Fair Information Practices: A Basic History - Version 2.22».

- Não deve haver sistemas de manutenção de registos de dados pessoais cuja existência seja secreta.
- Deve haver sempre uma maneira de qualquer indivíduo descobrir quais as informações sobre si que constam num registo e como são usadas.
- Deve haver uma maneira de um indivíduo impedir que informações sobre ele, obtidas para um propósito, sejam usadas ou disponibilizadas para outros fins sem o seu consentimento.
- Deve haver uma maneira de um indivíduo corrigir ou alterar um registo de informações identificáveis sobre ele.
- Qualquer organização que crie, mantenha, utilize ou divulgue registos de dados pessoais identificáveis deve garantir a fiabilidade dos dados para a utilização pretendida e deve tomar precauções para evitar a utilização indevida dos dados.

As FIP representaram um desenvolvimento importante na evolução da proteção da privacidade de dados, tendo sido o elemento precursor de práticas responsáveis de gestão da informação[66]. Uma grande parte das leis de privacidade por todo o mundo baseia-se nas práticas elencadas neste código. A co-autora do termo *privacy by design* defendia que a privacidade desde a conceção seria alcançada através deste conjunto de diretrizes éticas, aplicadas em tecnologia da informação, práticas comerciais, *design* físico e infraestruturas. Mobilizando as organizações para adotarem os princípios fundamentais em que se baseiam as FIP universais, seria possível atualizar e adaptar a privacidade às necessidades e requisitos modernos do gerenciamento de informações[67]. Convém, contudo, mencionar que muitas organizações encararam a promoção da privacidade através das FIP e leis associadas como encargos regulatórios que inibiam a inovação[68]. Além disso, «os primeiros redatores e adotantes de FIP não poderiam ter imaginado como o salto revolucionário em sensores, largura de banda, (capacidade de) armazenamento e poder de processamento convergiriam no nosso atual mundo hiperconectado em rede 2.0, e sua disponibilidade ubíqua de dados»[69]. Em rigor, o nosso mundo atual já não corresponde ao da era da *Internet* 2.0 mas sim da *Internet* 4.0, que é marcada pela integração de tecnologias avançadas como a Inteligência Artificial, a *Internet* das Coisas, *big data*, a automação, entre outras.

Em resposta aos desafios apresentados por este rápido crescimento, surgiram as *Privacy-Enhancing Technologies* (PET), ou «tecnologias que aumentam a privacidade», um conjunto de soluções e abordagens tecnológicas apontando à melhoria da proteção da privacidade em ambientes digitais. Estes mecanismos tecnológicos relativamente discretos, como pseudónimos digitais baseados em protocolos criptográficos, foram criados intencionalmente para reforçar interesses relacionados com a privacidade. As PET constituem uma componente importante da privacidade desde a conceção e tendem também a integrar uma dimensão organizacional, mas não são tão amplas quanto a proposta mais holística das diretrizes de privacidade desde a conceção.

A exposição dos sete princípios orientadores que configuram o conceito de privacidade desde a conceção[70] é relevante para compreender a gama potencialmente vasta de decisões implicadas no ciclo de vida do desenvolvimento de sistemas digitais, e que ultrapassa a mera dimensão das medidas técnicas:

66 Cavoukian e Chibba. 2018.

67 Ann Cavoukian. 2009. «Privacy by design: The 7 foundational principles».

68 Cavoukian e Chibba. 2018.

69 Cavoukian, Taylor e Abrams. 2010.

70 Cavoukian. 2009. - incluíndo a definição dos princípios que se seguem.

- Princípio 1) *Proactive not Reactive; Preventative not Remedial* – «Tomar medidas proativas em vez de reativas, medidas preventivas e não corretivas». Ou seja, antecipar, identificar e prevenir possíveis riscos à proteção de dados, antes de acontecerem. O que pressupõe agir previamente,e não depois de acontecimentos invasivos.

Isto implica um compromisso claro em aplicar padrões elevados de privacidade, mesmo que possam ser mais exigentes do que a jurisdição estabelece. Envolve também o empenho de melhoria contínua. Este primeiro princípio definiu a génese principal da observação deste trabalho, no sentido de fazer questionar o quão em prática estará a ser implementado por parte dos agentes responsáveis e implicados no desenvolvimento dos sistemas de informação, o compromisso das organizações em encontrar mecanismos preventivos e não corretivos, à luz das preocupações de proteção do consumidor.

- Princípio 2) *Privacy as the Default Setting* – «Avocar a privacidade como configuração padrão», vulgarmente designado *Privacy by Default*. Pressupõe a garantia de que os dados pessoais são protegidos automaticamente em todos os sistemas de informação ou processos de negócios, sem que nenhuma ação adicional seja exigida ao indivíduo para proteger a sua privacidade. Isto exclui que o consentimento para a partilha de dados seja assumido sem intervenção do indivíduo.

Deste segundo princípio derivam as delimitações pelas quais se foi acertando a investigação, na medida em que nos interrogámos também acerca do grau necessário de intervenção do utilizador para que a proteção da privacidade se cumpra.

- Princípio 3) *Privacy Embedded into Design* – «Integrar a privacidade no *design* e na arquitetura de desenvolvimento dos produtos ou serviços, bem como nas práticas organizacionais». As medidas de privacidade não devem ser um complemento segregado ou opcional, mas sim componentes totalmente integradas dos sistemas de informação, sem que a incorporação de privacidade na fase de *design* diminua as suas funcionalidades.

Este terceiro princípio convoca uma circularidade de responsabilidade nos agentes decisórios, intervenientes no desenvolvimento do ambiente digital. Esta incumbência acrescentou um sentido de complementariedade aos objetivos deste trabalho académico, na medida em que a autora se insere na categoria dos profissionais construtores da tecnologia, enquanto *designer*.

- Princípio 4) *Full Functionality: Positive-Sum, not Zero-Sum* – «Assegurar um funcionamento pleno com base no «todos ganham» (soma positiva e não soma zero), acomodando todos os objetivos legítimos de *design* do sistema». Ou seja, tanto a privacidade como a segurança são importantes, e não é necessário abdicar ou prejudicar funcionalidades para alcançar as mesmas.

Este princípio permite conjeturar o alinhamento entre os objetivos de construtores e decisores, ao sugerir que o empenho em adotar estas medidas para encontrar soluções garante vantagem para mais pessoas.

- Princípio 5) *End-to-End Security: Full Lifecycle Protection* – «Garantir a segurança de «ponta a ponta» (de um extremo ao outro) ou seja, durante todo o período de proteção da informação». Presumindo que as organizações preveem a incorporação da privacidade em todos os processos do ciclo de vida dos dados envolvidos: desde a avaliação prévia à recolha, à supervisão quando são retirados, retidos e destruídos no final dos processos, sempre em segurança e em tempo útil.

- Princípio 6) *Visibility and Transparency: Keep it Open* – «Confiável, mas verificável, a transparência é a chave». Assegurar a todas as partes interessadas (os *stakeholders*) que quaisquer vertentes desde a comercial, a organizacional, a do processo de negócio ou das tecnologias envolvidas, são operadas de acordo com objetivos definidos de forma visível, transparente, aberta e documentada, sujeitos a verificação independente. Os seus componentes e operações permanecem visíveis e transparentes, tanto para utilizadores como fornecedores.

- Princípio 7) *Respect for User Privacy, Keep it User-Centric* – Respeitar a privacidade do utilizador mantendo a atenção centrada no utilizador. O que significa arquitetos e operadores manterem os interesses dos indivíduos em primeiro lugar, proporcionando-lhes medidas com fortes padrões de privacidade, avisos detalhados de informações de privacidade, opções fáceis de usar bem como notificação clara de alterações, de forma a capacitar os titulares dos dados para desempenharem um papel ativo na gestão dos seus próprios dados.

Este último princípio não só reforçou o ponto de vista envolvido no segundo princípio (privacidade por defeito ou padrão), como permitiu lançar outra questão pertinente, a respeito de interligações equacionáveis entre o tema da privacidade e outras áreas que se desenvolvam centradas no utilizador. As leituras que realizámos nesta fase permitiram-nos então encontrar o postulado de uma problemática que se articulou melhor enquanto pergunta de partida: 'As políticas de privacidade e outros mecanismos em vigor demonstram conformidade com uma abordagem centrada no utilizador para a proteção da privacidade?' (Q2A). Esta pergunta a propósito da privacidade digital está ligada à abordagem *privacy by design*, e centra a atenção no utilizador que se relaciona com o conceito *user-centric*[71]. Daqui emergiram duas questões derivadas que orientaram a investigação para aspetos mais específicos: 'De que maneiras podemos observar e avaliar a conformidade das políticas de privacidade com uma abordagem centrada no utilizador?' (Q2B); e 'Como podemos verificar a conformidade com a proteção da privacidade centrada no utilizador, na realidade portuguesa?' (Q2C).

Com igual interesse, seria perceber se a conformidade para a proteção da privacidade digital está dependente da intervenção do utilizador, ou não e, nesse caso, colocar a hipótese de que os agentes responsáveis e implicados no desenvolvimento dos sistemas de informação salvaguardam *a priori* a proteção da privacidade, independentemente da intervenção do utilizador, o que se manifesta na questão: 'A conformidade para a proteção da privacidade está dependente da intervenção do utilizador ou os agentes responsáveis pelo desenvolvimento dos sistemas de informação salvaguardam *a priori* a proteção da privacidade, independentemente da intervenção do utilizador?' (Q3).

Até porque, conforme mencionado por Cavoukian e Chibba, «incorporar a privacidade e a proteção de dados requer uma abordagem sistemática e fundamentada, que não apenas dependa de normas

71 Os termos «*user-centric*» e «*user-centered*» são frequentemente empregues de forma intercambiável, sobretudo em contexto de *design* de experiência do utilizador. O comentário de um internauta expressa rapidamente esta dinâmica: «Vi o *Design* Centrado no Utilizador (DCU) espalhar-se pela indústria do *design* há 20 anos, na sequência da disseminação da *Internet* (embora seja muito mais antigo do que isso enquanto disciplina) e nunca ninguém concordou se é «centred» ou «centric». Tecnicamente falando, «Centred» implica que está centrado no utilizador, enquanto «Centric» implica pensar no utilizador; mas os processos, os objetivos e os resultados finais são idênticos, por isso não importa!» (Roux Martin, Maio 2017). Estas diferenças entre os dois termos não vão ser exploradas neste estudo, embora reconheçamos que abrir a discussão a este aspeto da conceção centrada no utilizador poderia reforçar e trazer novos contributos ao trabalho, nomeadamente pela crítica do investigador Birger. Sevaldson (2018) contra a atenção dominante dada à conceção centrada no utilizador que, entende, reforçar as divisões de poder e deveria ser complementada por uma abordagem de conceção sistémica que considere múltiplas perspetivas além da do utilizador, por exemplo as preocupações ambientais.

aceites e estruturas de processo, mas que também possa resistir a avaliações externas e auditorias»[72]. Por isso, formulada a problemática que nos dispusemos explorar, considerámos relevante a possibilidade de perscrutar a realidade portuguesa ao filtro reunido nestes princípios.

Mas, antes, prosseguimos no sentido de compreender melhor ainda a especificidade das políticas de privacidade, nomeadamente pela abordagem da privacidade desde a conceção e da atenção centrada no utilizador, bem como a relevância dos agentes envolvidos na sua redação.

2.1.3.4 PAPEL DO ENCARREGADO DA PROTEÇÃO DE DADOS NA PROMOÇÃO DE UMA CULTURA DE PRIVACIDADE NAS ORGANIZAÇÕES

Na sequência da entrada em vigor do RGPD, e de leis semelhantes em todo o mundo, tornou-se necessária a nomeação de um responsável pela proteção de dados nas organizações, o que gerou o cargo de Encarregado da Proteção de Dados (EPD)[73]. Estes agentes são os principais intervenientes da aplicação dos regulamentos e harmonização das leis de proteção de dados pré-existentes e são fundamentais para fomentar uma abordagem proativa à privacidade, uma vez que entre as suas responsabilidades principais estão englobadas: 1) a incumbência de monitorizar e avaliar as práticas de tratamento de dados pessoais da organização, 2) aconselhar a organização que os nomeia sobre as obrigações de proteção de dados e 3) sensibilizar e formar os colaboradores da organização em matéria de proteção de dados; 4) além das indubitáveis competências em assegurar a conformidade com o RGPD e outras legislações de proteção de dados, 5) bem como a atuação enquanto ponto de contato entre a organização e as autoridades de proteção de dados[74]. Salientamos que embora o EPD desempenhe um papel crucial na garantia da conformidade, a responsabilidade final pertence às organizações que tratam os dados pessoais. Essa obrigação cabe aos responsáveis pelo tratamento de dados, e a subcontratantes, e não ao responsável pela proteção de dados, pelo que o EPD não é considerado pessoalmente responsável por violações regulamentares[75].

Apesar de serem peças-chave na promoção da cultura de privacidade nas organizações, os EPDs podem deparar-se com alguns obstáculos no cumprimento das suas funções, como o risco de conflito de interesses, particularmente quando acumulam funções em cargos de gestão superiores que podem comprometer a independência necessária para o desempenho eficaz das suas responsabilidades[76]. Uma sobreposição de funções coloca em causa a autonomia do EPD e, consequentemente, a conformidade rigorosa com o RGPD. Além disso, muitas vezes os EPDs podem ser pressionados a equilibrar as necessidades empresariais com os direitos de privacidade dos titulares dos dados. As rápidas mudanças tecnológicas e a inovação nas práticas empresariais tornam este equilíbrio particularmente difícil, dado que muitas vezes os interesses comerciais podem colidir com os princípios da proteção de dados. Outro desafio significativo é a falta de conhecimento especializado e de recursos disponíveis dentro das organizações, muitas empresas enfrentam uma escassez de profissionais qualificados para assumir o cargo de EPD, o que frequentemente as obriga a recorrer a consultores externos ou a investir em formação interna. A falta de apoio financeiro e estrutural por parte da gestão superior em muitos casos limita a sua capacidade de auditar, formar e monitorizar eficazmente as práticas de tratamento de dados.

Segundo Barbara Eggl «os elementos estabelecidos no RGPD devem ser devidamente combinados e ponderados, a fim de garantir que o EPD possa desempenhar as suas funções de uma forma que

72 Cavoukian e Chibba. 2018.

73 Em inglês esta figura é conhecida como *Data Protection* Officer (DPO).

74 European Data Protection Supervisor sd «Data Protection Officer (DPO)».

75 Aurima Sidlauskas. 2021. «The Role and Significance of the Data Protection Officer in the Organization».

76 Ibid.

cumpra não só a letra, mas também a intenção da lei»[77]. A especialista aponta para que a complexidade crescente das operações de tratamento exija que os EPD: 1) compreendam mais profundamente as complexidades técnicas envolvidas, além das necessidades da empresa – por exemplo o facto de o tratamento ser efetuado «na nuvem»; 2) que equilibrem corretamente o ponto de vista da proteção de dados com o entusiasmo das organizações em querer utilizar as novas tecnologias («*always stand up for privacy*»[78] e; 3) que todas as ações da concretização enquanto EPD sejam documentadas, para constituírem um processo transparente e detetável.

Acerca da lacuna de conhecimento dentro das organizações, ou a falta de uma cultura de privacidade sólida, foi um assunto para resolver que identificámos como uma oportunidade na nossa investigação e viria converter-se num produto desta (o Produto de Investigação 2).

2.1.4 ESTUDOS SOBRE AS POLÍTICAS DE PRIVACIDADE

Podemos considerar o RGPD da UE um modelo adaptável, capaz de responder às dinâmicas trazidas pelas novas tecnologias e pelo crescimento exponencial de dados digitais. Em simultâneo, o RGPD funcionou como elemento contextualizante que veio introduzir um reforço dos direitos dos titulares dos dados, uma vez que os utilizadores passaram a ter a possibilidade de «negociar a política de privacidade de acordo com as suas preferências pessoais (escolhendo) quais e como é que os seus dados serão tratados»[79].

A importância das políticas de privacidade é destacada como ferramenta influente na promoção da confiança e fidelidade dos clientes[80]. Segundo os autores, algumas descobertas indicam que uma grande parte dos utilizadores da *Internet* têm a perceção de que os *sites* que disponibilizam uma política de privacidade estão a proteger melhor os seus utilizadores, assumindo que não partilham informações pessoais dos seus clientes com empresas terceiras. Os mesmos autores acrescentam que, como os utilizadores tendem a considerar esses *sites* mais fiáveis, facilmente permitem divulgar as suas informações pessoais para realizar as operações proporcionadas pelos *sites*. Contudo, salientam que a compreensão real da política de privacidade também é crucial para a construção da confiança do utilizador. Diversos estudos demonstraram que os consumidores *online* tendem a desenvolver mais confiança em *sites* com políticas de privacidade percebidas como facilmente compreensíveis e realmente compreendidas[81].

No entanto, a leitura das políticas de privacidade pelos utilizadores é frequentemente negligenciada, seja por completa ausência de leitura ou devido às dificuldades em compreender esses documentos, decorrentes de descrições pouco claras e do uso de terminologia técnica[82]. Chama-se «paradoxo da privacidade da informação» ou «paradoxo da privacidade» à dicotomia existente entre a

77 Barbara Eggl. 2019. «Learning to Walk a Tightrope: Challenges DPOs Face in the Day-to-Day Exercise of Their Responsibilities».

78 Ute Kallenberge e Barbara Eggl. 2019. «Being a Data Protection Officer in the Public Sector: The EU Side of Things».

79 Stefan Becher, Armin Gerl e Bianca Meier. 2020. «Don't Forget the User: From User Preferences to Personal Privacy Policies».

80 Fabian, Ermakova e Lentz. 2017.

81 Ibid.

82 Hana Habib et al. 2021. «Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts».

mentalidade dos utilizadores relativa à privacidade da informação e o seu comportamento efetivo nos ambientes digitais[83].

As políticas de privacidade têm sido objeto de interesse entre investigadores que conduziram estudos específicos nesta área, abrangendo diversas disciplinas, tais como saúde, direito, ciências informáticas, privacidade e segurança, aprendizagem automática, entretenimento digital, media e comunicação, entre outras[84]. Três abordagens principais são identificadas neste campo de estudo:

a. A análise das políticas de privacidade com o intuito de compreender as práticas de utilização de dados de diferentes entidades, investigando se o comportamento real das empresas reflete de forma precisa os princípios delineados nas suas políticas.
b. Simultaneamente, outras investigações focam-se na avaliação da usabilidade das políticas de privacidade, considerando aspetos como a legibilidade e a complexidade destes documentos. Algumas dessas investigações procuraram examinar a facilidade de utilização e de leitura, incluindo a quantificação da imprecisão e legibilidade das políticas. Estes resultados têm sido obtidos através da análise da extensão das políticas, da determinação do nível necessário de compreensão de leitura e da avaliação da capacidade de os utilizadores demonstrarem compreensão. Fabian, Ermakova, e Lentz destacam a falta de consistência no uso de medidas de legibilidade em relação às políticas de privacidade[85].
c. Outros estudos exploraram a interação entre as políticas de privacidade e a legislação, investigando a conformidade entre serviços selecionados e a legislação relevante, como o RGPD e o impacto das legislações específicas na proteção da privacidade. Adicionalmente, foram desenvolvidas ferramentas para resumir e analisar políticas de privacidade, incluindo algumas destinadas a fornecer resumos informativos para consumidores e reguladores e, para este objetivo têm contribuído significativamente, as técnicas de processamento de linguagem natural.

As metodologias usadas nessas pesquisas ainda se configuram como «processos pouco consistentes»[86] que dificultam o apuramento de boas práticas para a análise de políticas de privacidade. A investigação deste entrave colocou a descoberto algumas barreiras enfrentadas durante a análise de políticas de privacidade: 1) incluindo o carácter abstrato e a dificuldade de interpretação dessas políticas pelos utilizadores, bem como a possibilidade de especialistas discordarem na sua interpretação; 2) a complexidade na partilha e manutenção de ferramentas de investigação, 3) a ausência de uma esfera de publicação específica para políticas de privacidade, 4) a dificuldade em promover colaboração interdisciplinar e 5) a falta de apoio para estudar políticas de privacidade que não estejam em inglês.

A abundância de estudos que procuram automatizar ou agilizar a análise das políticas de privacidade sugere que esta tarefa é demorada, fastidiosa e complexa de automatizar e expandir. Realmente, as políticas de privacidade que se destinam a proteger o titular dos dados resultam frequentemente em documentos longos e fastidiosamente jurídicos, e mesmo o sistema de autorização interativo que se encontra nos telemóveis modernos não permite compreender suficientemente os riscos para a privacidade inerentes à utilização de uma aplicação[87]. Adicionalmente, considerando o tempo estimado

83 Spyros Kokolakis. 2017. «Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon».
84 Mhaidli et al. 2023.
85 Fabian, Ermakova e Lentz. 2017.
86 Mhaidli et al. 2023.
87 Barth, Ionita e Hartel. 2022.

necessário para ler as políticas de privacidade dos *sites* visitados, seria irrealista esperar que os utilizadores as lessem regularmente[88].

A privacidade representa uma dificuldade tanto para as organizações como para os consumidores, que se complica com os avanços contínuos da tecnologia e as sucessivas introduções de regulamentação[89]. A composição atual da maioria das políticas de privacidade não comunica eficazmente as práticas de privacidade aos consumidores e também não está sempre em conformidade com o RGPD, sendo necessário ajustar as políticas de privacidade para informar melhor os consumidores sobre a forma como as suas informações são utilizadas[90].

2.1.4.1 FORMATOS DE POLÍTICAS DE PRIVACIDADE

Os investigadores Victor Morel e Raúl Pardo (2020) identificaram três categorias principais das políticas de privacidade, cada uma surgindo da necessidade de atender às necessidades de diferentes públicos: 1) existem as políticas de privacidade que se encontram detalhadas em linguagem natural, componente essencial para os advogados verificarem a conformidade dos textos com os regulamentos de proteção da privacidade que, no entanto, acabam por ser menos acessíveis para o público em geral uma vez que os utilizadores leigos frequentemente não têm o conhecimento técnico para as entender; 2) existem também as políticas de privacidade legíveis por máquinas, escritas num formato que inclui todos os detalhes técnicos necessários para uma aplicação automática. Embora sejam ideais para sistemas automatizados, estas políticas são difíceis de compreender por humanos, sejam utilizadores leigos ou advogados; 3) e há ainda as políticas de privacidade expressas de forma gráfica, que representam uma tentativa de tornar essas informações mais acessíveis ao público geral sendo, no entanto, uma modalidade de apresentação não satisfatória para advogados, que precisam de detalhes específicos, ou para a aplicação por máquinas que requerem um formato legível por sistemas automatizados[91]. Os autores do estudo comparativo entre estas facetas das políticas de privacidade concluíram que as soluções de dimensão única são inadequadas e sugerem que uma abordagem integrada seja adotada.

Embora não existam limites para o modo de apresentar os conteúdos de uma política de privacidade, a maioria dos *sites* aplica um formato textual. Os defensores da privacidade, juristas e investigadores académicos têm defendido mecanismos normalizados para fornecer avisos e opções de privacidade[92]. Isto é, formas de ajudar os consumidores a encontrar e compreender as informações e escolhas relacionadas com a privacidade. Por outro lado, a exigência de que os avisos de privacidade e as escolhas disponíveis sejam claras e acessíveis também tem surgido plasmada em regulamentação recente. O que justifica o surgimento de propostas de soluções alternativas da divulgação das opções apresentadas nas políticas de privacidade, tais como painéis de controlo, certificações, classificações, rótulos, *banners*, *pop-ups* ou ícones de privacidade, concebidos com o intuito de facilitar o entendimento e a tomada de decisões por parte dos utilizadores.

Os investigadores no campo da interseção entre a área de design e privacidade, Susanne Barth, Dan Ionita e Pieter Hartel realizaram um estudo que apura as dimensões de privacidade abrangidas por um conjunto de representações visuais de privacidade. Elencam-se deste modo as tipologias de visualizações de privacidade[93] que são estabelecidas para comunicar aspetos relacionados com o tra-

88 McDonald e Cranor (2008) citados por Shomir Wilson et al. 2018. «Analyzing Privacy Policies at Scale: From Crowdsourcing to Automated Annotations».

89 Fox, Lynn e Rosati. 2022.

90 Ibid.

91 Victor Morel e Raúl Pardo. 2020. «SoK: Three Facets of Privacy Policies».

92 Habib et al. 2021).

93 Barth, Ionita e Hartel. 2022.

tamento de dados pessoais aos utilizadores de serviços *online*:

- Os painéis de privacidade permitem aos consumidores inspecionar a natureza dos dados que as empresas recolheram sobre eles e ajustar as suas definições de privacidade.
- As certificações e selos de privacidade destinam-se a indicar que as empresas cumprem os requisitos legais ou as normas industriais.
- As classificações e pontuações de privacidade indicam até que ponto os *sites* protegem a privacidade dos seus utilizadores através de classificações numéricas.
- Os rótulos de privacidade, semelhantes aos rótulos nutricionais dos alimentos, ajudam os utilizadores a conhecer e comparar rapidamente os atributos de produtos ou serviços relacionados com a privacidade.
- As opções de privacidade apresentadas em *banners* e *pop-ups* de consentimento, principalmente relacionadas com a gestão de *cookies*, muitas vezes oferecem aos utilizadores opções limitadas e incitam-nos a aceitar o rastreio.
- Os ícones de privacidade, indicadores sucintos de conceitos complexos de privacidade, podem ser marcadores de informação úteis, uma vez que são fáceis de reconhecer e permitem comunicar visualmente a informação de forma concisa, contornando simultaneamente as barreiras linguísticas e culturais. Quando colocados ao lado de longas declarações de privacidade, os ícones podem melhorar a legibilidade ajudando os utilizadores a navegar pelo texto; *designers* e decisores de políticas de privacidade devem fazer acompanhar os ícones com descrições de texto e utilizar símbolos visuais padronizados para que ajudem os consumidores a localizar os mecanismos de escolha de privacidade e ainda, incorporar testes de utilizadores nos processos de elaboração de políticas[94].

2.1.4.2 FUNDAMENTOS DA PRIVACIDADE

Em geral, parece existir uma falta de acordo em termos de caracterização da privacidade *online*, isto é, das suas componentes principais, conforme apontado por Barth, Ionita e Hartel[95]. Para ajudar a compreender a privacidade *online*, o estudo «Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines» identifica uma «Lista Unificada de Atributos de Privacidade» (doravante LUAP) e ordena-os com base na importância de cada atributo. Resultado da comparação sistemática entre propostas de conceptualização da privacidade destinadas aos utilizadores (visualizações de privacidade) e as diretrizes *privacy by design* que afetam os programadores; teve também em consideração diversas fontes académicas, da indústria e do governo, bem como, incluiu as perspetivas dos utilizadores e dos especialistas em privacidade, o que consubstanciou a pertinência e robustez deste estudo. Estas categorias de privacidade tão consistentemente identificadas apresentaram-se para nós como um contributo crucial na presente dissertação, uma vez que forneceram a base dos indicadores para a análise quantitativa, abordada no capítulo seguinte.

O estudo menciona que tanto os utilizadores quanto os peritos em privacidade concordam que a Recolha, Partilha e Venda são os atributos de privacidade mais importantes. Os especialistas atribuem uma importância ligeiramente superior, até cerca de 10%, à maioria dos atributos, face ao que os utilizadores consideram. Mas em relação aos atributos Anonimização e Direito a ser esquecido, os peritos tendem a conferir uma importância até 10% inferior do que os utilizadores atribuem.

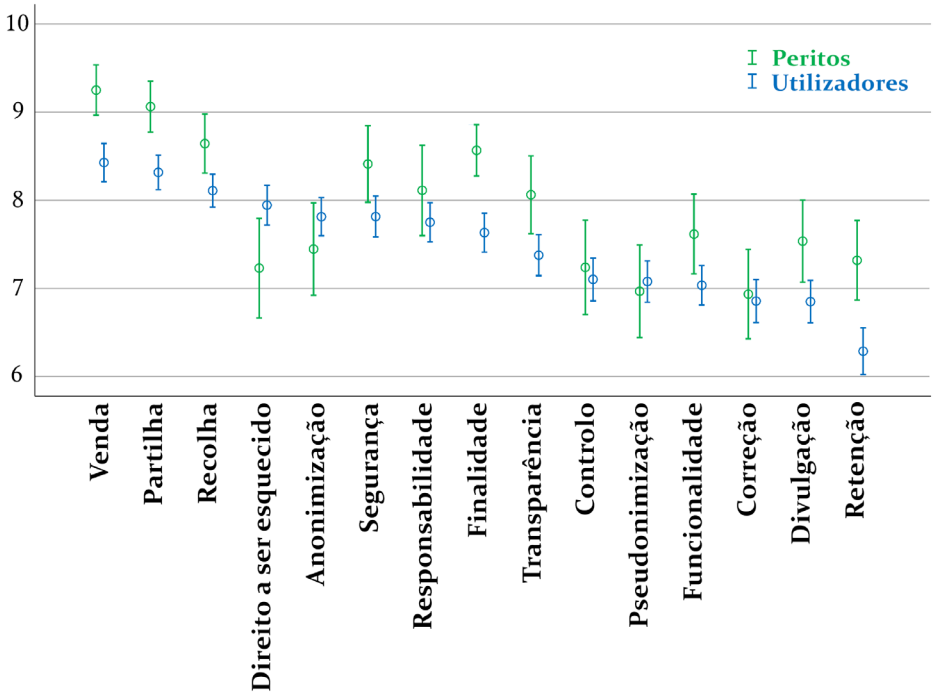
O gráfico seguinte, extraído da publicação referida, mostra a importância média (de 0 a 10) e o intervalo de confiança dos atributos de privacidade, para os utilizadores e para os especialistas. Através desta visualização é possível obter uma noção dos atributos recolhidos e da sua significância. Contudo,

94 Habib et al. 2021.

95 Barth, Ionita e Hartel. 2022.

na amostra do estudo, 59% dos peritos em privacidade e 49% dos utilizadores indicaram que classificariam os atributos de forma diferente consoante diferentes tipos de serviços, o que está em sintonia com a ideia de que as preocupações com a privacidade dependem do contexto e do tipo de serviço.

Figura 2.1 - Distribuição da importância média e do intervalo de confiança dos atributos de privacidade, para especialistas em privacidade e utilizadores



Fonte: Adaptação e tradução nossa a partir da Fig. 14 apresentada em Susanne Barth, Dan Ionita e Pieter Hartel. 2022. «Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines».

O significado concreto de cada atributo será compreendido ao longo do capítulo seguinte. Interessa-nos agora salientar que o conjunto das circunstâncias referidas até aqui continuou a despertar-nos a curiosidade em conhecer as equivalências dirigidas ao panorama português.

2.2 CONJUNTURA DIGITAL DA ADMINISTRAÇÃO PÚBLICA

Para o estudo das práticas relativas à privacidade online na realidade portuguesa, considerámos que a Administração Pública pudesse ser o ambiente que melhor assumisse e refletisse uma vontade de privilegiar a privacidade da informação centrada no utilizador, uma vez que é assumido que o desenho dos serviços públicos digitais tem como principal foco o cidadão.

António Tavares fornece uma visão da Administração Pública portuguesa, proveniente do seu contacto com esta, no âmbito da sua experiência multifacetada enquanto investigador, formador e cidadão: «(a Administração Pública) trata-se do poder de gestão do Estado, que se manifesta no poder de regulamentar, tributar e fiscalizar, através dos seus órgãos e outras instituições, tendo em vista a prossecução do serviço público»[96].

A abrangência da Administração Pública é ampla, não se cingindo à interação dos balcões de atendimento e aos processos administrativos que a suportam, pois engloba uma série de outras profissões com que os cidadãos contactam frequentemente. Razão adicional pela qual, o impacto é amplamente sentido na comunidade, sobretudo quando decorre mal. De resto, não é uma originalidade portuguesa que a função pública e a Administração Pública sejam temas constantes do debate público. Pois por um lado, o universo eleitoral que abrange a Administração Pública é relevante, e por isso há interesse por parte do governo em não interromper a satisfação das pessoas, por outro, por ter repercussões notórias na coletividade, manifesta-se em serviços muito visíveis, de onde é natural que a insatisfação sobressaia[97].

Para enquadrar o tema da Administração Pública e a justificação da observação do seu contributo para esta investigação, remetemos lateralmente à leitura do apêndice 'Breve descrição da Administração Pública segundo ensaio de António Tavares'. No texto extraímos do ensaio de António Tavares a trajetória sucinta da Administração Pública portuguesa até 2019, salientando o que mais importa referir para o nosso assunto e abstendo-nos de debater as problemáticas envolvidas, uma vez que não é essa a incidência aqui pretendida.

Em resumo, o que mais importa referir sobre o conjunto das medidas descritas no apêndice é que caracterizam um pulsar reformista da Administração Pública portuguesa, e que deve ser elogiado, mas que também denunciam a brecha pela qual as melhores intenções escapam. De certo modo, a investigação que procurámos desenvolver aspira a contribuir para o colmatar da lacuna na avaliação das medidas implementadas na Administração Pública portuguesa, visto que a falha na avaliação dos resultados se revela uma tendência seriamente identificada por António Tavares.

2.2.1 MOSAICO, MODELO COMUM DE PORTUGAL

Convém acrescentar que no que diz respeito a *sites* sob responsabilidade da Administração Pública, a inclinação para desprezar a avaliação dos resultados pode ser atualmente contornada. O Mosaico é uma plataforma pública, criada pela Agência para a Modernização Administrativa (AMA) que «pretende ajudar todas as equipas da Administração Pública, sejam colaboradores internos ou externos, a desenhar e desenvolver serviços públicos digitais. Este «modelo comum de Portugal» é proveniente de uma abordagem baseada nos direitos humanos reconhecidos internacionalmente, e resulta numa metodologia de trabalho com nove princípios básicos que devem ser considerados na

96 António Tavares. 2019. *Administração Pública Portuguesa.*

97 45 Graus. 2024. «#158 António Tavares - Além da Política: devíamos pensar mais a Administração Pública». 45grauspodcast.com.

criação e evolução de qualquer serviço público digital[98]. Conheçamos genericamente este grupo de orientações[99] que é também «o ponto de partida essencial para a exploração de um conjunto muito alargado de referências, ferramentas e conceitos técnicos»:

1. Promover a participação dos cidadãos em todas as fases do processo, em particular dos grupos excluídos ou mais desfavorecidos.
2. Desenhar, em primeiro lugar, para as comunidades em situações vulneráveis.
3. Analisar de forma sistemática as consequências esperadas e imprevistas da disponibilização do serviço.
4. Valorizar tanto o processo quanto o resultado.
5. Garantir a privacidade e a proteção de dados pessoais dos cidadãos.
6. Considerar os casos de uso indevido como um problema sério a resolver.
7. Promover a monitorização e avaliação contínua dos serviços.
8. Desenvolver as capacidades dos titulares de direitos e dos detentores de deveres.
9. Garantir a transparência sobre obrigações, responsabilidades e direitos das pessoas relativos aos serviços.

Destacam-se como elementos-chave da utilização sistemática destes princípios: a participação e a responsabilidade, a não discriminação e a ênfase na dignidade humana, a transparência e a prestação de contas. Enunciando através da garantia de serviços inclusivos, acessíveis e seguros, uma Administração Pública «ainda mais aberta, transparente, eficiente e promotora das sociedades em que todas e todos queremos viver»[100], confirmando assim, que o questionamento que fomos levantando conflui nas intenções descritas para o sector da modernização administrativa.

Simultaneamente, estes termos reforçaram e situaram-nos na corrente especializada da conceção centrada no utilizador, que assenta numa metodologia em que os *designers* colocam o utilizador no centro do processo de conceção, com o objetivo de criar produtos digitais que respondam às necessidades, preferências e expectativas dos utilizadores.

Entre as ferramentas e orientações estratégicas reunidas no Mosaico para o efeito, encontra-se o «modelo de conformidade» que permite às equipas aferir o nível de cumprimento das boas práticas e recomendações do Mosaico, relativa aos serviços públicos digitais que têm sobre a sua responsabilidade. E também, destacam, «permite às entidades avaliar a maturidade dos seus serviços públicos digitais e identificar áreas de melhoria, tendo sempre em vista (o aperfeiçoamento) do serviço prestado ao utilizador (seja cidadão, empresa ou outras entidades da sociedade civil) e, consequentemente, a sua experiência de interação com a Administração Pública»[101].

O Modelo de Conformidade do Mosaico permite obter um diagnóstico de avaliação do serviço ou entidade, cruzando áreas técnicas da acessibilidade, da arquitetura empresarial, da computação em *cloud,* dos dados abertos, da Inteligência Artificial, da interoperabilidade, das metodologias ágeis (*Agile*), da segurança de informação, do *service design*, dos testes de *software* e da usabilidade. Estas áreas estão relacionadas entre si por regras a que obedecem, por etapas implicadas e por perfis dos profissionais envolvidos nos seus processos. As regras constituem uma versão dos princípios que adaptam as orientações estratégicas mencionadas anteriormente, à realidade concreta, tais como: 1) compreender

98 LABX - Centro para a Inovação no setor Público. 2021. «Guia Metodológico para Serviços Públicos baseados em Direitos Humanos».

99 Para um conhecimento detalhado da definição, relevância e obrigatoriedade legal de cada princípio reporta-se o leitor à navegação da página https://mosaico.gov.pt/principios.

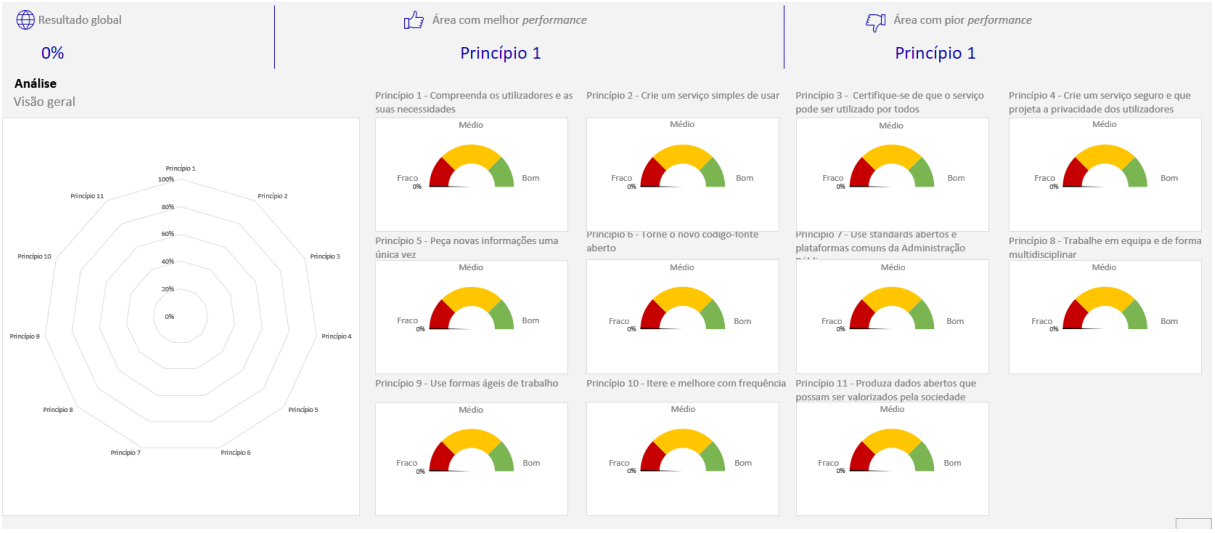
100 Mensagem introdutória da Secretária de Estado da Inovação e da Modernização Administrativa (entre 2019-10-26 até 2022-03-30), Fátima Fonseca, em «Guia Metodológico para Serviços Públicos baseados em Direitos Humanos». 2021.

101 AMA-Agência para a Modernização Administrativa. 2024. «Modelo de Conformidade do Mosaico». www.mosaico.gov.pt/ferramentas/modelo-de-conformidade.

os utilizadores e as suas necessidades, 2) criar serviços simples de usar, 3) assegurar que os serviços podem ser utilizados por todos, 4) criar serviços seguros e que protejam a privacidade dos utilizadores, 5) pedir novas informações uma única vez, 6) tornar o novo código-fonte aberto, 7) usar *standards* abertos e plataformas comuns da Administração Pública, 8) trabalhar em equipa e de forma multidisciplinar, 9) usar formas «ágeis» de trabalho, repetir e melhorar com frequência, e 10) disponibilizar dados abertos para que possam trazer valor para a sociedade[102].

O Modelo de Conformidade em si, é um questionário de 75 perguntas desdobradas a partir dos princípios expostos no Mosaico. As opções de respostas disponíveis são: Não aplicável / Não / Parcialmente / Sim; sendo possível comentários a cada campo respondido. No final, consoante a grelha de respostas é possível visualizar os resultados num gráfico de radar cujas multivariáveis correspondem a cada princípio. E também é possível visualizar um indicador de intensidade quanto ao nível de conformidade (de «fraco» a «bom»), para cada princípio.

Figura 2.2 - Painel de controlo do Modelo de Conformidade do Mosaico [103]



Fonte: Ferramenta «Modelo de Conformidade» de apoio às equipas da Administração Pública na criação e evolução dos serviços públicos digitais, consoante os princípios orientadores do Mosaico (versão 1.0, julho 2022).

Na plataforma Mosaico, o tema da privacidade surge incluído na área da segurança de informação, sendo até referida «a lógica do *privacy by design*» como um dos fundamentos da segurança. No entanto, os guias práticos e as ferramentas de avaliação desta área técnica parecem enquadrar-se mais na ótica da cibersegurança do que da privacidade.

A salvaguarda da privacidade está sem dúvida relacionada com a proteção dos dados, nomeadamente através da garantia protetora dos dados desde a conceção, e por defeito. A diferença mais substancial entre a noção de «proteção da privacidade» e a noção de «proteção de informação» do ponto de vista da cibersegurança, poderá ser que, a privacidade dos dados versa mais sobre o acesso autorizado, isto é, quem tem acesso e quem o define. Já o conceito de proteção de dados (do ponto de vista da segurança) poderá incidir mais sobre as salvaguardas dirigidas contra o acesso não autorizado.

102 AMA-Agência para a Modernização Administrativa. 2024. «Princípios». https://mosaico.gov.pt/principios.

103 Figura apenas para visualização de painel de controlo, valores não preenchidos.

Esta é meramente uma hipótese que colocamos e cuja resposta objetiva implicaria desencadear um levantamento exaustivo que investigasse as opções técnicas disponíveis para o efeito.

Mas é esta distinção que permite pensarmos, de forma separada, acerca do exercício do acesso autorizado e do acesso não autorizado e abre uma janela importante para refletirmos sobre o desempenho da privacidade enquanto fator fundamental para a perpetuação de outros direitos sociais, particularmente a liberdade, a dignidade, a autonomia, a justiça e a democracia. Isto ilustra como o âmbito do conceito de proteção de privacidade vai muito além do escopo da segurança dos dados, expressa pela corrente da cibersegurança. A pesquisa que levámos a cabo neste trabalho, esclareça-se, endereçou-se essencialmente à primeira noção, a da «proteção da privacidade».

Ainda no Mosaico, a partir da secção da área técnica «segurança de informação» pudemos constatar que estão previstas duas certificações: uma Certificação da Conformidade com o Quadro Nacional de Referência para a Cibersegurança e um «Selo de Maturidade Digital». A primeira denuncia-se, pelo nome, fora do âmbito que nos interessou investigar pelas razões supramencionadas. Mas a segunda permitiu-nos identificar uma oportunidade útil para a solução do nosso questionamento.

2.2.2 SELOS DE MATURIDADE DIGITAL

Os Selos de Maturidade Digital foram apresentados no final de 2021, como modelo oficial de certificação de boas práticas digitais, dirigido a organizações de ambos os sectores, público e privado. São uma criação nacional, proveniente do XXII Governo Constitucional (2019-2022), por um consórcio que reuniu o Instituto Português de Acreditação (IPAC), o Instituto Português da Qualidade (IPQ), a Imprensa Nacional Casa da Moeda (INCM) e a, atualmente extinta, Estrutura de Missão Portugal Digital (EMPD). Foi uma ideia inspirada em iniciativas internacionais propostas pela *Global Enabling Sustainability Initiative* (GeSI)[104].

Os Selos de Maturidade Digital propõem um esquema de certificação assente num modelo flexível e evolutivo. Foram apresentadas quatro dimensões certificáveis, concretamente: a da sustentabilidade, a da cibersegurança, a da acessibilidade e a da privacidade e proteção de dados pessoais. Convergem em cinco Selos de Maturidade Digital distintos, sendo previsto existir o Selo de Cibersegurança, o Selo de Sustentabilidade, o Selo de Acessibilidade, o Selo de Privacidade e Proteção de Dados Pessoais e o Selo de Maturidade Digital global, que integra os anteriores. Por sua vez, cada selo pode atingir respetivamente três níveis de maturidade: baixo (bronze), médio (prata) e bom (ouro).

Os selos permitem conhecer o estado real das entidades que se candidatam à sua obtenção, potenciando simultaneamente uma melhor gestão das organizações, acompanhada de avanços no caminho da maturidade digital de cada organização. Quando uma organização atinja os critérios necessários em cada dimensão, recebe o direito ao uso da marca Selo de Maturidade Digital, na categoria e nível acreditados correspondentes. E, supostamente, poderia beneficiar de um incentivo financeiro suportado pelo Plano de Recuperação e Resiliência, por cada dimensão de certificação obtida. A iniciativa teria como meta «certificar 15 mil entidades no período de vigência do PRR (até 2026) com a dotação de 30 milhões de euros previstos para a sua concretização»[105].

As entidades que se encarregaram da definição das normas de atribuição da certificação, para cada dimensão, foram o Centro Nacional de Cibersegurança (CNCS), a Agência para a Modernização

104 GeSI é uma «organização mundial de membros da sociedade civil, dedicada a permitir que o sector das tecnologias de informação e comunicação aproveitem as oportunidades geradas, pela aplicação de soluções digitais, aos desafios ambientais e sociais mais prementes do mundo» (gesi.org)

105 Direção-Geral das Atividades Económicas. s.d. «Selos de Maturidade Digital». www.dgae.gov.pt/servicos/politica-empresarial/competitividade/selos-de-maturidade-digital.aspx.

Administrativa (AMA), a Direção-Geral das Atividades Económicas (DGAE) e a Comissão Nacional de Proteção de Dados (CNPD).

O contributo mais relevante dos selos pretendia ser a «confiança como bem comum», permitindo «a cada cidadão o conforto e a confiança de saber que por trás de cada sítio certificado na *Internet* que os utilize, estão um conjunto de regras técnicas e organizacionais claramente definidas, cuidadosamente implementadas que permitirão assegurar a segurança, a privacidade, a usabilidade e a sustentabilidade desse ato»[106]. Mas a ambição detrás da construção, implementação e operação deste sistema de Certificação da Maturidade Digital das empresas e organismos públicos foi também permitir posicionar Portugal como referência ao nível da União Europeia nestas matérias. Ou seja, exportar esse referencial para a escala europeia, segundo a lógica de que com o aumento da confiança e da maturidade digital as empresas portuguesas capitalizariam o poder digital, acrescentando valor económico ao reconhecimento do caso português, nos mercados nacionais e internacionais[107].

As expressões «Portugal pioneiro na certificação» e «a certificação é fundamental para a transição digital da economia» podem sugerir motivações ligeiramente afastadas do timbre sugerido na mensagem introdutória do «Guia metodológico para serviços públicos baseados em direitos humanos» (alusivo à plataforma Mosaico), mas admitamos a confluência das intenções entre empresas «mais seguras, mais ágeis, mais digitais e mais perto dos clientes» e a visão centrada no utilizador. Visão justificada pelo sentido de compromisso dos dirigentes envolvidos na transição digital, traduzido nas palavras: «Assegurar a transição digital da nossa economia e sociedade significa garantir que cada vez mais pessoas, empresas e organizações beneficiem amplamente das vantagens que a eficácia, a eficiência e a transparência podem oferecer através da utilização mais disseminada das tecnologias digitais.»[108]. Contudo, não fica esquecida a relação subsidiária de apoio às empresas que denota o peso económico do programa financiado no âmbito do PRR[109].

Os Selos de Maturidade Digital no domínio da Cibersegurança, Privacidade, Proteção de dados e Acessibilidade vêm mencionados no Relatório Nacional sobre a Década Digital 2023, proporcionado pela Comissão Europeia, com a possibilidade de verem a sua adoção implementada através da rede de Pólos de Inovação Digital[110]. Mas no relatório do ano seguinte já não aparecem referidos, nem no anexo do Relatório sobre o estado do sector digital, um breve relatório por país que avalia os roteiros estratégicos nacionais da Década Digital adotados pelos Estados-Membros em 2023 e que apresenta uma panorâmica dos seus esforços de digitalização, formula recomendações de melhoria e acompanha a aplicação da Declaração Europeia sobre os Direitos e Princípios Digitais – sendo por isso, um lugar expectável para encontrar referência aos Selos de Maturidade Digital.

Dada a ausência atual de informações prontamente disponíveis acerca das instruções e passos envolvidos para cada um destes selos, em particular o da privacidade que mais nos interessava consultar, presumimos que cada dimensão terá tido o seu processo temporal de normalização independente.

106 Discurso de Mariana Vieira da Silva, enquanto Ministra de Estado e da Presidência, na Conferência «Selos de Maturidade Digital – Portugal pioneiro na certificação» INCM. 2021. Gravação em vídeo da conferência disponível no YouTube.

107 Discurso de Carlos Silva, Assessor do Conselho de Administração da INCM, na Conferência «Selos de Maturidade Digital – Portugal pioneiro na certificação» INCM. 2021. Gravação em vídeo da conferência disponível no YouTube.

108 Texto ligeiramente revisto para melhorar a clareza e adequar-se ao formato escrito, a partir do discurso de Pedro Siza Vieira enquanto Ministro do Estado, da Economia e da Transição Digital, na Conferência «Selos de Maturidade Digital – Portugal pioneiro na certificação» INCM. 2021.

109 Direção-Geral das Atividades Económicas. s.d. «Componente C16 Empresas 4.0» www.dgae.gov.pt/prr/componente-c16empresas-40.

110 Espaços que permitem às empresas testar a inovação e incorporar tecnologia.

Sendo compreensível que a eliminação de um dos agentes participantes se faça ressentir na história destes selos. A informação mais recente obtida acerca do Selo de Privacidade indicia que o respetivo documento de normalização, o «DNP 4577-2:2021 Maturidade digital – Selo digital, Parte 2 – Privacidade e Proteção de Dados, Requisitos» se encontraria no crivo da CNPD. Sendo certo que, à data, a dimensão da privacidade é a única das quatro categorias que não se encontra nos separadores das dimensões do *site* desta certificação.

2.2.3 SELO DE USABILIDADE E ACESSIBILIDADE

Nas restantes áreas técnicas do Mosaico, chamou-nos a atenção um modelo de certificação disponibilizado, já completo e com os resultados de implementação consultáveis: o «Selo de Usabilidade e Acessibilidade» (doravante SUA)[111] que tem por objetivo simplificar e tornar mais eficiente a utilização dos serviços públicos *online* para todos os cidadãos, independentemente das suas capacidades sensoriais, motoras ou cognitivas. Este selo insere-se numa série de programas e estratégias introduzidas internacionalmente, destinadas a proporcionar o acesso às Tecnologias da Informação e Comunicação (TIC) e dando mérito a uma conceção universal, política, de inclusão digital.

Este selo resulta de uma iniciativa desenvolvida pela Agência para a Modernização Administrativa (AMA) e pelo Instituto Nacional para a Reabilitação e permite identificar, promover e distinguir a implementação «das melhores práticas de usabilidade e acessibilidade em sítios *web* e aplicações móveis»[112]. O selo encontra-se dividido em três níveis de exigência: bronze, para requisitos básicos de acessibilidade e usabilidade; prata, nos casos que incluem requisitos básicos e intermédios e ouro, quando abrangem todos os requisitos, incluindo testes com utilizadores.

A primeira etapa implica sucessivamente a avaliação, o preenchimento e a publicação de uma «Declaração de Acessibilidade e Usabilidade», no *site* de cada organização. Sendo que o decreto-lei n.º 83/2018, de 19 de outubro estabelece a obrigatoriedade de que todos os *sites* da Administração Pública em Portugal publiquem a sua Declaração de Acessibilidade[113], tendo o prazo para a publicação desta exigência terminado a 23 de setembro de 2020 e, desde então, todos estes *sites* devem ter disponível publicamente essa declaração.

Para a elaboração de uma Declaração de Acessibilidade e Usabilidade existem dois procedimentos obrigatórios e um processo recomendado. Os imperativos são: que exista uma avaliação automática e outra manual; quanto à opcional, diz respeito à realização de testes de usabilidade com pessoas com deficiência.

Avaliação automática e avaliação manual necessárias à Declaração de Acessibilidade e Usabilidade

Na avaliação automática é sugerida a utilização da ferramenta desenvolvida pela AMA, o validador AccessMonitor, parametrizado de acordo com as recomendações de práticas de acessibilidade *web*

111 Esta certificação une duas áreas distintas que iremos de detalhar adiante mas abordando-as previamente de forma sucinta: a acessibilidade digital refere-se ao princípio fundamental pelo qual é conferida aos utilizadores virtuais «igual oportunidade de uso, de forma amigável, digna e segura», permitindo que todos eles interajam com os conteúdos de qualquer *site* ou aplicação móvel, independentemente de usarem estratégias de adaptação ou tecnologias de apoio diferentes; já a usabilidade é uma disciplina de desenho de produto, aplicável ao contexto digital, que fornece as orientações para que um produto seja, simultaneamente, eficaz e satisfatório para o seu utilizador. Esta última é uma área técnica que abrange especificidades concernentes à interação dos utilizadores com determinados produtos como, por exemplo aplicações ou *interfaces* em âmbito digital, permitindo a minimização das suas frustrações ou a criação de uma experiência de navegação agradável.

112 Portal ePortugal. 2019. «Foi lançado o Kit do Selo de Usabilidade e Acessibilidade».

113 República Portuguesa. 2018. «Decreto-Lei n.º 83/2018».

WCAG 2.1, provenientes da comunidade internacional *World Wide Web Consortium* (W3C)[114], ou, em alternativa, o RocketValidator e o *plug-in* para Chrome Axe, da DeQue. No nosso entender, o facto de oferecer estas alternativas confere ao enredo narrativo da certificação uma tónica de complementaridade, em detrimento de exclusividade vinculativa.

Para a avaliação manual, a AMA desenvolveu uma lista de verificação de dez aspetos críticos de acessibilidade funcional, resultante de diversos estudos em *sites* da Administração Pública portuguesa, elaborados pela equipa da Unidade ACESSO (integrada na Equipa de Experiência Digital da AMA) e baseada também na lista de verificação do «W3C Easy Checks - A First Review of Web Accessibility». Este procedimento específico de verificação de uma listagem fundamentada em trabalhos anteriores, com reapreciações não exclusivas do âmbito académico, foi determinante para a intenção deste trabalho em elaborar um produto que pudesse ser utilizado como diretório de observação da dimensão da privacidade nos *sites*.

Do mesmo modo, também o procedimento opcional de realização de testes de usabilidade com pessoas com deficiência foi inspirador, porque espelha a participação da comunidade mais afetada pela problemática em questão, que é chamada e envolvida no trabalho de pesquisa e operacionalização das soluções. Assim, justifica-se que no tema da privacidade, os utilizadores da *Internet* possam ser também recrutados no processo de definição do modo como as políticas de privacidade expressam este assunto em cada organização.

A consonância das declarações de acessibilidade divide-se em três situações: plenamente conforme, parcialmente conforme e não conforme. Qualquer uma destas posições é obtida consoante o preenchimento de um formulário que conduz a organização pelas secções da declaração e apresenta no final do preenchimento, uma página online pronta a publicar. Sendo que, nesse processo, são anexados documentos elaborados previamente, constituindo prova das evidências que anunciam e permitindo às organizações a possibilidade de corrigir aspetos que detetem durante o processo. Este modelo pareceu-nos interessante de replicar por várias razões:

a. Está publicamente descrito e qualquer pessoa interessada pode investigar se tem condições para empreender esforço semelhante. No que diz respeito aos organismos fora da responsabilidade da Administração Pública, esta iniciativa pode exercer uma influência positiva.
b. Não exige uma sobrecarga na qualificação dos agentes que iniciem estas avaliações, porque a informação sobre o processo é convenientemente organizada em passos sucessivos, corrigíveis e sem com isso comprometer a complexidade do assunto.
c. Faculta os resultados da iniciativa, permitindo a consulta posterior a entidades interessadas.

Por fim, as organizações que vejam concluída nesta etapa uma «Declaração de Acessibilidade Plenamente conforme», podem passar ao patamar seguinte: o da candidatura ao Selo, que irá atribuir à entidade o carimbo consoante o grau de execução das práticas de acessibilidade e usabilidade, listadas nos requisitos do «kit-selo».

Os estados diversos das declarações dos *sites* da Administração Pública, bem como a atribuição da tipologia dos Selos, podem ser consultados nos dados disponibilizados pelo Observatório Português da Acessibilidade que afere, no período decorrente entre 15 de dezembro 2020 a 29 de julho 2024, 2044 *sites*, sob responsabilidade de 1180 entidades, arrumados em 35 diretórios.[115]

114 Esta organização é de interesse público e sem fins lucrativos, procura implementar estratégias, normas e recursos para tornar a *Internet* acessível a pessoas com deficiência.

115 AMA-Agência para a Modernização Administrativa. 2021. «Observatório Português da Acessibilidade Web». https://observatorio.acessibilidade.gov.pt/directories.

2.2.3.1 INCLUSÃO E ACESSIBILIDADE DIGITAL

À medida que as sociedades contemporâneas foram convertendo mais tarefas e experiências da vida quotidiana em interações automatizadas e digitalizadas, a inclusão digital foi ganhando relevância e surgindo como questão fundamental para a redução das desigualdades. A inclusão digital pode ser definida, em sentido amplo, como o conjunto de diferentes medidas concebidas para garantir que todas as pessoas tenham igualdade de acesso, oportunidades e competências para beneficiar das tecnologias e sistemas digitais. Desde 2015, a inclusão digital tem sido uma componente estipulada numa das visões globais estabelecidas pela Assembleia Geral das Nações Unidas para um modelo global de governação com a finalidade de acabar com a pobreza, proteger o ambiente e promover a prosperidade e o bem-estar de todos até 2030. Esta finalidade destaca-se, particularmente, na décima meta dos Objetivos de Desenvolvimento Sustentável (ODS), que prevê reduzir as desigualdades através da capacitação e promoção da inclusão social, económica e política de todos.

A investigadora grego-britânica Panayiota Tsatsou identificou as pessoas com deficiência, as minorias étnicas, os refugiados, os idosos, os sem-abrigo e os agregados familiares monoparentais como os grupos vulneráveis que mais são deixados para trás nos avanços tecnológicos, carecendo de mais soluções combativas da exclusão digital[116]. Por outro lado, barreiras transversais como a falta de literacia informacional, a utilização ineficaz da tecnologia e novos riscos associados ao aumento da transformação digital como o assédio digital, o discurso de ódio e a desinformação, dificultam ainda mais a inclusão destes grupos vulneráveis.

Numa investigação em países em vias de desenvolvimento, Özlem Yorulmaz, da Universidade de Ankara, salienta o impacto significativo das TIC, destacando-o enquanto vetor de mudanças sociais e económicas, que podem dar origem a potenciais consequências a longo prazo no bem-estar geral e no desenvolvimento dos indivíduos e das sociedades, sugerindo que possam ser considerados como indicadores das TIC o trio composto pelo Índice de Economia e Sociedade Digital (DESI), o Índice de Mulheres no Digital (WID) e o Índice Digital Rural (RDI), propostos pela Comissão Europeia[117]. O seu estudo sobre o efeito destes índices no desenvolvimento humano e na desigualdade de género, mostrou que, mesmo entre os países da UE, existe desigualdade no acesso e na utilização da tecnologia, caraterizada como fosso digital (*digital divide*), seja pela falta ou limitação de acesso a serviços digitais decorrentes de impedimentos físicos, económicos, ou de literacia. É relevante a constatação de que o fosso digital, por atuar condicionalmente ao nível individual, compromete o crescimento económico.

Esta noção é também evidenciada pela investigadora Olga Buchinskaia, do Instituto de Economia da Academia das Ciências da Rússia, que examinou a relação entre a riqueza, conhecimento e digitalização como fonte de crescimento da riqueza dos países e dos indivíduos. O seu estudo indica que, para aumentar o bem-estar a um nível micro, é necessário o acesso a pelo menos dois desses três fatores (riqueza, conhecimento e digitalização), classificando a sua inter-relação como definidora de «uma armadilha de pobreza a nível individual»[118]. Sendo que estas componentes estão sujeitas ao princípio segundo o qual «os ricos ficam mais ricos e os pobres ficam mais pobres» (também conhecido como efeito Mateus, ou da vantagem acumulada), numa conjuntura em que as restrições impostas pelos principais intervenientes no mercado financeiro podem aumentar a divergência. Mas as suas conclusões estendem-se além dessa confirmação, aprofundando rastros de iniciativas já avançadas, ao demonstrar que a dependência do PIB em relação ao nível de conhecimento é maior do que a dependência do PIB em relação ao desenvolvimento de tecnologias digitais.

Percebemos que por um lado, num sentido lato, a trajetória da economia pode perfeitamente

116 Panayiota Tsatsou. 2022. «Vulnerable people's digital inclusion: intersectionality patterns and associated lessons».

117 Özlem Yorulmaz. 2023. «A Detailed Analysis of the Digital Divide and Its Impact on the Development of Countries».

118 Olga Buchinskaia. 2022. «The Threefold Divergence of Socio-Economic Development in the Digital Age».

incluir as preocupações com o fosso digital na medida em que, potencialmente, se convertem em vantagens económicas. O que vem demonstrar a pertinência de incluir todos, numa sociedade que abarca acrescidamente o aspeto digital às várias dimensões da vida corrente. Mesmo que as dificuldades de acesso, conduzidas pelo fenómeno da tecnologia, não sejam assunto de completa novidade, reconhece-se que com a digitalização a sua complexidade no mundo digital se intensificou.

A acessibilidade digital envolve o processo de desenho e desenvolvimento de produtos e serviços digitais de tal forma que estes permitam às pessoas com deficiência, ou quaisquer outras necessidades específicas, interagirem eficazmente com conteúdos *online* e utilizarem esses produtos de maneira significativa e equitativa, independentemente das suas capacidades cognitivas ou físicas[119]. Esta abordagem inclusiva é fundamental para assegurar que as tecnologias sejam acessíveis a todos os membros da sociedade. Daqui se antevendo a justificação da ponte com a área técnica da usabilidade.

Em consonância com tais preocupações, Luciana Terceiro reflete sobre as práticas de acessibilidade digital no desenvolvimento de produtos e serviços digitais, como os *sites*, destacando a importância da incorporação da acessibilidade como prática rotineira, integrada na visão das metodologias do design, que constata não ser uma questão priorizada[120]. Aponta como razões para essa lacuna fatores como custos e tempo de desenvolvimento nos projetos tecnológicos e a tendência para uma cultura organizacional das empresas e *designers* que, inadvertidamente, exclui pessoas com deficiência no processo de criação e teste de produtos, resultando na falta de consideração pelas suas necessidades de acessibilidade[121]. O que evidência um certo insucesso dos produtos digitais por, ao excluírem as questões de acessibilidade, aumentarem a frustração de alguns utilizadores. Assim, a inclusão das melhores práticas de acessibilidade digital no desenvolvimento de produtos e serviços digitais permite, também, obter decisões mais informadas sobre os próprios produtos. Esta observação foi essencial para acionar a questão de partida para a investigação que fizemos, no sentido de nos interrogarmos sobre se também as práticas de salvaguarda da privacidade, uma vez incluídas no processo de conceção dos produtos e serviços digitais, fariam resultar em decisões mais esclarecidas, formuladas no seu desenho final.

Um estudo de Carie Fisher, Sunghyun Kang e Cyndi Wiley investigou a representação das pessoas com deficiência na indústria tecnológica e corrobora a ideia de limitação de práticas de acessibilidade por falta de recursos e constrangimentos de tempo, revelando além do mais, que os profissionais de tecnologia digital têm níveis variados de sensibilização e compreensão da acessibilidade digital - em geral com algum desconhecimento sobre as orientações e recursos de acessibilidade, ainda que os participantes tenham reconhecido positivamente a importância da acessibilidade para a inclusão e a igualdade de acesso à informação[122]. De resto, as conclusões do mesmo estudo destacam: a relevância em desenvolver uma cultura de acessibilidade nas organizações de forma a integrar as considerações de acessibilidade no processo de conceção e desenvolvimento desde o início; bem como a necessidade de uma maior sensibilização, educação e apoio aos profissionais de tecnologia para garantir a implementação efetiva da acessibilidade digital no seu trabalho[123]. Aliás, uma das razões pelas quais o SUA junta as duas áreas (acessibilidade e usabilidade) é que «a reunião desses esforços permite às equipas que elaboram os serviços digitais não só melhorarem a sua reputação, como contornarem a morosidade de reuniões muitas vezes fracassadas, não tardando em resolver o tema da acessibilidade com frequência

119 Izabel Rodrigues da Silva et al. 2021. «Acessibilidade digital em tempos de ensino remoto».

120 Luciana Terceiro. 2023. «Nothing about us without us: The journey of digital accessibility in the making».

121 Ibid.

122 Carie Fisher, Sunghyun Kang e Cyndi Wiley. 2023. «Awareness, Understanding, and Attitudes of Digital Accessibility in Technology Professionals».

123 Ibid.

remetido a fases seguintes e abandonado»[124]. O que aponta para um ponto comum com a privacidade digital, uma vez que também se trata de uma área marcada pela escassez de literacia organizacional no âmbito de uma cultura de privacidade.

No seu conjunto, estas constatações vão ao encontro do que Buchinskaia apurou acerca dos países caracterizados por rendimentos médios, ou seja que estes têm potencial para se desenvolverem através do avanço do conhecimento e de uma política racional de digitalização[125].

2.2.3.2 USABILIDADE

A evolução do conceito de usabilidade iniciou-se nos anos 80 com o lema «fácil de aprender, fácil de usar» que se refere à capacidade de um produto ser facilmente utilizado, consistente com o que a norma ISO 9126-11 define como qualidade de *software*. Brian Shackel, citado por Lukas Windlinger e Deniz Tuzcuoglu, discutiu a usabilidade como um conceito situacional, ou seja, a conceção de ferramentas como dependente dos utilizadores, tarefas e ambientes e descreveu o paradigma da usabilidade em termos de: 1) utilidade (ou seja, se a ferramenta fará o que é necessário em termos funcionais), 2) usabilidade (ou seja, se os utilizadores a utilizarão com êxito) e 3) simpatia (ou seja, se os utilizadores a consideram adequada)[126]. Estas dimensões tornaram-se as caraterísticas definidoras do entendimento moderno de usabilidade, tal como é definido pela Organização Internacional de Normalização (ISO) enquanto «medida em que um produto pode ser utilizado por determinados utilizadores para atingir objetivos precisos com eficácia, eficiência e satisfação num contexto de utilização específico»[127].

A usabilidade é um atributo fundamental para o sucesso de produtos de *software*, e a abordagem denominada «*Design* Centrado no Utilizador» (*User-Centered Design*, UCD) tem sido amplamente promovida como um quadro metodológico eficaz para melhorar a experiência do utilizador[128]. Por sua vez, a «experiência do utilizador»[129] é um conceito amplo que se refere à qualidade da interação de um utilizador com um produto ou serviço, indo além de simplesmente atender às suas necessidades imediatas. Envolve a criação de produtos que não são apenas funcionais mas também agradáveis de usar, através da integração em concordância entre várias disciplinas como a engenharia, o *marketing*, o *design* gráfico e industrial e o *design* de *interfaces*[130].

No contexto da *Internet* a usabilidade é um fator crucial para o desempenho dos *sites*, pois se apresentarem dificuldades de uso os utilizadores tendem a abandoná-los rapidamente. Jakob Nielsen apela a que a experiência de utilização seja intuitiva e eficiente: a página inicial de um *site* deve comunicar de forma clara e concisa os serviços ou produtos oferecidos pela empresa, bem como as ações que os utilizadores podem realizar nele, caso contrário, os utilizadores também perderão o interesse; e se a navegação for confusa ou se as informações apresentadas forem difíceis de ler e não responderem às principais questões dos utilizadores, estes procurarão alternativas[131], portanto a usabilidade, defende Nielsen, não permite margem para ambiguidades ou complexidades desnecessárias, pois os

124 Discurso de Pedro Alves, *User Experience Researcher* da AMA, nas «Jornadas de Acessibilidade e Usabilidade Digital da Administração Pública 2023» AMA. 2023.

125 Buchinskaia. 2022.

126 Lukas Windlinger e Deniz Tuzcuoglu. 2021. «Usability theory: Adding a user-centric perspective to workplace management».

127 ISO 9241-11 2018 citado por Windlinger e Tuzcuoglu. 2021.

128 Elizabeth Salinas, Rony Cueva e Freddy Paz. 2020. «A Systematic Review of User-Centered Design Techniques».

129 Em inglês o termo conhecido é *User Experience* (UX).

130 Don Norman e Jakob Nielsen. 1998. «The Definition of User Experience (UX)». www.nngroup.com/articles/definition-user-experience.

131 Jakob Nielsen. 2012. «Usability 101: Introduction to Usability». www.nngroup.com/articles/usability-101-introduction-to-usability.

utilizadores não investem tempo a tentar decifrar *interfaces* complicadas, preferindo explorar outras opções disponíveis.

O teste com utilizadores é o método de avaliação de usabilidade mais comum, considerado essencial para a identificação direta de problemas de usabilidade. Outras abordagens incluem questionários, entrevistas e métricas de usabilidade[132].

Simultaneamente e no seu conjunto, estes termos continuaram a reforçar e situar-nos na corrente especializada da conceção centrada no utilizador, que tem como objetivo criar produtos digitais que respondam às necessidades, preferências e expectativas dos utilizadores, inserindo-se na abordagem *user-centric*, já referida.

Conclusão sobre o Selo de Usabilidade e Acessibilidade

Rematando o tópico, e de volta ao resultado da convergência entre a acessibilidade e a usabilidade, manifestada pelo processo de certificação envolvido no Selo com o mesmo nome (SUA): identificamos nele um carácter escrutinador, de transparência das organizações e conferente de *compliance*.

Concordamos com a utilidade da ferramenta descrita no SUA que diagnostica e identifica as melhorias a realizar em ambas as áreas, dado que: permite ganho de tempo despendido nesta operação ao possibilitar às equipas superarem a lacuna da representatividade da acessibilidade de um produto final; e por outro lado, potenciar intervenções mais extensas nestas duas matérias (acessibilidade e usabilidade) em projetos seguintes, dada a preparação proporcionada aos agentes intervenientes.

A proposta de aproximação de esforços entre áreas distintas, no caso, comungada a partir da centralidade na experiência do utilizador, e ainda pela necessidade formal de articulação com a regulamentação própria, faz da metodologia operacionalizada no Selo de Acessibilidade e Usabilidade uma referência interessante de seguir, até para dar resposta à tendência anteriormente apontada, da falha na avaliação dos resultados das medidas políticas da Administração Pública.

Adicionalmente, sendo o caracter humanístico das ciências sociais uma lente pela qual se observa a realidade, logicamente se entende a preferência de exploração na pista deixada pelo SUA, em detrimento do Selo de Maturidade Digital que se afigurou um padrão mais intransponível.

Assim surgiria a questão: 'É possível realizar um diagnóstico da privacidade *online*, de modo semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4A) A replicação do modelo usado no Selo pressuporia conhecer a ferramenta automática mais adequada para o efeito de diagnóstico da privacidade *online*, bem como perceber qual a ferramenta manual indicada para o mesmo efeito.

2.3 SÍNTESE DAS QUESTÕES DE INVESTIGAÇÃO

A pergunta geral que serviu de ponto de partida à investigação foi: 'A privacidade individual é adequadamente salvaguardada no ecossistema digital?' (Q1) Esta questão apareceu antes de uma mudança na compreensão do problema, pois o RGPD e a propagação do impacto das suas medidas, representam já uma transformação crucial no equilíbrio entre a inovação tecnológica e a proteção da privacidade individual: ao impor responsabilidades rigorosas às entidades que processam dados pessoais *online* e exigindo-lhes que demonstrem ativamente essa conformidade de forma clara e acessível, conferiu aos cidadãos maior controlo sobre os seus dados. A pergunta de investigação Q1 evoluiu então para: 'As políticas de privacidade e outros mecanismos em vigor demonstram conformidade com uma aborda-

132 Salinas, Cueva e Paz. 2020.

gem centrada no utilizador para a proteção da privacidade?' (Q2A). Esta questão viu-se fundamentada pela análise do conceito *privacy by design* e seus sete princípios que salientam a importância de uma abordagem proativa e centrada no utilizador. Estudos indicam que apesar do interesse em que as políticas de privacidade proporcionem um fator de confiança do utilizador, estas são frequentemente difíceis de compreender e negligenciadas, fenómeno conhecido como o «paradoxo da privacidade».

Da reformulação da pergunta de investigação Q2A emergiram duas questões derivadas que orientaram a investigação para aspetos mais específicos: 'De que maneiras podemos observar e avaliar a conformidade das políticas de privacidade com uma abordagem centrada no utilizador?' (Q2B); e: 'Como podemos verificar a conformidade com a proteção da privacidade centrada no utilizador, na realidade portuguesa?' (Q2C).

Com a questão derivada Q2B procurámos identificar métodos e indicadores concretos para avaliar se as políticas de privacidade e outros mecanismos realmente demonstram conformidade com uma abordagem centrada no utilizador. Encontrámos alguns esclarecimentos nas formas de visualização e comunicação das políticas de privacidade, nomeadamente através de painéis de controlo, certificações, rótulos, *banners*, *pop-ups* e ícones de privacidade, que facilitam a compreensão e gestão das opções de privacidade pelos utilizadores e que por serem mecanismos claros e acessíveis, se tornam indicadores concretos da validade das políticas de privacidade. Adicionalmente, a LUAP resultante do trabalho de Barth, Ionita e Hartel (2022) ofereceu-nos uma base qualitativa para a investigação, permitindo apreciar as diversas categorias de práticas de privacidade. Esta lista forneceu um quadro robusto para observar e avaliar se as políticas de privacidade estão alinhadas com os princípios de uma abordagem centrada no utilizador, conforme estipulado pelo RGPD e pela privacidade desde a conceção, assim, a pesquisa realizada para responder à questão Q2B foi crucial para operacionalizar a investigação numa metodologia própria e definir critérios mensuráveis de análise.

Em simultâneo, surgiu a interrogação acerca do grau de intervenção do utilizador para a conformidade da proteção da privacidade digital, declarada na questão: 'A conformidade para a proteção da privacidade está dependente da intervenção do utilizador ou os agentes responsáveis pelo desenvolvimento dos sistemas de informação salvaguardam *a priori* a proteção da privacidade, independentemente da intervenção do utilizador?' (Q3).

Relacionado com a questão derivada Q2C ('Como podemos verificar a conformidade com a proteção da privacidade centrada no utilizador, na realidade portuguesa?') identificámos a Administração Pública portuguesa como um setor-chave, devido ao seu compromisso com a prestação de serviços centrados no cidadão. A plataforma Mosaico, desenvolvida pela AMA, forneceu duas pistas fundamentais para o efeito da investigação:

- Explorámos inicialmente o Selo de Maturidade Digital, criado no âmbito do PRR com o objetivo de certificar a maturidade digital das organizações em várias dimensões, incluindo a da privacidade. Contudo, a investigação revelou que a operacionalização da dimensão de privacidade ainda se encontra incompleta, com critérios de avaliação pouco claros e um processo de certificação que carece de transparência, logo, o Selo de Maturidade Digital não constituiu material relevante para sistematizar uma análise sobre a privacidade digital no contexto português;
- Em seguida analisámos o Selo de Usabilidade e Acessibilidade que demonstra melhorias na experiência do utilizador em termos de acessibilidade. A metodologia usada nesta certificação apresentou uma estrutura sólida para a avaliação que poderia ser adaptada para analisar a privacidade *online*. Os temas da privacidade e da acessibilidade partilham (1) um foco no *design* centrado no utilizador, (2) a necessidade de cumprimento com regulamentações, (3) a importância da transparência nos processos de forma que sejam verificáveis e (4) a relevância de uma

maior literacia sobre ambos os assuntos.

Deste modo, a abordagem articulada exposta no SUA e a sua ênfase na participação da comunidade, destacaram a possibilidade de replicar um modelo semelhante para avaliar e promover boas práticas de privacidade *online*. O que levou à formulação da questão: 'É viável realizar um diagnóstico da privacidade *online*, de modo semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4A) Por sua vez, esta pergunta resulta em duas perguntas operacionais: 'Qual seria a ferramenta automática mais adequada para o efeito de diagnóstico da privacidade *online*, de forma semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4B) e 'Qual seria a ferramenta manual mais adequada para o efeito de diagnóstico da privacidade *online*, de forma semelhante à metodologia apresentada no SUA?' (Q4C).

Na ausência de um sistema específico que classifique a privacidade dos *sites* na realidade portuguesa e para operacionalização da resposta sobre o mecanismo automático, considerou-se a adoção de modelos existentes para uma avaliação preliminar conforme será abordado no próximo capítulo. Quanto à extensão da observação manual, as opções existentes no mercado implicam o recurso à intervenção de especialistas Encarregados de Proteção de Dados (EPD) ou auditores.

Até aqui vimos como a privacidade pode ser um ponto crítico na era da informação, profundamente entrelaçada nas dinâmicas sociais e tecnológicas. A análise dos desafios associados e dos contextos internacionais proporcionou uma visão comparativa das abordagens regulatórias e as suas implicações para a proteção de dados. Podemos agora afirmar que uma visão da privacidade deste a conceção e por defeito tende a implementar melhores práticas de privacidade digital.

Ao trazer a problemática para o contexto português, identificamos a relevância das certificações de maturidade digital e a sua possível contribuição para a melhoria contínua das práticas de privacidade. A interseção entre privacidade, acessibilidade e usabilidade surge com um campo fértil para novas investigações, destacando a necessidade de soluções inovadoras que conciliem a proteção do utilizador com uma experiência digital aperfeiçoada.

E por último, após sucessivas formulações de um problema chegamos a uma hipótese que queremos estudar. A questão central que colocamos é se 'O Selo de Usabilidade e Acessibilidade pode, ou não, contribuir para uma configuração mais robusta na salvaguarda da privacidade digital do utilizador?' (Q5). Pretendemos verificar se a implementação bem-sucedida dos princípios de acessibilidade e usabilidade, conjuntamente formalizada na certificação do SUA pode influenciar positivamente a consideração e incorporação de princípios de privacidade desde a conceção, promovendo assim a proteção da privacidade em *sites* e aplicações móveis da Administração Pública portuguesa.

Este enquadramento teórico serviu como base sólida para o desenvolvimento subsequente da nossa investigação empírica, onde procuraremos aplicar e testar a hipótese formulada, bem como as questões que surgiram na trajetória da pesquisa.

CAPÍTULO 3

TRABALHO EMPÍRICO

O capítulo que se segue constitui o trabalho empírico desta investigação e encontra-se estruturado em duas partes: a primeira, 'Metodologia', delineia o plano metodológico do Produto da investigação 1 (PI1) detalhando os aspetos específicos da sua justificação, finalidades, processos de desenvolvimento, orientações de utilização e as considerações sobre a sua fiabilidade e validade; a segunda, 'Apresentação e Discussão de Resultados', apresenta as reflexões sobre os resultados obtidos que conduziram à origem do Produto da investigação 2 (PI2).

3.1 METODOLOGIA

3.1.1 DESENHO DO PLANO METODOLÓGICO

A metodologia que considerámos mais apropriada para responder à questão mais recente, ou a questão principal, 'O Selo de Usabilidade e Acessibilidade pode, ou não, contribuir para uma configuração mais robusta na salvaguarda da privacidade digital do utilizador?' (Q5) é de natureza quantitativa e caracteriza-se por um estudo do tipo correlacional.

Para operacionalizar estas duas áreas em variáveis quantitativas, foi elaborada uma ferramenta de registo dos indicadores observados nos *sites*, com a finalidade de reunir uma amostra para análise estatística: o instrumento de análise PI1 (PI1).

Esta ferramenta consiste num formulário construído na plataforma *online* Airtable, composto por diversos campos a preencher. Cada campo corresponde ao indicador de uma condição averiguável nos diferentes *sites*. O preenchimento de cada campo permite escolher a confirmação do indicador observado. Complementarmente, podem ser acrescentadas notas explicativas ou dúvidas. Sendo, por isso, um formulário misto, de pesquisa essencialmente dicotómica, que constata acerca da ocorrência nos *sites* dos critérios apresentados na ferramenta.

Depois de anotadas todas as observações, extrai-se da plataforma a base de dados com as respostas indicadas, compilando assim uma amostragem para análise.

Posteriormente, numa fase de tratamento estatístico dos dados, haverá lugar a uma análise comparativa para investigar a correlação entre as particularidades da proteção da privacidade e o estado da acessibilidade pressuposto nos *sites* da Administração Pública. Utilizaremos predominantemente o teste do qui-quadrado para variáveis categóricas, com o intuito de verificar a independência ou associação entre essas variáveis. Este teste permitirá identificar se existe uma relação estatisticamente significativa entre a proteção da privacidade e a acessibilidade, proporcionando uma compreensão mais aprofundada das interações entre estas duas áreas.

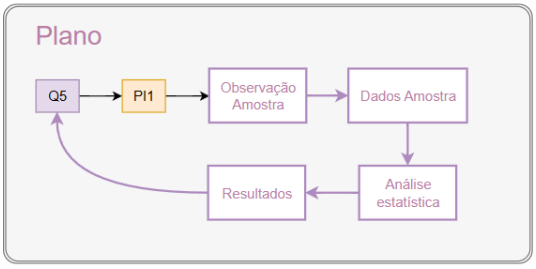


Figura 3.1 - Etapas operacionais da investigação

3.1.2 PROCEDIMENTO DE AMOSTRAGEM

O objeto de estudo que se pretende examinar são todos os *sites* da Administração Pública em Portugal que apresentem Selo de Usabilidade e Acessibilidade. Cada *site* individual constitui uma unidade da amostra.

A informação de ponto de partida, necessária para observação das unidades amostrais, encontra-se disponível nos dados do Observatório Português da Acessibilidade Web. As orientações para proceder ao levantamento dos *sites* certificados são as seguintes:

1) Aceder a uma página de diretório do Observatório Português da Acessibilidade *Web*;
2) No cabeçalho da tabela, ordenar por ordem crescente a coluna do ícone com descritivo «Com Selo de Usabilidade e Acessibilidade»;
3) Ordenar também por ordem crescente, a coluna do ícone que apresenta o descritivo «Com declaração de usabilidade e acessibilidade»;
4) Escolher a unidade da amostra que se pretende observar.

O tamanho delineado da amostra é condicionado pelo reduzido número de *sites* certificados até à data, que é cerca de 30 unidades amostrais.

Para ampliar a amostra e verificar se as mesmas características de privacidade ocorrem em *sites* sem a certificação de acessibilidade, propomos incluir adicionalmente mais 30 unidades amostrais da Administração Pública que não apresentem o Selo. O critério de seleção dos *sites* desta segunda etapa deve seguir o de uma amostragem não probabilística por escolha racional, com base em características específicas, de forma a garantir a representatividade de uma gama variada dos serviços públicos.

A identificação das unidades amostrais realiza-se a cada inserção de *site* observado, no momento prévio à observação dos indicadores, nomenclando a unidade amostral com:

- uma designação lógica para o item que dá entrada (ex: nome da entidade ou domínio do *site*);
- a *url* do *site*;
- a data e hora em que se inicia a observação (informação acrescentada automaticamente).

3.1.3 INSTRUMENTOS E MATERIAIS USADOS

3.1.3.1 INSTRUMENTO DE ANÁLISE PI1 - EIXO DA PRIVACIDADE

O instrumento de análise PI1, por conseguinte destinado a observar a proteção da privacidade desenvolvida de forma centrada no utilizador (presumida pela abordagem *privacy by design*) e alterado para se ajustar à realidade portuguesa, é então constituído por dois eixos principais: o da privacidade e o da acessibilidade.

PI1 – Opções metodológicas na construção de indicadores do eixo da privacidade

A terceira fase da investigação teórica trouxe a questão: 'É possível realizar um diagnóstico da privacidade *online*, de modo semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4A), com um processo de avaliação transparente e aberto.

Na ausência de um sistema de classificação de privacidade para a realidade portuguesa, análogo ao da acessibilidade, ensaiou-se a possibilidade de adotar algum sistema já existente que pudesse fornecer um grau de avaliação prévio. Esta etapa corresponde ao desenvolvimento da questão: 'Qual seria a ferramenta automática mais adequada para o efeito de diagnóstico da privacidade *online*, de forma semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4B),

Ao longo das leituras realizadas para a revisão de literatura foram recolhidas algumas pistas potencialmente úteis no sentido de encontrar um instrumento, simples de operar, para determinar a parametrização da privacidade nos *sites* da Administração Pública portuguesa. Designadamente:

- A aplicação Claudette, uma ferramenta de processamento de linguagem natural, desenvolvida para detetar automaticamente cláusulas possivelmente problemáticas em documentos que determinam os termos de serviço *online*. Foi explorada provisoriamente, sendo apenas possível analisar textos em inglês. Submeteu-se uma versão traduzida de uma política de privacidade, obtida rapidamente através do tradutor *online* DeepL, tendo resultado somente a indicação de não ter encontrado nenhuma cláusula potencialmente abusiva.

Pelo facto de não ser um processo transparente e não ser possível entender os critérios de validação durante o processo de diagnóstico, decidimos que não seria o instrumento identificador de privacidade adequado para esta investigação.

- A extensão de navegador Polisis que publicita fornecer um resumo legível de qualquer política de privacidade recorrendo a aprendizagem profunda (*deep learning*). Pareceu um indicativo promissor por derivar de um modelo de linguagem centrado na privacidade, construído a partir de 130 mil políticas de privacidade e com uma hierarquia de classificadores de redes neuronais sensíveis ao tema, abarcando asssim tanto a visão ampla quanto os detalhes específicos das práticas de privacidade. Porém, todas as tentativas realizadas demoraram demasiado tempo a obter resposta, acabando por não funcionar. Um desfecho que é coincidente com a descrição mais recente reportada nos comentários de classificação acerca do produto, na loja *online* de extensões (a Chrome *Web Store*).
- A extensão de navegador do projeto PrivacySpy que avalia e monitoriza políticas de privacidade *online*, atribuindo-lhe uma pontuação de acordo com um sistema de classificação que pode ser consultado. Tratando-se de um projeto que utiliza código aberto e por indicar o método que o algoritmo executa para calcular a pontuação geral, considerámos um contributo interessante a ser considerado. No entanto, as classificações só estão disponíveis para os *sites* previamente submetidos a avaliação, realizadas em inglês, e listadas num diretório acessível. Ainda que pudéssemos programar uma versão adaptada do programa, tal exigiria competências que se afastam do escopo da investigação, que pretendemos manter dirigida a utilizadores não especializados.
- A extensão de navegador PrivacyCheck que utiliza modelos de extração de dados para resumir qualquer página HTML que contenha uma política de privacidade, analisando o texto e resumindo-o automaticamente. Alegadamente fornece uma visão geral da forma como as empresas utilizam os dados pessoais dos consumidores, num formato gráfico e rápido e, efetivamente, apresenta resultados interessantes.

Quando a ferramenta PrivacyCheck reconhece uma página (obrigatoriamente em inglês) produz uma classificação em percentagem, de duas vertentes distintas: o ponto de vista de controlo do utilizador e o da abordagem planeada no RGPD. Permite, também, consultar a pontuação atribuída a cada rubrica que compõe a classificação final. Se não esbarrasse na barreira da língua, seria exatamente o tipo de ferramenta que pretendíamos colocar à prova nesta investigação.

- O sistema de Inteligência Artificial Guard que analisa automaticamente as políticas de privacidade em serviços digitais, supostamente gerando relatórios de privacidade que identificam e alertam sobre as principais ameaças à privacidade presentes nas políticas examinadas. Este era o produto resultante de um projeto académico que deixou de ter o *site* ativo.

- O Privacy Program da Common Sense cujo objetivo anunciado é fornecer avaliações de privacidade de aplicações e serviços populares para crianças. Faculta notificações bastante concretas, mas apenas funciona nos *sites* que foram submetidos para avaliação da equipa de especialistas da empresa e está orientado para o mercado americano.
- O projeto comunitário Terms of Service; Didn't Read (abreviado como ToS;DR) procura analisar e classificar os termos de serviço e as políticas de privacidade dos principais *sites* e serviços da *Internet*. Devolve as informações importantes para os consumidores, mostrando uma lista simples do que está descrito nos documentos contratuais do *site*, se este for compatível. E mostra uma classificação final de A (melhor) a E (pior); resultante de um processo transparente e revisto por pares, num grupo de trabalho público no Google Groups.

A proposta é interessante por apresentar um sistema de classificação intuitivo visualmente intuitivo, associado aos avisos listados no breve relatório de linguagem informal, retirando o tecnicismo que muitas vezes complica a compreensão destas informações. Disponibiliza as perguntas e respostas efetuadas no processo de classificação, mas a informação é fornecida apenas nos *sites* submetidos a avaliação e os requerimentos não são de resposta automática.

Supomos que a barreira da língua também existiria, embora talvez fosse possível contorná-la com conhecimento qualificado que viabilizasse a instalação e funcionamento do *plug-in* necessário para avaliar outras línguas.

- O rótulo Privacy Rating é semelhante à etiquetagem da União Europeia relativa ao consumo de energia. Trata-se de um instrumento de mapeamento e visualização de características de privacidade dos serviços *online* que resultou do inventário sistematizado proposto por Barth et al. Da «Lista Unificada de Atributos de Privacidade» utilizam apenas doze, agrupando-os em quatro grupos principais: recolha, partilha, controlo e segurança[1]. A classificação é gerada de acordo com as respostas submetidas a um formulário, que podem ser consultadas *a posteriori*.

Esta ferramenta foi concebida para aumentar a consciencialização sobre privacidade entre utilizadores não motivados e para fornecer informações organizadas e relevantes, aos utilizadores que já estão preocupados com a privacidade. A sua principal vantagem face a outros instrumentos é o facto de permitir obter sempre um resultado imediato. Mas também não ultrapassa o constrangimento da obrigatoriedade de ser preenchido por um utilizador fluente em inglês. Foi, no entanto, o instrumento que reuniu maior probabilidade de vir a ser utilizado para um diagnóstico prévio.

Foram, ainda, investigados alguns outros projetos que não conduziram a considerações pertinentes de acrescentar. O que é relevante referir é que nenhum dos processos experimentados demonstrou ser particularmente eficaz para a missão que procurávamos caraterizar. Seja pela barreira da língua, que inevitavelmente adicionava mais passos à obtenção das classificações, podendo trazer o risco de algum enviesamento resultante das traduções, ou porque as apreciações obtidas não permitiam uma leitura tão apurada quanto a proposta unificada dos quinze atributos permite detetar. Mesmo no caso do Privacy Rating que derivou do próprio estudo que cunhou a lista, ao terem os seus critérios de avaliação simplificados acabaram por eliminar algumas camadas da privacidade que seria pertinente conhecer.

Considerámos importante para a presente investigação não abdicar de nenhum dos parâmetros possíveis de analisar, para que fosse possível obter uma perceção exata das vertentes onde a interseção com a acessibilidade pudesse ocorrer.

---

1 Susanne Barth et al. 2021. «Privacy Rating: A User-Centered Approach for Visualizing Data Handling Practices of Online Services».

PI1 – Parametrização dos indicadores do eixo da privacidade

Assim, uma vez estabelecido o referencial que o eixo da privacidade deveria satisfazer, investigámos e refletimos acerca das possibilidades observáveis nos *sites*, capazes de comprovarem a existência, ou a ausência, de cada categoria da LUAP fornecida por Barth, Ionita e Hartel (2022).

Primeiro, procedemos a um levantamento dos aspetos que poderiam confirmar a qualidade de determinado atributo, a que chamam os «argumentos». Concretamente, procurámos conhecer a matéria abordada na definição dos atributos. Consultámos o quadro «Mapping of attributes to proposals» - material complementar do artigo que cunha a LUAP, onde são expostas as anotações que conduziram a investigação do estudo. Fomos cruzando os indicativos aí encontrados com os presentes nos diversos sistemas de classificação (averiguados na fase prévia) que apresentam mais informação específica associada aos atributos. Contrapôs-se sistematicamente a ponto de vista do utilizador, recorrendo aqui à experiência pessoal e individual, mas comum a qualquer pessoa que utiliza a *Internet* regularmente, ainda que esta experiência possa ser influenciada por níveis diferenciados de literacia.

Uma vez obtidas as características essenciais da observância de cada atributo, formulámos as frases que determinam como verificar cada um dos indicadores - os argumentos. Aqui procurámos usar termos simples e claros para que fosse imediata a compreensão do que era pretendido identificar nos *sites*, pois idealmente, qualquer pessoa não especializada estará apta a verificar e preencher os campos da observação. Os argumentos obtidos para cada atributo serão adiante listados.

A ordem pela qual cada atributo foi convocado está relacionada com o grau de importância identificado no estudo de Barth, Ionita e Hartel (2022). Lembrando que se trata de uma hierarquia fundamentada pois resulta do conjunto da avaliação robusta de utilizadores e peritos europeus em matéria de privacidade.

De início, o mecanismo de preenchimento do formulário foi orientado de forma que, a cada campo preenchido, resultasse uma variável categórica (sim/não). Mas, perante atributos que se definiam por mais do que um argumento, foi necessário encontrar outro processo para chegar à confirmação da existência, ou inexistência, de determinada categoria de privacidade (atributo). A este efeito chamamos «cobertura de um atributo».

Para o procedimento de comando da cobertura dos atributos ponderámos acerca do peso, em percentagem, que cada argumento tomaria na composição final do atributo.

Realizámos, em dias diferentes, pelo menos duas rondas de reflexão para a elaboração da «dosagem» adequada. Nos casos em que o consenso falhou, reavaliámos mais vezes, até chegar a um entendimento ajustado. A composição das diferentes componentes encontra-se indicada à frente de cada frase de argumento, consultável no anexo A – 'Parametrização das categorias de privacidade'.

Transferiu-se para o formulário a distribuição encontrada, compondo as respetivas fórmulas, para que a tarefa de cálculo da cobertura dos atributos fosse obtida automaticamente, consoante o preenchimento dos campos no formulário. O código que compõe as fórmulas usadas na plataforma Airtable é facultado no mesmo anexo A[2].

PI1 – Operacionalização dos indicadores do eixo da privacidade

No eixo da privacidade, o formulário passou a apresentar os argumentos correspondentes a cada atributo, sucintamente descritos no início de cada secção. Assim como mostra uma *checkbox*, respetiva a cada argumento, destinada à sinalização nas situações em que se confirma o argumento.

A ação do clique de ativação das *checkboxes* desencadeia um campo pré-preenchido, referente ao argumento relacionado, que indica a percentagem da resposta no valor final do atributo analisado.

2 Em cada atributo ver a fórmula da soma dos argumentos.

Na conclusão de cada atributo, repetiu-se a breve descrição do atributo, para reavivar o conceito. E colocou-se a pergunta «A partir da observação que fez, considera que o atributo está presente neste *site*?». A resposta indica-se consoante a ativação da *checkbox* a essa pergunta. Esta questão adicional permite recolher a subjetividade da observação, possibilitando posteriormente comparar os resultados da compreensão intuitiva do observador, com a objetividade resultante dos valores observados. Este cruzamento permitirá, também, conferir solidez ao estudo.

A cada unidade da amostra, quanto ao eixo da privacidade, devem observar-se os argumentos listados de seguida. Quando, no *site* observado, não se confirmam os argumentos, a *checkbox* ulterior é deixada em aberto. Podendo ser selecionada mais tarde, caso a perceção mude com o avançar da observação do *site*. Em caso de dúvida ou da necessidade de justificar determinadas escolhas, podem ser adicionadas notas num campo final de cada atributo.

1) Para marcação do atributo Venda:
- Confirma-se que o *site* não vende dados.
- Os dados pessoais são vendidos ou alugados.
- Alguns dados são vendidos a terceiros.
- O *site* omite informações sobre a venda de dados.

2) Para marcação do atributo Partilha:
- Confirma-se que o *site* não partilha dados.
- A partilha das informações recolhidas é restrita à transação pretendida.
- São fornecidas opções de controlo sobre a partilha de dados e manutenção da sua propriedade.
- O tratamento dos meus dados inclui transmissões para amigos.
- Os meus dados pessoais podem ser partilhados com outras empresas e fóruns públicos.
- Os meus dados pessoais podem ser apresentados abertamente.
- Prevê-se a partilha de informações para fins de anúncios.
- As informações recolhidas com as minhas atividades são rastreadas por entidades externas.
- As filiais e os terceiros já não estão vinculados às mesmas práticas de privacidade.
- Alguns dos dados recolhidos deixam de ser propriedade do fornecedor de serviços.
- Verifica-se que o *site* é omisso acerca da partilha de dados com entidades externas.

3) Para marcação do atributo Recolha:
- Confirmação da não recolha de dados.
- Limitação, adequação e relevância da recolha de dados.
- Inclusão de informações pessoais identificáveis.
- Inclusão de informações de contato.
- Inclusão de informações demográficas gerais.
- Inclusão do endereço IP do usuário.
- Inclusão de registos do comportamento de navegação.
- Inclusão de preferências específicas do utilizador.
- Inclusão da localização geográfica do utilizador.
- Inclusão de informações financeiras.
- Referência nos códigos-fonte: *pixel*.
- Referência nos códigos-fonte: *tracking*.
- Referência nos códigos-fonte: *analytics*.

4) Para marcação do atributo Finalidade:
- Confirmação da omissão dos fins específicos da utilização de dados pessoais.
- Os objetivos da utilização são identificados no momento da recolha de dados ou previamente.
- É explicado de forma clara para que são utilizados os dados recolhidos.
- Os dados são tratados com uma base legal e com interesse legítimo.
- É especificada uma utilização secundária para outros fins que não a conclusão da interação atual.

5) Para marcação do atributo Transparência:
- Omissão de qualquer informação sobre os dados recolhidos.
- Apresenta uma política de privacidade atualizada e documentada publicamente sobre os dados que recolhem.
- A política de privacidade informa sobre quem retém os dados do utilizador.
- A política de privacidade informa sobre por que utilizam os dados do utilizador.
- Existe uma indicação do período de conservação dos dados.
- A política de privacidade inclui os termos da divulgação dos dados.
- A política de privacidade menciona como são protegidas as informações pessoais.
- Disponibiliza pormenores sobre possibilidades de reidentificação.
- A política de privacidade é facilmente acessível.
- A *interface* do utilizador comunica e apoia os direitos da pessoa em causa através duma prática de gestão de dados aberta e facilmente disponível.
- Os titulares dos dados são informados sobre seus direitos e têm acesso às informações através de notificação prévia à obtenção do consentimento.
- A política de privacidade comunica de forma clara todas as informações essenciais sobre os dados recolhidos.
- O *site* permite que o utilizador tenha acesso às informações pessoais e possa fazer uma cópia de determinados dados.
- As promessas e objetivos declarados no *site* permitem uma verificação independente.
- Existe menção a alterações da política de utilização na política de privacidade.

6) Para marcação do atributo Segurança:
- Existe referência à encriptação das informações recolhidas e processadas.
- Os dados pessoais estão barrados a quem não tem acesso ao seu tratamento.
- A entidade garante a proteção das informações pessoais contra o acesso não autorizado dos dados.
- A entidade garante a proteção das informações pessoais contra a perda acidental dos dados.
- A entidade garante a proteção das informações pessoais contra a danificação dos dados.
- A entidade garante a proteção das informações pessoais contra a destruição dos dados.

7) Para marcação do atributo Responsabilidade:
- A organização responsável pelo tratamento de dados é identificada.
- O titular dos dados pode responsabilizar o serviço e contestar a conformidade dos dados obtidos.
- É mencionado o direito de apresentar queixa a uma autoridade de controlo.
- A resolução do tratamento das queixas é prevista e assegurada.
- A entidade assume a proteção das informações pessoais contra o acesso não autorizado dos dados.
- A entidade assume a proteção das informações pessoais contra a perda acidental dos dados.
- A entidade assume a proteção das informações pessoais contra a danificação dos dados.
- A entidade assume a proteção das informações pessoais contra a destruição dos dados.

8) Para marcação do atributo Retenção:
- O período de conservação dos dados é especificado consoante a finalidade prevista.
- Os dados pessoais não são mantidos por mais tempo do que o necessário para os fins declarados.
- Os dados são destruídos de forma segura mediante pedido ou após o cumprimento dos objetivos.

9) Para marcação do atributo Direito a ser esquecido:
- A possibilidade de apagar informações é abordada.
- A participação individual no direito de solicitar a remoção dos dados do contexto específico ou a quem foram divulgados é garantida.

10) Para marcação do atributo Anonimização:
- É referido o tratamento de forma anónima.

11) Para marcação do atributo Pseudonimização:
- É mencionado que os dados são pseudonimizados.

12) Para marcação do atributo Correção:
- Existe a possibilidade de aceder aos dados de forma simples, rápida e eficiente.
- Existe notificação explícita dos meios pelos quais o utilizador pode solicitar a alteração de dados incorretos.
- A exatidão e o carácter exaustivo dos dados podem ser contestados e revistos.

13) Para marcação do atributo Controlo:
- O utilizador pode optar por não participar na recolha ou no tratamento dos dados e não autorizar.
- O utilizador tem de dar o seu consentimento para a recolha e o tratamento dos seus dados.
- O utilizador pode limitar a recolha, nomeadamente controlar a partilha com terceiros.
- O utilizador pode modificar o período de retenção.
- A descrição das escolhas que conduzem ao pedido de consentimento para recolha e tratamento dos dados é explicita e por isso permite um consentimento realmente informado para qualquer utilizador.
- As opções de utilização apresentam-se em *interface* fácil para qualquer utilizador.

14) Para marcação do atributo Divulgação:
- A entidade especifica a amplitude da divulgação dos dados, mencionando concretamente se o armazenamento é feito na UE.
- A entidade especifica a amplitude da divulgação dos dados, mencionando concretamente se existe transferência de dados pessoais para países terceiros fora da UE.
- Em caso de transferência de dados para fora da UE são garantidas medidas de proteção antes da divulgação de identificadores para o exterior.
- A comunicação de informações pessoais entre jurisdições geopolíticas é feita em conformidade com os requisitos legais, seguindo o princípio da limitação da utilização.

15) Para marcação do atributo Funcionalidade:

- O *site*/*app* limita o aproveitamento dos serviços prestados se o utilizador não partilhar as informações solicitadas.
- O *site*/*app* permite utilizar o serviço sem qualquer prejuízo caso o utilizador opte por não participar na recolha de dados.
- O sistema aparenta incorporar a privacidade do utilizador durante a maior parte da sua utilização funcional.

3.1.3.2 INSTRUMENTO DE ANÁLISE PI1 - EIXO DA ACESSIBILIDADE

Recorrendo à verificação da certificação do SUA, é possível obter uma caracterização mensurável para o eixo da acessibilidade, de onde resultam as seguintes possibilidades:

1) Quanto à certificação do Selo:

- Sem atribuição de Selo de Usabilidade e Acessibilidade;
- Selo Ouro;
- Selo Prata;
- Selo Bronze.

2) Quanto à verificação de uma declaração de conformidade:

- Sem presença de declaração
- Declaração plenamente conforme;
- Declaração parcialmente conforme;
- Declaração não conforme.

3.1.3.3 PI1 - SECÇÃO FINAL DO FORMULÁRIO

No final do formulário existe um campo que proporciona a possibilidade de juntar notas. Não havendo orientações para o que deve ser preenchido, deixa-se ao observador a consideração do que entender pertinente mencionar.

Uma vez terminada a observação do *site*, em todos os parâmetros, deve ser inserido o registo horário do momento em que a tarefa foi concluída. Existe um campo aberto que permite colocar o número total de minutos que a unidade amostral demorou a ser observada, mas o preenchimento dessa informação pode ser realizado mais tarde, e por outra pessoa, na fase de tratamento dos dados. Sugerimos que, preferencialmente, não se interrompam as observações no mesmo *site*.

3.1.3.4 PI1 - TESTES

Uma vez implementada na plataforma Airtable a parametrização completa do formulário, constitui-se o instrumento de análise PI1, acessível aqui[3]. Esta ferramenta de observação assenta, presumivelmente, num modelo adaptável a uma escala maior consoante a quantidade e disponibilidade de recursos (pessoas, tempo e proventos) sendo replicável em qualquer ocasião. A tarefa de construção da ferramenta não estaria concluída sem passar à fase de testagem.

Testámos, então, alguns *sites* com perfis diferenciados, nomeadamente com e sem SUA. Nesta testagem, o observador dos *sites* e ao mesmo tempo utilizador de PI1 foi a própria autora desta investigação. Cada site implicou a caracterização de 3 a 6 campos prévios, correspondentes à identificação da unidade amostral e à classificação do eixo de acessibilidade. Posteriormente, procedeu-se à observação dos 85 argumentos de privacidade, confirmando também a presença de quinze atributos de privacidade. A mediana de seis testes indica que o tempo de duração de cada observação ronda os 32 minutos.

3 https://airtable.com/app4bGtuChn0IiyYC/pagbj0S6adlLVKg6E/form

Os registos destas observações podem ser consultados no anexo B – 'Registos das observações dos testes', bem como as anotações apontadas (informalmente) durante as observações que permitiram algumas opiniões empíricas, acerca da utilização de PI1.

Não apresentamos graficamente os dados obtidos pois poderia induzir em falsas certezas, que ainda não foram confirmadas, uma vez que a representação gráfica deixa supor um grau de fiabilidade que não é permitida pelo facto de estarmos a lidar com testes.

3.1.3.5 PI1 - IMPRESSÕES DE UTILIZAÇÃO DURANTE OS TESTES

As impressões preambulares deduzidas pela utilização de PI1 durante a realização dos testes foram as seguintes:

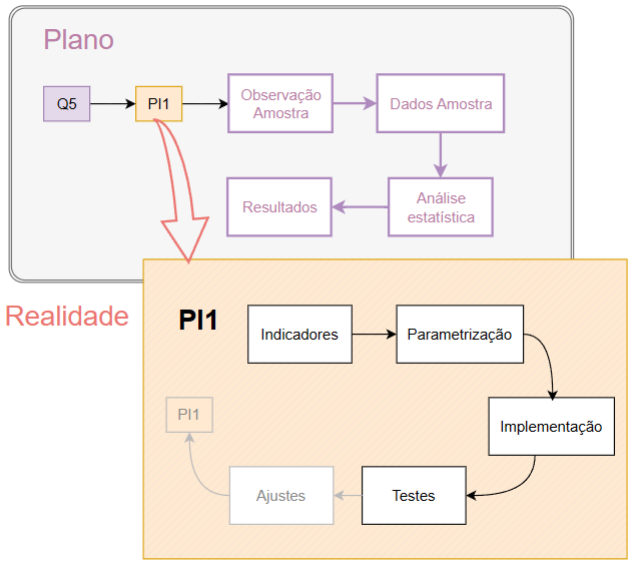
- Experiência desgastante devido à carga do formulário: mesmo com a utilização de uma linguagem simples e objetiva para descrever rapidamente o que procurar em cada *site*, o PI1 revelou-se bastante complexo e exaustivo, com a sua centena de questões a preencher por unidade amostral - em cada *site* podem ser observados entre 103 e 123 campos. Esta grande quantidade de perguntas torna a tarefa de observação cansativa e pode levar a uma diminuição na acuidade dos dados recolhidos.
- Falhas na identificação de campos não previstos: nesta testagem descobrimos que apesar da exaustividade do processo de construção dos indicadores de PI1, ainda há respostas difíceis de encaixar nos registos da observação. O que sugere a necessidade de mais testes para melhoria do instrumento de análise PI1.
- Dificuldades com informações omissas: simultaneamente, lidámos com dificuldades em classificar algumas respostas devido à falta de informações claras em muitos *sites*. Este aspeto destaca a necessidade premente de educar melhor os profissionais sobre a importância de uma política de privacidade bem estruturada e clara, mesmo antevendo o efeito do paradoxo da privacidade, segundo o qual parece incontornável que uma política de privacidade para não ser omissa, tenha de ser extensa, e ao sê-lo, cai invariavelmente no risco de desconsideração.
- Ordem dos atributos: a ordem dos atributos em PI1 que guia o observador nos seus registos pode não refletir a prática real dos utilizadores na navegação pelos *sites*, embora seja lógica em teoria, na medida em que corresponderá à escala de importância que estas dimensões terão para os utilizadores.
- Diversidade de contextos: percebemos que a privacidade digital é abordada de formas muito variadas dependendo do propósito e das finalidades de cada *site*. A caracterização da privacidade digital pode encontrar muitas nuances distintas.

A diversidade dos *sites* e a complexidade de cenários indicam que precisamos de uma abordagem mais refinada no formulário, o que sugere que o instrumento de análise PI1 ainda precisa de ajustes para ser mais eficiente e menos cansativo.

3.1.4 SÍNTESE FINAL DA METODOLOGIA

A figura 4 situa-nos quanto ao ponto de situação atual da pesquisa face ao gráfico inicial da metodologia.

Figura 3.2 - Do plano de investigação ao desenvolvimento conseguido



3.2 APRESENTAÇÃO E DISCUSSÃO DE RESULTADOS

3.2.1 IMPOSSIBILIDADE DE APRESENTAÇÃO DOS RESULTADOS DO ESTUDO CORRELACIONAL PREVISTO

Compreendemos que o trabalho de recolha de dados suporia mais disponibilidade do que a planeada e já não nos foi possível concretizar a observação da amostra prevista no plano metodológico, para saber se 'O Selo de Usabilidade e Acessibilidade pode, ou não, contribuir para uma configuração mais robusta na salvaguarda da privacidade digital do utilizador?' (Q5). Por esta razão não dispomos de dados da amostra a apresentar, nem de resultados da análise estatística.

Em todo o caso, acreditamos que não haveria resultados dececionantes, pois qualquer que fosse o resultado da análise, desde que válida, permitiria concluir algo acerca da convergência ou discordância destas duas contendas (privacidade e acessibilidade) que podem, ou não, estar relacionadas.

3.2.2 PERCEÇÕES COMPLEMENTARES: OPÇÕES DE NAVEGAÇÃO E APROFUNDAMENTO DA USABILIDADE NA PRIVACIDADE DIGITAL

Durante a fase em que procurámos saber sobre a existência de algum projeto que permitisse analisar políticas de privacidade em português, dialogámos com vários profissionais encarregues de projetar *sites* e que estão familiarizados com o Selo de Usabilidade e Acessibilidade. Estes especialistas exprimiram, sucintamente, duas dificuldades diferentes que conduzem a uma oportunidade comum.

A primeira relaciona-se com a limitação de opções criativas no desenho de *sites* para responder às questões de acessibilidade, o que aparenta implicar uma diminuição do potencial da experiência da navegação. Os *sites* construídos totalmente em linguagem *HTML* e *PHP*, como os *blogues*, tendem a ser mais acessíveis porque usam tecnologias que são amplamente suportadas por ferramentas de acessibilidade. Já os *sites* feitos em *Java* ou *Flash* podem excluir os leitores de ecrã e navegadores de texto e não serem compatíveis em muitos dispositivos móveis. Também a implementação de um *design* inclusivo pode exigir a simplificação de efeitos visuais, por diminuir a gama de opções nos contrastes de cores adequados, bem como por obrigar a uma navegação por teclado ou à existência de descrições textuais nas imagens.

A segunda dificuldade liga-se ao esforço em corresponder à proteção legal de dados sem comprometer a usabilidade, dando como exemplo concreto a obrigação de navegar em demasiadas opções por imposição legal do RGPD. Talvez a usabilidade relacionada com a privacidade digital ainda esteja numa fase de articulação inicial, o que indicia a necessidade de mais investigação sobre a privacidade digital na ótica da usabilidade.

Uma possibilidade para a resolução destas sensações de conflito pode, porventura, ser a coexistência de alternativas de navegação mais evidentes. A área da acessibilidade digital já contempla alguns modelos que traçam pistas neste sentido: a Comissão Europeia publica frequentemente documentos oficiais em versões de fácil leitura, projetados para serem compreendidos por pessoas com dificuldades intelectuais[4] .

3.2.3 VISUALIZAÇÃO DE «CORPOS DE PRIVACIDADE DIGITAL» E DIREÇÕES FUTURAS PARA PESQUISA

A diversidade na caracterização da privacidade digital dos *sites* sugere que alguns riscos podem ser identificados e mitigados. Por exemplo, um *site* que cubra completamente o atributo de Recolha não é necessariamente crítico se a Partilha for mínima e combinada com um atributo de Segurança robusto. Da mesma forma, um *site* que apresenta uma cobertura completa do atributo Funcionalidade, mas sem Recolha, pode ser percebido como respeitador da privacidade digital. No entanto, se a Funcio-

4 Veja-se a versão de leitura fácil «Uma estratégia para as pessoas com deficiência 2021-2030» https://ec.europa.eu/social/main.jsp?catId=1535&langId=pt

nalidade estiver comprometida e associada à Partilha, isso pode levantar suspeitas sobre a prioridade dada à privacidade por defeito. Além disso, no atributo Recolha, a justificação para a recolha de dados com o objetivo de melhorar a funcionalidade do serviço, embora possa garantir cobertura do atributo Controlo, pode não permitir ao utilizador interferir na dinâmica global da utilização de dados sobre o comportamento dos internautas, e que acaba por afetar a privacidade do utilizador.[5]

A este respeito podemos deixar outros exemplos reveladores das nuances que poderão definir tipologias específicas de «corpos de privacidade digital». Numa impressão recolhida já numa fase posterior aos testes, reparámos que a Imprensa Nacional Casa da Moeda. (INCM) é bastante criteriosa nas políticas de privacidade que apresenta no seu *site*, bem como da loja *online*. A INCM faz parte do consórcio de Certificação de Maturidade Digital abordado anteriormente, destinado a qualquer organização, pública ou privada, que deseje certificar-se nas dimensões mais relevantes para o seu negócio, incluindo Sustentabilidade, Cibersegurança, Privacidade e Proteção de Dados, e Acessibilidade. É notório que a INCM demonstra um compromisso com a acessibilidade; tem, aliás, uma declaração plenamente conforme e, curiosamente, o *site* do Museu da Casa da Moeda junta na mesma página os temas da acessibilidade e da privacidade. No entanto, a informação sobre a privacidade é limitada, afirmando-se que a informação recolhida sobre os visitantes não é pessoal, e apresenta avisos mais voltados para a segurança da informação do que para a privacidade. Vemos que o cuidado com a questão da acessibilidade existe sim, embora a arrumação conjunta possa ser resultado de uma mera coincidência de conveniência na arrumação do «espaço» do *site*[6].

No seguimento desta constatação, interrogamo-nos acerca de quais as tipologias de cenários que podem ser extrapoladas como «corpos de privacidade digital», dadas tão variadas possibilidades. Este raciocínio sugere algumas consequências. Uma, é a de que podem existir ameaças não previstas no instrumento de análise PI1 e, portanto, não identificadas. Concretamente, que periculosidade poderia ser detetada num simplismo como os corpos de privacidade deliberados pela INCM, por exemplo?

Outra consequência é que a noção de corpos de privacidade digital é um apuramento desta investigação que conduz a uma ideia alternativa à das visualizações de privacidade elencadas no capítulo anterior, na medida em que permitem uma proposta de configuração visual diferente e não tão hermética quanto as classificações e pontuações de privacidade, as certificações ou selos de privacidade, os painéis de privacidade, as opções de privacidade (apresentadas em *banners* e *pop-ups* de consentimento, principalmente relacionadas com a gestão de *cookies*) ou os ícones de privacidade.

Imaginamos que PI1, devidamente refinado e finalizado, possa ser uma ferramenta configurada enquanto plataforma própria, na qual as entidades submetem as respostas do inquérito e através desses dados se desencadeia uma visualização de privacidade, como se fossem organismos vivos. Sugerimos uma representação de aspeto tentacular e concentrada num único círculo por entidade, cuja forma específica seria definida pela variação dos argumentos apresentada em cada tentáculo (cada um correspondente a um atributo). A plataforma poderia mostrar as diversas formas nela submetidas, de modo a disponibilizar os padrões a qualquer pessoa interessada (sem ter de recorrer ao tratamento de dados). Por sua vez as entidades talvez pudessem optar entre divulgar a identidade da organização ou

5 Daí que, disponibilizar a navegação através de abordagens mais claras, proporcionando por defeito a salvaguarda de uma navegação verdadeiramente privada a utilizadores que não estão motivados para decidir sobre as questões de privacidade digital, talvez fosse uma solução mais coerente. Simultaneamente, permitiria aos outros utilizadores usufruir de experiências de navegação estimulantes e pormenorizadas, em sintonia com a protagonização atual da intervenção dos dados resultantes das interações na Internet na economia global.

6 Da nossa parte reforçamos que a origem principal da abordagem por nós proposta, de cruzar a observação da privacidade com a da acessibilidade digital, se relaciona, sobretudo, com a possibilidade de aproveitamento de recursos, sensibilidades e esforços.

mantê-la oculta (encriptada). Explorada a hipótese até este ponto, deixamos por agora a possibilidade de concretizar experimentalmente semelhante abordagem - a qual acabou por se verificar inexequível nos limites do tempo estabelecidos para a presente dissertação - remetendo-a para uma eventual futura direção de pesquisa, dedicada a apurar o modo de visualização de um balanço sobre a aplicação de privacidade *online*.

Apesar de tudo, defendemos que o ponto a que chegámos na exploração da ferramenta PI1 é consistente com um outro resultado, que nos parece relevante, quer por ser inédito dentro da problemática investigada, quer por lhe acrescentar valor, pelo que o considerámos como um segundo Produto de Investigação (PI2), e passamos de seguida a expor.

3.2.4 ADEQUAÇÃO DE PI1 A PI2

Havíamos depreendido das questões suscitadas pelo enquadramento teórico que, se as motivações dos agentes responsáveis e implicados no desenvolvimento dos sistemas de informação estiverem alinhadas com as necessidades dos utilizadores, à partida, os padrões definidos para os produtos digitais podem priorizar a privacidade do utilizador por defeito, independentemente da intervenção posterior do utilizador, o que é corroborado pelo princípio 4 das diretrizes *privacy by design*: «Assegurar um funcionamento pleno com base no «todos ganham», acomodando todos os objetivos legítimos de *design* do sistema»[7].

Ao mesmo tempo, uma das pistas deixada nos testes ensaiados em PI1 sugere que a solução para o impasse do paradoxo da privacidade possa ser a sensibilização para o tema da privacidade digital junto das pessoas que compõem as organizações, revelando-as como o potencial público-alvo de PI1. Visto que, uma vez compreendendo melhor o alcance das questões de privacidade colocadas, estes profissionais poderão chamar a si a responsabilidade de melhor configurar os parâmetros das políticas de privacidade durante os processos decisórios da construção ou de manutenção de um *site*.

Durante o processo de investigação para esta dissertação, reconheceu-se uma experiência representativa de conduta comum entre muitos utilizadores da *Internet*: raramente se altera a atitude face ao consentimento na interação com os *cookies*, limitando-se, frequentemente, a uma leitura superficial destes avisos. Não foi realizado nenhum levantamento sistemático passível de corroboração científica para apurar a veracidade desta afirmação, mas é uma perceção a que facilmente se chegou durante a auscultação aleatória feita: poucos são os utilizadores que desativam consistentemente os *cookies* e, apenas os detentores de maior grau de literacia em engenharia da privacidade manobram uma experiência anónima capaz de usufruir livremente da *Internet*, através de serviços de ligação à *Internet* encriptados (VPNs) e programas ou extensões de navegador que bloqueiam os anúncios e impedem que empresas de publicidade descubram o comportamento *online* dos utilizadores.

Os bloqueadores de anúncios são extensões de navegador ou programas que evitam a apresentação de publicidade, filtrando o conteúdo das páginas *web* e bloqueando elementos identificados como anúncios. Funcionam através de listas de filtros que contêm regras específicas para identificar e bloquear publicidade intrusiva. Não é possível aos demais internautas terem uma experiência de navegação realmente privada enquanto estiverem dependentes da otimização comercial das informações pessoalmente identificáveis, ou mesmo das inferências obtidas por agregação de dados.

Considerar a implementação de práticas que salvaguardam *a priori* a proteção da privacidade do utilizador, independentemente da sua intervenção posterior, pode desempenhar um papel crucial na alteração do modelo da *Internet* que leva já anos de uso, conjuntamente com a melhoria da experiência do utilizador e a proteção da sua privacidade. Sublinhamos que essa mudança poderia mitigar alguns dos problemas trazidos pela atual dinâmica de rentabilização de grandes volumes de dados,

7 Cavoukian. 2009.

mencionada no capítulo anterior. No fundo, trata-se de «olhar para trás» na abordagem praticada e alterar os processos decisórios que resultam em transições tecnológicas, transformação essa que é também civilizacional.

Daí que nos tenhamos concentrado em procurar aproveitar o material produzido em PI1, como contributo para uma consciencialização que possa conduzir a diferentes escolhas sobre o consentimento nas experiências de navegação, junto dos profissionais envolvidos nas decisões da construção de *sites* ou interfaces. Destacando a importância de fornecer recursos e materiais educativos que possam capacitar estes agentes de mudança produtores de tecnologia, a enveredar por escolhas mais informadas sobre a privacidade dos utilizadores na construção de produtos digitais. Portanto, a compilação de informações exaustivas sobre práticas de privacidade na *Internet*, tal como realizada nesta dissertação, pode revelar-se útil como atalho, embora de leitura longa, para informar e facilitar decisões mais conscientes no *design* de *interfaces* digitais. O que nos conduziu à elaboração de uma tabela de consulta que permita melhorar a literacia sobre a privacidade digital: o Produto da investigação 2 (PI2), consultável no anexo C 'Tabela de consulta para diagnóstico das práticas de privacidade *online*'.

Em teoria, a missão de promover a literacia sobre a privacidade digital pode ser incluída nas responsabilidades dos EPD ao serviço de autoridades e organismos públicos. Estes são legalmente obrigados a nomear um EPD, que pode então desempenhar um papel na sensibilização da organização. Contudo, a viabilidade dessa tarefa pode variar significativamente de acordo com a dimensão e as prioridades das diferentes entidades. Em grandes organizações, onde o controle do cumprimento das normas do RGPD é a competência central do EPD, a sensibilização pode ser uma responsabilidade secundária. Por outro lado, entidades fora do setor público, que não têm a obrigação de nomear um EPD, ainda precisam de se posicionar de maneira clara quanto à forma de recolher, utilizar, armazenar e partilhar dados ou informações pessoalmente identificáveis, esclarecendo os utilizadores sobre os seus direitos de privacidade. Deste modo, embora aceitemos que os EPD constituiriam excelentes observadores-utilizadores de PI1, procurámos satisfazer perfis menos especializados, dada a ampla aplicabilidade da ferramenta.

Desta consideração decorreu um alargamento no mapa esquemático desta investigação, correspondente a uma outra fase que é expressa na seguinte pergunta: 'Conseguimos elaborar uma ferramenta de diagnóstico da privacidade *online* que não exija uma sobrecarga na qualificação dos agentes que a queiram verificar?' (Q6).

É importante familiarizarmo-nos com a linguagem da privacidade digital e reforçar o sentido de responsabilidade de quem elabora o panorama digital. No presente trabalho debruçamo-nos sobre os produtos digitais específicos dos *sites*, mas o exercício de reflexão proporcionado por PI1 e PI2 pode ser estendido e empregue noutras aplicações digitais. Porque a definição do modo de participação, no que diz respeito à privacidade é abrangente e relevante para o resultado final atual, que tem agravado alguns assuntos controversos conforme abordados no início do capítulo anterior. É positivo que as pessoas conversem sobre os conteúdos de PI2, porque essa discussão molda os comportamentos das organizações espelhados nas práticas de privacidade do ecossistema digital.

O capítulo que se segue reúne o desfecho desta investigação.

CAPÍTULO 4

CONCLUSÃO

Percorridas as etapas anteriores da dissertação sobre a privacidade digital e a sua salvaguarda no ecossistema digital contemporâneo, passemos agora, para concluir, a uma síntese crítica dos resultados obtidos ao longo desta investigação. Neste capítulo revisitamos as principais descobertas, apresentamos as suas implicações à luz da literatura existente e consideramos as limitações encontradas, bem como as perspetivas futuras que este estudo pode abrir. No percurso da investigação explorámos o desenvolvimento do instrumento PI1, que culminou na criação da tabela PI2, e ambos proporcionam aprendizagens sobre os desafios e oportunidades na proteção da privacidade *online*, particularmente aplicável no contexto da Administração Pública portuguesa.

Sumário dos resultados

Em relação à questão: 'A privacidade individual é adequadamente salvaguardada no ecossistema digital?' (Q1), foi possível apurar que existe um certo equilíbrio entre a inovação tecnológica e a proteção da privacidade individual, através de medidas que visam criar um ambiente digital mais transparente e seguro para os utilizadores, nomeadamente o Regulamento Geral de Proteção de Dados da União Europeia que representa uma transformação decisiva na legislação de privacidade digital, conferindo aos cidadãos maior controlo sobre os seus dados pessoais *online* e impondo responsabilidades rigorosas às entidades que os processam, exigindo às organizações que demonstrem ativamente essa conformidade de forma clara e acessível, geralmente através de políticas de privacidade nos *sites* e serviços *online*.

Em relação à questão: 'As políticas de privacidade e outros mecanismos em vigor demonstram conformidade com uma abordagem centrada no utilizador para a proteção da privacidade?' (Q2A), foi possível apurar que apesar da importância das políticas de privacidade para a confiança do utilizador, estas são frequentemente difíceis de compreender ou até negligenciadas, fenómeno conhecido como o «paradoxo da privacidade». Algumas pesquisas consultadas têm examinado a usabilidade e conformidade legal destas políticas, identificando algumas dificuldades de uso que limitam a sua eficácia. No conjunto, estes aspetos sugerem que apesar dos esforços para desenvolver políticas centradas no utilizador, persistem desafios significativos na implementação efetiva desta abordagem, fornecendo assim um contexto rico de explorar.

Em relação à questão: 'De que maneiras podemos observar e avaliar a conformidade das políticas de privacidade com uma abordagem centrada no utilizador?' (Q2B), foi possível apurar que já existem alguns mecanismos que facilitam a compreensão e gestão das opções de privacidade pelos utilizadores. Podem ser formas de visualização ou de comunicação das políticas de privacidade, como painéis de controlo, certificações, rótulos, *banners*, *pop-ups* e ícones de privacidade, que por serem claros e acessíveis, podem funcionar como indicadores tangíveis da eficácia das políticas de privacidade, e desse modo, da conformidade com uma abordagem centrada no utilizador.

Adicionalmente, a «Lista Unificada de Atributos de Privacidade» (LUAP) resultante do trabalho de Barth, Ionita e Hartel no estudo intitulado «Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines» (2022), oferece um quadro robusto para observar

e avaliar se as políticas de privacidade estão alinhadas com os princípios de uma abordagem centrada no utilizador, conforme estipulado pelo RGPD e pelas diretrizes *privacy by design*.

Em relação à questão: 'Como podemos verificar a conformidade com a proteção da privacidade centrada no utilizador, na realidade portuguesa?' (Q2C), foi possível identificar na Administração Pública portuguesa o setor-chave a examinar para o contexto português, devido ao seu compromisso com a prestação de serviços centrados no cidadão.

Explorámos o Selo de Maturidade Digital que visa certificar a maturidade digital das organizações em várias dimensões, incluindo a da privacidade. Contudo, a investigação revelou que a operacionalização da dimensão de privacidade ainda se encontra incompleta, com critérios de avaliação pouco claros e com um processo de certificação que carece de transparência. Esta barreira indicou que, apesar do potencial do Selo para o efeito pretendido, não se mostra de momento como uma ferramenta útil para avaliar a conformidade com os princípios de privacidade centrados no utilizador.

Em contraste, o Selo de Usabilidade e Acessibilidade (SUA) que comprova melhorias na experiência do utilizador em termos de acessibilidade apresenta uma metodologia articulada e com ênfase na participação da comunidade, interessante para ser adaptada à avaliação da privacidade *online*.

Em relação à questão: 'A conformidade para a proteção da privacidade está dependente da intervenção do utilizador ou os agentes responsáveis pelo desenvolvimento dos sistemas de informação salvaguardam *a priori* a proteção da privacidade, independentemente da intervenção do utilizador?' (Q3), não se encontraram respostas evidentes para esta questão nas leituras realizadas. É provável que a conformidade para a proteção da privacidade nas tecnologias digitais seja mais dependente dos intervenientes que concebem originalmente os seus parâmetros, tendo, nesse caso, o utilizador um peso menor; embora continue a ser relevante a forma como o utilizador acede aos serviços *online* e permite a transformação do comportamento humano em dados digitais.

Em relação à questão: 'É possível realizar um diagnóstico da privacidade *online*, de modo semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4A), entendemos que a viabilidade em replicar o modelo mencionado pressupõe o recurso a uma ferramenta de análise automática e outro de análise manual.

Em relação à questão: 'Qual seria a ferramenta automática mais adequada para o efeito de diagnóstico da privacidade *online*, de forma semelhante à metodologia apresentada no Selo de Usabilidade e Acessibilidade?' (Q4B), foi possível apurar que não existe nenhuma ferramenta particularmente eficaz para o efeito pretendido, apesar de terem sido testados alguns métodos. A insatisfação quanto às ferramentas existentes prende-se, sobretudo, com a barreira da língua, pois estão quase todas direcionadas para o inglês, o que adiciona um risco de enviesamento pela tradução; e prende-se ainda, com a simplificação da avaliação, uma vez que as classificações resultantes permitem informar rapidamente os utilizadores, mas não apresentam análises tão detalhadas quanto os indicadores da LUAP. Mesmo o sistema de classificação Privacy Rating, que foi desenvolvido a partir do estudo que criou a lista, acabou por eliminar alguns critérios de avaliação, omitindo aspetos importantes da privacidade.

Em relação à questão: 'Qual seria a ferramenta manual mais adequada para o efeito de diagnóstico da privacidade *online*, de forma semelhante à metodologia apresentada no SUA?' (Q4C), foi possível apurar que o método de auditoria realizada por especialistas e Encarregados de Proteção de Dados

pode apresentar metodologias de avaliação da privacidade *online*, mas estas não se encontram amplamente disponíveis como no método de avaliação que o SUA propõe.

Como resposta a tal necessidade elaborámos os instrumentos PI1 e PI2. Inicialmente, o PI1 foi desenvolvido quer como ferramenta de diagnóstico da privacidade dos *sites*, quer como instrumento de recolha de dados para análise, mas a sua complexidade e as dificuldades encontradas durante os testes evidenciaram a necessidade de melhorias. Como solução para as limitações encontradas, reuniu-se em PI2 o conteúdo de PI1, dirigido a profissionais envolvidos no desenvolvimento de *sites*, com o objetivo de permitir a avaliação sistemática da conformidade das políticas de privacidade aplicadas nas organizações. Simultaneamente, com o recurso a PI2, ao melhor compreenderem o alcance das questões de privacidade colocadas, estes profissionais terão aumentando a sua literacia sobre privacidade digital e poderão ser capazes de promover melhores práticas na proteção da privacidade *online*.

Em relação à questão: 'O Selo de Usabilidade e Acessibilidade pode, ou não, contribuir para uma configuração mais robusta na salvaguarda da privacidade digital do utilizador?' (Q5), não foi possível apurar uma resposta com base no estudo realizado, uma vez que não se chegaram aos resultados esperados para o instrumento PI1 e não houve lugar a análise quantitativa.

Em relação à questão: 'Conseguimos elaborar uma ferramenta de diagnóstico da privacidade *online* que não exija uma sobrecarga na qualificação dos agentes que a queiram verificar?' (Q6), estabelecemos que PI2 corresponde a uma proposta de instrumento com esse intuito.

Discussão dos resultados

No contexto digital português, a Administração Pública apresenta-se como um terreno fértil para a aplicação de práticas que privilegiem a proteção da privacidade do utilizador. A plataforma Mosaico, «modelo comum de Portugal», oferece um conjunto de princípios que, se bem implementados, podem garantir a transparência e a segurança dos serviços públicos digitais. No entanto, ainda há um caminho a percorrer na aplicação prática, no que toca à privacidade digital.

O SUA insere-se numa prática que visa salvaguardar um direito. Se a tomada de consciência sobre direitos humanos for sedimentada, é natural que se verifiquem mais frequentemente padrões que priorizem também a privacidade do utilizador. Acreditamos que a aplicação de um modelo sistemático de avaliação, como o proposto pelo SUA, poderia beneficiar significativamente a proteção da privacidade *online*.

Com o intuito de aumentar a aplicabilidade da ferramenta PI1 e por termos compreendido que a sensibilização para o tema da privacidade digital junto das pessoas que compõem as organizações pode ser uma solução para ultrapassar o paradoxo da privacidade, conforme apurado em pistas deixadas nos testes ensaiados a PI1, procurámos satisfazer perfis menos especializados do que os EPD, apesar de admitirmos que estes constituiriam excelentes observadores-utilizadores de PI1.

Deduzimos das questões resultantes do quadro teórico que, se as motivações dos participantes no desenvolvimento dos sistemas de informação estiverem em sintonia com as necessidades dos utilizadores, os padrões estabelecidos para os produtos digitais poderão dar prioridade à privacidade por defeito do utilizador, independentemente da ação posterior deste.

Implementar práticas que protejam a privacidade do utilizador desde o início, sem depender de ações posteriores, pode ser fundamental para mudar o modelo da *Internet* que já está em uso há anos. Isso também melhora a experiência do utilizador e protege a sua privacidade. Destacamos que essa mudança pode ajudar a resolver alguns dos problemas trazidos pelo recurso intensivo a enormes conjuntos de dados digitais, conforme mencionados no segundo capítulo. Em essência, trata-se de rever a

abordagem atual e modificar os processos de decisão que levam a transições tecnológicas, uma transformação que também é civilizacional, como sublinhámos.

Limites do trabalho e melhorias

O trabalho de investigação realizado permitiu apurar que apesar dos avanços significativos na proteção da privacidade digital ainda existem barreiras consideráveis à implementação efetiva dessas políticas. Por isso foi projetado o instrumento PI1, com o objetivo de permitir uma análise objetiva e sistemática da avaliação da conformidade das práticas de privacidade.

Reconhecemos a limitação evidente de PI1 em relação aos resultados esperados dada a ausência de análise pela falta de dados. Conforme explicado no capítulo anterior, a recolha de dados exigiria uma disponibilidade maior do que a inicialmente planeada, o que impossibilitou a observação da amostra prevista no plano metodológico.

A utilização de PI1 revelou-se cansativa para o utilizador e apresentou dificuldades na identificação e classificação de algumas informações, além de nem sempre refletir uma prática real de navegação. A fim de resolver este obstáculo numa próxima fase da investigação é imprescindível garantir que haja mais tempo ou pessoas disponíveis para a recolha de dados. Isto tanto pode incluir a alocação de mais horas para o investigador, como criar parcerias com outras entidades que possam partilhar recursos humanos para as observações ou ainda equacionar a contratação de assistentes de pesquisa. Numa fase de melhoria do instrumento de análise PI1 é aconselhável conduzir testes de usabilidade para avaliar a ordem de apresentação dos atributos, no sentido de encontrar a solução mais frequente e eficiente. Todavia, a ordem elegida refletirá sempre uma decisão editorial que indica as prioridades estabelecidas, particularmente no que diz respeito ao período ótimo de atenção do observador. Seria importante, também, estabelecer um sistema de respostas contínuo durante a fase de recolha de dados para identificar e corrigir problemas rapidamente, evitando que se acumulem e comprometam os resultados. Adicionalmente, colaborar com outras entidades que pudessem contribuir com ajustes ao plano metodológico para torná-lo mais flexível e adaptável às condições reais de recolha de dados pode conferir maior sucesso à ferramenta. No conjunto, estas sugestões podem, além de melhorar a eficiência da ferramenta PI1, permitir ampliar a amostra para análise.

Por outro lado, a escolha da plataforma Airtable para a construção do formulário não encerra uma possibilidade vinculativa: poderão existir outras opções mais adequadas para estruturação da ferramenta, nomeadamente pela sua extensão de variáveis de observação, e para a extração dos dados para a análise. Toda a informação necessária a réplicas deste modelo de observação fica disponibilizada com este trabalho, pelo que é transferível a sua aplicação para outros *softwares* ou plataformas de bases de dados.

Deixamos adiante outras sugestões de trabalho após o aprimoramento do instrumento PI1 nas 'Recomendações e propostas para trabalho futuro '. Lembramos que os conteúdos de PI1 foram transferidos para PI2 e que algumas das recomendações de melhorias deste segundo produto são comuns ao primeiro.

Como discutido ao longo do trabalho, a conformidade com as políticas de privacidade não depende apenas da aplicação de normas legais, mas também da capacidade das organizações para integrarem os seus princípios fundadores nas atividades profissionais. O PI2 reuniu numa tabela os conteúdos da análise sistemática de práticas de privacidade *online* de PI1, a fim de que este sistema de conceitos seja partilhado com os agentes envolvidos no processo de definição de privacidade digital. Supomos que seja um material útil, mas desconhecemos o seu real contributo, uma vez que nenhum estudo ou entrevista exploratória foram realizados para o apurar.

Como melhoria de PI2 recomendamos que se proporcione uma participação interdisciplinar, envolvendo especialistas de diferentes áreas (jurídica, tecnológica, de gestão, *designers*) na sua revisão e melhoria, pois poderá conferir-lhe uma abordagem holística relevante.

Para colocar em andamento o objetivo pretendido para PI2 é importante encontrar um local adequado para a divulgação deste, de forma a facilitar o seu acesso e a sua utilização, pelos agentes implicados na manutenção ou construção de *sites*. Para esse efeito, sugerem-se algumas soluções: a criação de uma plataforma *online* que disponibilize PI2, ou a integração do PI2 em portais já existentes, como o Mosaico; a organização de sessões de formação para os utilizadores-observadores de PI2, garantindo que compreendem plenamente a aplicação de PI2; e a manutenção do PI2 atualizado com mudanças nas políticas de privacidade digital e desenvolvimentos tecnológicos marcantes, assegurando a relevância contínua de PI2.

Recomendações e propostas para trabalho futuro

A investigação realizada não obteve esclarecimentos óbvios sobre a relação entre a adequação para a proteção da privacidade e a intervenção do utilizador (questão Q3), mas sugere que esta relação dependa mais dos responsáveis que definem os parâmetros iniciais. Uma possível direção de pesquisa sobre o tema da privacidade digital pode ser a aferição do grau de interferência do utilizador e o seu impacto possível, nomeadamente em contextos de resistência ou oposição ao negócio da previsibilidade a partir da informação digital. Um olhar sobre os movimentos contracorrente dentro desta matéria pode originar conhecimento pertinente.

Consideramos conveniente a criação de uma ferramenta em língua portuguesa que automatize a avaliação das posições das entidades em termos de privacidade digital (questão Q4B). Esta ferramenta deverá gerar diagnósticos preliminares sobre o tema e permitir acesso ao processo de análise. Para esta finalidade pode contribuir a participação de organizações relevantes na matéria, convidadas a integrar a operação de melhoria do método de recolha de dados de PI1, conforme anteriormente aconselhado.

Recomendamos que se investiguem, e integrem em PI1, formas de mapeamento e representação visual dos dados nele submetidos, que permitam uma consideração tão ampla da privacidade quanto as suas características apuradas. Ou seja, o modo de visualização de «corpos de privacidade», por nós sugerido com a forma «tentacular», é uma ideia alternativa à tendência de simplificação observada nas representações de privacidade. A visualização gráfica de informação constitui uma disciplina própria dentro do universo da ciência de dados que tem vindo a ganhar terreno, pois é útil para explorar e comunicar mensagens complexas[8]. No entanto a possibilidade de visualizações cada vez mais convincentes e que aumentam o poder persuasivo dos números contabilísticos acarreta o risco de limitar o discernimento dos decisores ao serem encarados como verdades únicas, quando são apenas possibilidades analíticas[9].

Além destas sugestões, pensamos também que é oportuno desenvolver alguma investigação a propósito do efeito da literacia sobre privacidade digital. A condução de pesquisas para avaliar a eficácia do PI2 na conscientização sobre privacidade digital entre os trabalhadores envolvidos no desenvolvimento de *sites* e aplicações móveis, e do impacto que o aumento da literacia teve nas suas escolhas e ações, é uma proposta para trabalho futuro.

Considerações Finais

Em conclusão, consideramos que este estudo contribui significativamente para o campo da privacidade digital, disponibilizando não apenas uma análise crítica das práticas atuais, mas também ferra-

8 Alberto Cairo. 2019. *How Charts Lie: Getting Smarter about Visual Information.*

9 Paolo Quattrone. 2016. «Management accounting goes digital: Will the move make it wiser?».

mentas concretas para a sua avaliação e melhoria. O PI1 e o PI2, embora enfrentem complexidade na sua implementação, representam passos importantes na direção de uma abordagem mais sistemática e centrada no utilizador para a proteção da privacidade *online*. As limitações encontradas, longe de diminuírem o valor deste trabalho, abrem caminhos para futuras investigações e aperfeiçoamentos.

À medida que avançamos numa era cada vez mais digital, a importância de salvaguardar a privacidade individual torna-se ainda mais premente. Este estudo serve como um lembrete da necessidade contínua de acompanhamento, inovação e adaptação das abordagens à privacidade digital. Esperamos que as ferramentas e contributos aqui apresentados inspirem futuros investigadores e profissionais a continuar este trabalho, contribuindo para um ecossistema digital mais seguro, transparente e respeitador dos direitos individuais.

REFERÊNCIAS BIBLIOGRÁFICAS

45 Graus, 2024. #158 António Tavares - Além da Política: devíamos pensar mais a Administração Pública? https://www.youtube.com/watch?v=czWFsfyqytw.

Aceto, Giuseppe, Valerio Persico, e Antonio Pescapé. 2019. «A Survey on Information and Communication Technologies for Industry 4.0: State-of-the-Art, Taxonomies, Perspectives, and Challenges». IEEE Communications Surveys & Tutorials 21 (4): 3467–3501. https://doi.org/10.1109/COMST.2019.2938259.

Aho, Brett, e Roberta Duffield. 2020. «Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China». Economy and Society 49 (maio):1–26. https://doi.org/10.1080/03085147.2019.1690275.

AMA-Agência para a Modernização Administrativa. 2023. «Princípios». 24 de novembro de 2023. https://www.mosaico.gov.pt/principios.

AMA-Agência para a Modernização Administrativa. 2024. «Modelo de conformidade do Mosaico». 30 de agosto de 2024. https://www.mosaico.gov.pt/ferramentas/modelo-de-conformidade.

AMA-Agência para a Modernização Administrativa. 2021. «Observatório Português da Acessibilidade Web». 30 de agosto de 2024. https://observatorio.acessibilidade.gov.pt/directories.

Andrade, Vinícius Camargo, Rhodrigo Deda Gomes, Sheila Reinehr, Cinthia Obladen De Almendra Freitas, e Andreia Malucelli. 2022. «Privacy by Design and Software Engineering: A Systematic Literature Review». Proceedings of the XXI Brazilian Symposium on Software Quality, novembro, 1–10. https://doi.org/10.1145/3571473.3571480.

Barreto, Helena Martins do Rêgo. 2024. «Desinformação em meio à crise do capitalismo e à configuração de uma nova estrutura de mediação social». Revista Eco-Pós 27 (1): 330–52. https://doi.org/10.29146/eco-ps.v27i1.28045.

Barth, Susanne, D. Ionita, Menno De Jong, Pieter Hartel, e Marianne Junger. 2021. «Privacy Rating: A User-Centered Approach for Visualizing Data Handling Practices of Online Services». IEEE Transactions on Professional Communication PP (novembro):1–20. https://doi.org/10.1109/TPC.2021.3110617.

Barth, Susanne, Dan Ionita, e Pieter Hartel. 2022. «Understanding Online Privacy—A Systematic Review of Privacy Visualizations and Privacy by Design Guidelines». ACM Computing Surveys 55 (3): 63:1-63:37. https://doi.org/10.1145/3502288.

Becher, Stefan, Armin Gerl, e Bianca Meier. 2020. «Don‘t Forget the User: From User Preferences to Personal Privacy Policies». Em 2020 10th International Conference on Advanced Computer Information Technologies (ACIT), 774–78. https://doi.org/10.1109/ACIT49673.2020.9208810.

Bruin, Ruben de. 2022. «A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence». SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.4251540.

Buchinskaia, Olga. 2022. «The Threefold Divergence of Socio-Economic Development in the Digital Age». Ideas and Ideals 14 (junho):239–60. https://doi.org/10.17212/2075-0862-2022-14.2.2-239-260.

Cairo, Alberto. 2019. *How Charts Lie: Getting Smarter about Visual Information*. New York; WW Norton & Company.

Campenhoudt, Luc Van, Jacques Marquet e Raymond Quivy. 2019. *Manual de Investigação em Ciências Sociais*. Lisboa; Gradiva.

Canaan, Renan Gadoni. 2022. «Estímulo à inovação através de regulamentações para a proteção de dados pessoais: o impacto da replicação da GDPR na LGPD». Blucher Engineering Proceedings, maio, 1117–33. https://doi.org/10.5151/vi-enei-836.

Carrillo, Arturo J., e Matías Jackson. 2022. «Follow the Leader? A Comparative Law Study of the EU's General Data Protection Regulation's Impact in Latin America». ICL Journal 16 (2): 177–262. https://doi.org/10.1515/icl-2021-0037.

Castells, Manuel. 2007. *A Era da Informação: Economia, Sociedade e Cultura*. Traduzido por Rita Espanha. Lisboa ; Fundação Calouste Gulbenkian. Vol. I. Fundação Calouste Gulbenkian. Serviço de Educação e Bolsas.

Cavoukian, Ann. 2009. «Privacy by design: The 7 foundational principles.» Information and privacy commissioner of Ontario.

Cavoukian, Ann, e Michelle Chibba. 2018. «Start with Privacy by Design in All Big Data Applications». Em Guide to Big Data Applications, editado por S. Srinivasan, 29–48. Studies in Big Data. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-53817-4_2.

Cavoukian, Ann, Scott Taylor, e Martin E. Abrams. 2010. «Privacy by Design: Essential for Organizational Accountability and Strong Business Practices». Identity in the Information Society 3 (2): 405–13. https://doi.org/10.1007/s12394-010-0053-z.

Conselho da Europa. 2021. «Convenção para a Proteção das Pessoas quanto ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108+)». https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2.

Couldry, Nick, e Ulises A. Mejias. 2019. «Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject». Television & New Media 20 (4): 336–49. https://doi.org/10.1177/1527476418796632.

Eggl, Barbara. 2019. «Learning to Walk a Tightrope: Challenges DPOs Face in the Day-to-Day Exercise of Their Responsibilities». Journal of Data Protection & Privacy, julho. https://hstalks.com/article/5172/learning-to-walk-a-tightrope-challenges-dpos-face-/.

Eichenberger, Hernandez Vivan. 2020. «Resenha de "Big Tech: A Ascensão Dos Dados e a Morte Da Política" de Evgeny Morozov». Crítica Marxista, janeiro. https://www.academia.edu/45155409/Resenha_de_Big_Tech_a_ascens%C3%A3o_dos_dados_e_a_morte_da_pol%C3%ADtica_de_Evgeny_Morozov.

ePortugal (portal). 2019. «Foi lançado o Kit do Selo de Usabilidade e Acessibilidade». 12 de junho de 2019. https://eportugal.gov.pt/noticias/foi-lancado-o-kit-do-selo-de-usabilidade-e-acessibilidade.

European Data Protection Supervisor. 2024. «Data Protection Officer (DPO)». 12 de setembro de 2024. https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en.

Fabian, Benjamin, Tatiana Ermakova, e Tino Lentz. 2017. «Large-scale readability analysis of privacy policies». Em Proceedings of the International Conference on Web Intelligence, 18–25. WI '17. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3106426.3106427.

Faria, Julian Affonso de, e Cláudio Márcio Magalhães. 2021. «O Capitalismo de Vigilância e a Política da Desinformação». Interações: Sociedade e as novas modernidades, n.º 40 (junho), 60–79. https://doi.org/10.31211/interacoes.n40.2021.a3.

Fisher, Carie, Sunghyun R. Kang, e Cyndi Wiley. 2023. «Awareness, Understanding, and Attitudes of Digital Accessibility in Technology Professionals». Em HCI International 2023 Posters, editado por Constantine Stephanidis, Margherita Antona, Stavroula Ntoa, e Gavriel Salvendy, 277–83. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-35992-7_38.

Flaxman, Seth, Sharad Goel, e Justin M. Rao. 2016. «Filter Bubbles, Echo Chambers, and Online News Consumption». Public Opinion Quarterly 80 (S1): 298–320. https://doi.org/10.1093/poq/nfw006.

Fox, Grace, Theo Lynn, e Pierangelo Rosati. 2022. «Enhancing consumer perceptions of privacy and trust: a GDPR label perspective». Information Technology & People 35 (8): 181–204. https://doi.org/10.1108/ITP-09-2021-0706.

Frias, Eliana Sanches de. 2022. «Inteligência artificial, desinformação e populismo digital: Como as plataformas digitais impulsionam os movimentos de extrema direita». Razón y Palabra 25 (112): 12–31. https://doi.org/10.26807/rp.v25i112.1854.

Gellman, Robert. 2022. «Fair Information Practices: A Basic History - Version 2.22». SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.2415020.

Graham, Rosie. 2017. «Google and Advertising: Digital Capitalism in the Context of Post-Fordism, the Reification of Language, and the Rise of Fake News». Palgrave Communications 3 (1): 1–19. https://doi.org/10.1057/s41599-017-0021-4.

Greenleaf, Graham. 2019. «Global Data Privacy Laws 2019: 132 National Laws & Many Bills». SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=3381593.

Habib, Hana, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman

Sadeh, e Florian Schaub. 2021. «Toggles, Dollar Signs, and Triangles: How to (In)Effectively Convey Privacy Choices with Icons and Link Texts». Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, maio, 1–25. https://doi.org/10.1145/3411764.3445387.

Horibe, Masao. 2020. «The Realization of Mutual Adequacy Recognition Between Japan and the EU and Issues Raised in the Process». Global Privacy Law Review 1 (3). https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2020091.pdf.

Instituto Nacional para a Reabilitação. 2020. «Acessibilidade Digital». 29 de julho de 2020. https://www.inr.pt/acessibilidade-digital.

Jacobs, Bart, e Jean Popma. 2019. «Medical Research, Big Data and the Need for Privacy by Design». Big Data & Society 6 (1): 2053951718824352. https://doi.org/10.1177/2053951718824352.

Kallenberge, Ute, e Barbara Eggl. 2019. «Being a Data Protection Officer in the Public Sector: The EU Side of Things». European Data Protection Supervisor. 25 de fevereiro de 2019. https://www.edps.europa.eu/press-publications/publications/podcasts/being-data-protection-officer-public-sector-eu-side-things_en.

Kokolakis, Spyros. 2017. «Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon». Computers & Security 64 (janeiro):122–34. https://doi.org/10.1016/j.cose.2015.07.002.

Kovac, Polonca, e Grega Rudolf. 2022. «Social Aspects of Democratic Safeguards in Privacy Rights: A Qualitative Study of the European Union and China». Central European Public Administration Review 20 (1): 7–32. https://doi.org/10.17573/cepar.2022.1.01.

LABX - Centro para a Inovação no setor Público. 2021. «Guia Metodológico para Serviços Públicos baseados em Direitos Humanos». 7 de dezembro de 2021. https://labx.gov.pt/destaques-posts/guia-metodologico-para-servicos-publicos-baseados-em-direitos-humanos/.

Marozzo, Fabrizio, e Domenico Talia. 2023. «Perspectives on Big Data, Cloud-Based Data Analysis and Machine Learning Systems». Big Data and Cognitive Computing 7 (2): 104. https://doi.org/10.3390/bdcc7020104.

Mayer-Schönberger, Viktor, e Kenneth Cukier. 2013. B*ig Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.

Mhaidli, Abraham, Selin Fidan, An Doan, Gina Herakovic, Mukund Srinath, Lee Matheson, Shomir Wilson, e Florian Schaub. 2023. «Researchers' Experiences in Analyzing Privacy Policies: Challenges and Opportunities». Proceedings on Privacy Enhancing Technologies 2023 (4): 287–305. https://doi.org/10.56553/popets-2023-0111.

Mohamed, Azlinah, Maryam Khanian Najafabadi, Yap Bee Wah, Ezzatul Akmal Kamaru Zaman,

e Ruhaila Maskat. 2020. «The State of the Art and Taxonomy of Big Data Analytics: View from New Big Data Framework». Artificial Intelligence Review 53 (2): 989–1037. https://doi.org/10.1007/s10462-019-09685-9.

Morel, Victor, e Raúl Pardo. 2020. «SoK: Three Facets of Privacy Policies». Em Proceedings of the 19th Workshop on Privacy in the Electronic Society, 41–56. WPES'20. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3411497.3420216.

Mulholland, Caitlin Sampaio. 2018. «Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18)». Revista de Direitos e Garantias Fundamentais 19 (3): 159–80. https://doi.org/10.18759/rdgf.v19i3.1603.

Munawar, Hafiz Suliman, Fahim Ullah, Siddra Qayyum, e Danish Shahzad. 2022. «Big Data in Construction: Current Applications and Future Opportunities». Big Data and Cognitive Computing 6 (1): 18. https://doi.org/10.3390/bdcc6010018.

Pawelec, Maria. 2022. «Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions». Digital Society 1 (2): 19. https://doi.org/10.1007/s44206-022-00010-6.

Pernot-Leplay, Emmanuel. 2020. «China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?» Penn State Journal of Law & International Affairs 8 (1). https://elibrary.law.psu.edu/jlia/vol8/iss1/6.

Quattrone, Paolo. 2016. «Management accounting goes digital: Will the move make it wiser?» Management Accounting Research, 25th Anniversary Conference, 31 (junho):118–22. https://doi.org/10.1016/j.mar.2016.01.003.

Quinn, Paul, e Gianclaudio Malgieri. 2021. «The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework». German Law Journal 22 (8): 1583–1612. https://doi.org/10.1017/glj.2021.79.

Rachur, Achyuth, Jonathan Putman, e Clifford Fisher. 2022. «What did the digital age mean for privacy in the United States?» Journal of Business & Retail Management Research 17 (01). https://doi.org/10.24052/JBRMR/V17IS01/ART-08.

República Portuguesa. 2021. «Resolução do Conselho de Ministros n.º 131/2021, Série I de 2021-09-10». https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/131-2021-171096337.

Salinas, Elizabeth, Rony Cueva, e Freddy Paz. 2020. «A Systematic Review of User-Centered Design Techniques». Em Design, User Experience, and Usability. Interaction Design, editado por Aaron Marcus e Elizabeth Rosenzweig, 253–67. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-49713-2_18.

Sarangi, Saswat, e Pankaj Sharma. 2020. *Big Data: A Beginner's Introduction*. London ; New York: Routledge, Taylor & Francis Group.

Sataka, Mayara Mayumi, e Matheus Felipe Silva. 2021. «"Big Tech". A ascensão dos dados e a morte da política». Revista Iberoamericana de Ciencia, Tecnología y Sociedad - CTS 16 (46). https://ojs.revistacts.net/index.php/CTS/article/view/221.

Sidlauskas, Aurimas. 2021. «The Role and Significance of the Data Protection Officer in the Organization». Em Socialiniai tyrimai, 44:8–28. https://doi.org/10.15388/Soctyr.44.1.1.

Silva, Izabel Rodrigues da, Thayane Nascimento Freitas, Nádia Fernanda Martins de Araújo, Deborah Lauriane da Silva Sousa, Maurício Amorim de Araújo Júnior, Aline Mendes Medeiros, e Rafael Soares Silva. 2021. «Acessibilidade digital em tempos de ensino remoto». Research, Society and Development 10 (4): e60010414966–e60010414966. https://doi.org/10.33448/rsd-v10i4.14966.

Silva, Thiago Henrique de Jesus. 2024. «A Desinformação como Instrumento de Dominação Capitalista». Interações: Sociedade e as novas modernidades, n.º 46 (junho), 9–27. https://doi.org/10.31211/interacoes.n46.2024.a1.

Tavares, António. 2019. *Administração Pública Portuguesa*. Lisboa ; Fundação Francisco Manuel dos Santos.

Terceiro, Luciana. 2023. «Nothing about us without us: The journey of digital accessibility in the making». Nordes Conference Series, junho. https://dl.designresearchsociety.org/nordes/nordes2023/exploratorypapers/14.

«The Definition of User Experience (UX)». 1998. Nielsen Norman Group. 8 de agosto de 1998. https://www.nngroup.com/articles/definition-user-experience/.

Trevisan, Guilherme Elias, Odisséia Aparecida Paludo Fontana, e Silvia Ozelame Rigo Moschetta. 2022. «Resolução de conflitos interinstitucionais nas relações entre usuários e plataformas digitais». Revista de Direito, Governança e Novas Tecnologias 8 (1): 146–67. https://doi.org/10.26668/IndexLawJournals/2526-0049/2022.v8i1.8941.

Tsatsou, Panayiota. 2022. «Vulnerable people's digital inclusion: intersectionality patterns and associated lessons». Information, Communication & Society 25 (10): 1475–94. https://doi.org/10.1080/1369118X.2021.1873402.

União Europeia. 2016. «Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)» OJ L. Vol. 119. http://data.europa.eu/eli/reg/2016/679/oj/por.

«Usability 101: Introduction to Usability». 2012. Nielsen Norman Group. 3 de janeiro de 2012. https://www.nngroup.com/articles/usability-101-introduction-to-usability/.

Vicente, Paulo Nuno. 2023. *Os Algoritmos e Nós*. Lisboa ; Fundação Francisco Manuel dos Santos.

Waldo, James, Herbert S. Lin, e Lawrence H. Cox. 2010. «Engaging Privacy and Information Technology in a Digital Age». Journal of Privacy and Confidentiality 2 (1). https://doi.org/10.29012/jpc.v2i1.581.

Walters, Robert, Leon Trakman, e Bruno Zeller. 2019. «Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches», janeiro. https://doi.org/10.1007/978-981-13-8110-2.

Wang, Min, e Zuosu Jiang. 2017. «The Defining Approaches and Practical Paradox of Sensitive Data: An Investigation of Data Protection Laws in 92 Countries and Regions and 200 Data Breaches in the World». International Journal of Communication, agosto. https://www.semanticscholar.org/paper/The-Defining-Approaches-and-Practical-Paradox-of-An-Wang-Jiang/922479b516c1e656262ca7f912919760f0029954.

Wilson, Shomir, Norman Sadeh, Noah Smith, Florian Schaub, Frederick Liu, Kanthashree Sathyendra, Daniel Smullen, et al. 2018. «Analyzing Privacy Policies at Scale: From Crowdsourcing to Automated Annotations». ACM Transactions on the Web 13 (dezembro):1–29. https://doi.org/10.1145/3230665.

Windlinger, Lukas, e Deniz Tuzcuoglu. 2021. «Usability theory: Adding a user-centric perspective to workplace management». Em A Handbook of Management Theories and Models for Office Environments and Services. Routledge.

Yorulmaz, Özlem. 2023. «A Detailed Analysis of the Digital Divide and Its Impact on the Development of Countries». Economic and Social Implications of Information and Communication Technologies, fevereiro, 104–21. https://doi.org/10.4018/978-1-6684-6620-9.ch007.

Zuboff, Shoshana. 2020. *A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira de poder*. Traduzido por Luis Filipe Silva e Miguel Serras Pereira. Relógio D'Água.

Zuboff, Shoshana, Norma Möllers, David Murakami Wood, e David Lyon. 2019. «Surveillance Capitalism: An Interview with Shoshana Zuboff». Surveillance & Society 17 (1/2): 257–66. https://doi.org/10.24908/ss.v17i1/2.13238.

APÊNDICE

BREVE DESCRIÇÃO DA ADMINISTRAÇÃO PÚBLICA SEGUNDO ENSAIO DE ANTÓNIO TAVARES[1]

Quanto à sua história

A teoria sobre a relação entre política e Administração Pública tem sofrido alterações ao longo dos anos. Inicialmente, a visão clássica defendia uma separação rigorosa entre ambas as esferas: os políticos eleitos seriam responsáveis por formular estratégias, enquanto os funcionários públicos se encarregariam de implementá-las de forma imparcial, seguindo uma hierarquia baseada nas suas competências técnicas. A Administração, nessa perspetiva, seria um instrumento para cumprir a vontade do eleitorado, subordinada às diretrizes políticas. No entanto, António Tavares sublinha que após a Segunda Guerra Mundial, verificou-se que essa separação era mais normativa do que prática. Por um lado, os ministros frequentemente não detinham o conhecimento técnico necessário para todas as decisões, o que implicava uma participação inevitável da Administração no processo decisório. Por outro lado, o crescimento do Estado-providência aumentou exponencialmente o número de funcionários públicos, ampliando a complexidade das suas funções. Paul H. Appleby (1945) citado por Tavares (2019) argumentou que os funcionários públicos desempenham um papel determinante no processo político, uma vez que «exercem discricionariedade administrativa (...) estabelecendo regras e procedimentos, interpretando a lei e decidindo a sua aplicação prática». Assim, todos os dirigentes e funcionários, além de uma função técnica, possuem também uma dimensão política, que pode influenciar, em diferentes graus, a implementação das decisões dos eleitos, segundo o autor. Portanto,

> «Política e Administração estão interligadas, sendo que esta deve ser encarada, na sua essência, como política utilizando-se aqui o termo no seu sentido mais amplo e apartidário. A Administração deve, pelo menos em contextos democráticos, estar sempre relacionada com as solicitações do público, e com a vontade pública expressa mediante decisões oficiais, formais e legislativas»[2].

Assim, a política não se limita à tomada de decisões formais, mas envolve também a participação ativa de dirigentes e funcionários na representação dos interesses públicos. Esta interligação sublinha a necessidade de examinar a relação entre a atividade administrativa e a governança democrática. António Tavares aponta que o sucesso de qualquer lei ou programa público depende tanto da disponibilização de recursos por parte do poder político quanto do comprometimento da Administração Pública, uma ideia que insere a Administração no centro da tríade de poder composta pela Administração, os funcionários e a estrutura política. Neste contexto, a Administração Pública representa «o rosto do Estado» e reflete o funcionamento do sistema político.

A política pública, segundo Tavares, pode ser dividida em três fases: adoção, implementação e avaliação. No caso português, o autor identifica uma grande ênfase na primeira fase, enquanto a imple-

1 Tavares. 2019.

2 Ibid.

mentação recebe menor atenção e a avaliação dos resultados é amplamente negligenciada. Esta falha na avaliação é um dos pontos fracos da Administração Pública em Portugal, onde há uma falta de cultura de medição de resultados que vá além dos números e quantidades.

> «Apesar de haver ilhas de excelência e serviços com particular mérito na forma de desempenho — a segurança social é um exemplo disso — a falta de cultura de avaliação prende-se mais com a necessidade de avaliar para além de quantidades. Um exemplo é o programa Novas Oportunidades, que contabiliza diplomas, mas não avalia o impacto real na vida das pessoas: se conseguiram emprego, se houve uma mudança efetiva nas suas condições de vida»[3].

Este défice de avaliação é visto como o «calcanhar de Aquiles» da Administração Pública, deixando a desejar na medição do impacto das políticas públicas e refletindo uma limitação na gestão eficaz dos programas. A identificação de indicadores que realmente traduzam o efeito de determinadas medidas é fundamental para assegurar uma Administração Pública eficiente e em sintonia com as necessidades da sociedade.

Continuando na análise histórica da Administração Pública em Portugal, Tavares observa que o regime do Estado Novo proporcionou uma estrutura burocrática estável que facilitou a transição para a democracia após o 25 de Abril de 1974. Contudo, grande parte da elite burocrática manteve-se no poder, preservando a cultura organizacional herdada do período autoritário. Apesar da reorganização dos altos quadros, essa mudança foi insuficiente para transformar significativamente a cultura da Administração Pública.

Durante o período democrático, o número de funcionários públicos cresceu consideravelmente, duplicando entre 1968 e 1979, acompanhando a expansão das funções do Estado nos setores da educação, saúde e segurança social. Esse crescimento refletiu também o papel do setor público em absorver os recursos humanos resultantes da descolonização e das nacionalizações, que aumentaram a intervenção estatal na economia. Até 2005, o número de funcionários públicos atingiu um pico de mais de 560 mil, estabilizando-se após a intervenção da Troika e a implementação de reformas que restringiram novas contratações.

Atualmente, os funcionários públicos em Portugal representam cerca de 15,2% da força de trabalho total, uma percentagem abaixo da média da Organização para a Cooperação e Desenvolvimento Económico (OCDE), (18,06%). Esta realidade, segundo Tavares, contraria a perceção generalizada de que a Administração Pública portuguesa é excessivamente onerosa. Embora o Estado-providência seja, de facto, dispendioso, não é a Administração Pública que deve ser responsabilizada por esse custo, uma vez que se tem tornado progressivamente menos significativa em termos de despesa total.

Quanto à sua estrutura

Relativamente à sua estrutura, a Administração Pública também passou por modificações assinaláveis. A partir da década de 1980, sob a influência do conjunto de reformas empreendidas nos países da OCDE e conhecidas como «Nova Gestão Pública», intensificou-se a atenção dada à modernização e eficiência da Administração Pública. Esta abordagem, inspirada em práticas de gestão do setor privado, focava-se na promoção da qualidade dos serviços e processos administrativos, adotando uma lógica de mercado. Esse novo paradigma conduziu à criação de agências públicas com maior autonomia administrativa e financeira, os chamados institutos públicos, que visavam maior eficiência na gestão dos recursos e na prestação de serviços.

3 Tavares. 2019.

A evolução da Administração Pública portuguesa, em sintonia com a democratização e o desenvolvimento dos Estados europeus, teve marcos significativos ao longo das últimas quatro décadas, contribuindo para a sua modernização e adaptação às exigências contemporâneas.

No final da década de 1960, com o estabelecimento do Secretariado da Reforma Administrativa, o governo procurou promover o desenvolvimento económico, preparando o terreno para a construção de um Estado social. Este órgão foi responsável por propor reformas estruturais nas organizações públicas e nos seus modos de funcionamento, mas essas iniciativas só se concretizariam com o 25 de Abril de 1974, que marcou o início da transição democrática.

Na década de 1980, após uma fase de instabilidade política nos anos imediatamente a seguir à Revolução, o processo de profissionalização da Administração Pública ganhou novo impulso, sobretudo após o pedido de adesão à Comunidade Económica Europeia (CEE). Reformas institucionais e a criação de programas de formação especializada para os funcionários e dirigentes públicos foram fundamentais nesse processo. Destacam-se a fundação do Instituto Nacional da Administração (INA) em 1979 e do Centro de Estudos e Formação Autárquica (CEFA) em 1980, ambos com a missão de qualificar os quadros da Administração Pública, melhorando a sua capacidade de resposta às novas exigências da governação democrática.

Paralelamente, o Estatuto do Dirigente da Administração Pública, aprovado em 1979, representou uma mudança importante ao eliminar a nomeação vitalícia dos dirigentes, introduzindo uma maior rotatividade e abertura nas nomeações, rompendo com o tradicional circuito fechado entre a alta Administração Pública e os partidos no governo. Esta medida foi vista como essencial para reduzir a dependência política dos cargos administrativos e promover uma maior meritocracia na seleção de dirigentes.

Em 1982, o Gabinete de Estudos e Coordenação da Reforma Administrativa (GECRA) produziu a primeira reflexão teórica sustentada sobre a reforma administrativa em Portugal. O GECRA focou-se em questões cruciais, como a desburocratização, a simplificação administrativa, e políticas de emprego e formação profissional. Esse esforço teórico teve impacto direto na formulação de políticas que seriam desenvolvidas pela Secretaria de Estado da Modernização Administrativa (SEMA), criada em 1986, cuja missão era reformar o Estado e torná-lo mais eficiente. Com a SEMA, deu-se início a uma agenda política que procurava alterar as estruturas e práticas tradicionais da Administração Pública, com o objetivo de transformar o Estado numa máquina mais ágil e voltada para o cidadão, visto como cliente dos serviços públicos.

Durante os dois primeiros governos liderados pelo primeiro-ministro Cavaco Silva, entre 1985 e 1995, foram implementadas as primeiras iniciativas de simplificação administrativa e desburocratização. Estas reformas visavam também a redução da intervenção estatal na economia, alinhando-se com a agenda liberalizante que marcou este período. Entre as medidas, destacam-se a redução do peso do Estado em setores produtivos e o estímulo ao setor privado, o que refletiu um movimento global de redimensionamento do papel do Estado nas economias ocidentais, influenciado por políticas neoliberais.

No âmbito dessas reformas, foram introduzidas ferramentas de gestão pública mais orientadas para os resultados, como a criação de contratos de gestão e mecanismos de avaliação de desempenho, tanto para os serviços como para os funcionários públicos. Esta mudança na estrutura e cultura administrativa procurou tornar a Administração Pública mais responsável e orientada para a prestação de serviços de qualidade aos cidadãos, incentivando maior transparência e responsabilização nos processos governamentais.

A estrutura da Administração Pública portuguesa foi profundamente moldada pelas dinâmicas de reforma iniciadas na década de 1980. Com base nos princípios da Nova Gestão Pública, houve um

esforço concertado para modernizar, profissionalizar e tornar a Administração mais eficiente e responsiva, inserindo-a num quadro de gestão orientado para resultados e focado na melhoria contínua da prestação de serviços públicos.

Quanto aos seus vetores

Ao longo do percurso fragmentado de modernização da Administração Pública, as «Mil Medidas de Modernização Administrativa» (1993) tiveram um impacto significativo na reforma administrativa, ainda que carecessem de uma orientação estratégica global. Entre essas medidas destacam-se a introdução de caixas de comentários e sugestões, a extensão dos horários de atendimento e dos meios de pagamento, bem como o reforço da formação em atendimento ao cliente-utente. A publicação e entrada em vigor do Código do Procedimento Administrativo (1992) consolidou diversas iniciativas anteriores, trazendo aos cidadãos novos direitos no seu relacionamento com a Administração Pública, além de incrementar a prontidão e a fiabilidade das decisões administrativas.

A capacidade da Administração Pública portuguesa de aderir a tendências contemporâneas, conforme salienta António Tavares, tornou-se uma característica distintiva. Nos anos 90, Portugal alinhou-se com as práticas de administrações mais avançadas da Europa, destacando a ênfase na qualidade como um eixo central da modernização administrativa. A criação do Conselho Nacional da Qualidade e a aprovação da Carta da Qualidade dos Serviços Públicos são exemplos dessas iniciativas. No entanto, a preocupação com a qualidade foi frequentemente suprimida pela rigidez normativa e legal, dificultando a eficácia das medidas implementadas. Segundo Tavares, o problema do «juridiquês» revela a tendência de as normativas se tornarem meros procedimentos formais, muitas vezes desvalorizadas em termos do seu mérito ou conteúdo intrínseco, comprometendo o impacto das reformas.

Outro vetor importante foi a adoção de políticas de simplificação, desburocratização e melhoria da qualidade dos serviços públicos. A criação do «Fórum Administração Cidadãos», que procurava promover a participação ativa na sugestão de melhorias nos serviços públicos, e a obrigatoriedade da presença do Livro de Reclamações nos serviços públicos, são medidas relevantes dessa fase. A criação da primeira Loja do Cidadão em 1999, que concentrou num só local diversos serviços públicos, facilitando o acesso dos cidadãos, é outro marco significativo. Além disso, Portugal participou em iniciativas internacionais como o *Quality Steering Group*, que culminou na adoção do *Common Assessment Framework* (CAF), um modelo de autoavaliação administrativa adotado por várias entidades, como o Instituto de Gestão Financeira da Segurança Social, mas que posteriormente caiu em desuso.

Estas iniciativas demonstram o esforço de Portugal em alinhar a sua Administração Pública com os padrões internacionais, especialmente na melhoria da qualidade dos serviços prestados aos cidadãos. Contudo, entre 1986 e 2001, esse alinhamento foi marcado por uma implementação pontual e muitas vezes desarticulada, conforme assinala António Tavares, devido à cedência a interesses de grupos económicos.

Por outro lado, as reformas administrativas implementadas entre 2003 e 2009 foram mais coerentes e articuladas do que nos quinze anos anteriores. Este período de estabilidade resultou da aplicação consistente dos princípios da Nova Gestão Pública, com respostas específicas às exigências contemporâneas, centradas na eficiência e na gestão por objetivos. Durante o mandato do primeiro-ministro Durão Barroso (2002-2004), retomou-se a adoção do Sistema Integrado de Avaliação do Desempenho da Administração Pública (SIADAP), baseado nos princípios da gestão por objetivos, que priorizou a eficiência na Administração Pública. A gestão por resultados passou a ter um papel central, e as organizações públicas foram incentivadas a definir metas claras e mensuráveis, o que proporcionou uma mudança substancial ao afastar o foco exclusivo nos procedimentos.

Entre as oportunidades identificadas neste contexto, destaca-se a possibilidade de aplicar os resultados das investigações acadêmicas e práticas administrativas nos procedimentos decorrentes da gestão por objetivos, uma estrutura que permanece ativa e relevante no panorama atual.

António Tavares menciona ainda dois programas emblemáticos que marcaram a continuidade das reformas administrativas, mantendo a lógica de gestão: o Programa de Simplificação Administrativa e Legislativa (Simplex) e o Programa de Reestruturação da Administração Central do Estado (PRACE), ambos implementados durante o mandato do XVII Governo, liderado por José Sócrates. O Simplex, gerido pela Unidade de Coordenação para a Modernização Administrativa (UCMA) e posteriormente pelo Gabinete da Secretária de Estado da Modernização Administrativa, teve como objetivo central simplificar as interações entre cidadãos e Administração, reduzir encargos para empresas, promover a transparência, incentivar a participação dos utentes e adaptar as exigências administrativas à complexidade de cada situação. Embora tenha sido tecnicamente bem-sucedido, o Simplex foi afetado pela crise financeira e pelo Programa de Assistência Económica e Financeira (PAEF), refletindo uma vulnerabilidade comum a muitos programas públicos bem-sucedidos.

Quanto ao PRACE, que visava melhorar a eficiência dos serviços públicos por meio de avaliação, descentralização e simplificação de procedimentos administrativos, culminou numa reorganização da administração central do Estado, com o objetivo de aproximar os serviços públicos dos cidadãos. Contudo, tal como outras iniciativas anteriores, o PRACE não foi avaliado de forma abrangente, o que, segundo António Tavares, revela uma persistente resistência da Administração Pública central em se submeter a escrutínios rigorosos e sistemáticos.

Em suma, os vetores de modernização da Administração Pública portuguesa, como a promoção da qualidade, a simplificação administrativa e a gestão por objetivos, refletiram uma tentativa consistente de alinhar a administração com os padrões internacionais. Contudo, apesar dos avanços e esforços significativos, a falta de articulação entre as iniciativas e a resistência ao escrutínio continuaram a dificultar a implementação plena e eficaz dessas reformas.

ANEXOS

ANEXO A

PARAMETRIZAÇÃO DAS CATEGORIAS DE PRIVACIDADE

▼ 1. Argumentos Venda

1.1 Confirma-se que o site não vende dados → condicional

1.2 Os dados pessoais são vendidos ou alugados. 30%

1.3 Alguns dados são vendidos a terceiros. 40%

1.4 O site omite informações sobre a venda de dados. 30%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - Fórmula SOMA ATRIBUTO Venda

```
((IF({1.1 Confirma-se que o site não vende dados?}=1, 1, 0) * 0) + (IF
({1.2 Os dados pessoais são vendidos ou alugados?}=1, 1, 0) * 0.3)+ (IF
({1.3 Alguns dados são vendidos a terceiros?}=1, 1,0) * 0.4)+ (IF({1.4 O
site omite informações sobre a venda de dados?}=1, 1, 0) * 0.3) )
```

▼ 2. Argumentos Partilha

2.1 Confirma-se que o site não partilha dados → condicional

2.2 A partilha das informações recolhidas é restrita à transação pretendida. (13%)

2.3 São fornecidas opções de controlo sobre a partilha de dados e manutenção da sua propriedade. (7%)

2.4 O tratamento dos meus dados inclui transmissões para amigos. (12%)

2.5 Os meus dados pessoais podem ser partilhados com outras empresas e fóruns públicos. (13%)

2.6 Os meus dados pessoais podem ser apresentados abertamente. (10%)

2.7 Prevê-se a partilha de informações para fins de anúncios. (14%)

2.8 As informações recolhidas com as minhas atividades são rastreadas por entidades externas. (10%)

2.9 As filiais e os terceiros já não estão vinculados às mesmas práticas de privacidade. (7%)

2.10 Alguns dos dados recolhidos deixam de ser propriedade do fornecedor de serviços. (7%)

2.11 Verifica-se que o site é omisso acerca da partilha de dados com entidades externas. (7%)

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - Fórmula SOMA ATRIBUTO Partilha

```
((IF({2.1 Confirma-se que o site não partilha dados?}=1, 1, 0)* 0)+(IF
({2.2 A partilha das informações recolhidas é restrita à transação preten
dida? }=1, 1, 0)* 0.13)+(IF(({2.3 São fornecidas opções de controlo sobre
a partilha de dados e manutenção da sua propriedade?}=1, 1, 0)* 0.07)+(IF
({2.4 O tratamento dos meus dados inclui transmissões para amigos? }=1,
```

```
1, 0)* 0.12)+(IF({2.5 Os meus dados pessoais podem ser partilhados com ou
tras empresas e fóruns públicos? } =1, 1, 0)* 0.13)+(IF({2.6 Os meus dado
s pessoais podem ser apresentados abertamente?} =1, 1, 0)* 0.10)+(IF({2.7
Há partilha das informações para fins de anúncios? }  =1, 1, 0)* 0.14)+(I
F({2.8 As informações recolhidas com as minhas atividades são rastreadas
por entidades externas ? } =1, 1, 0)* 0.10)+(IF({2.9 As filiais e os terc
eiros já não estão vinculados às mesmas práticas de privacidade? } =1, 1,
0)* 0.07)+(IF({2.10 Alguns dos dados recolhidos deixam de ser propriedade
do fornecedor de serviços?}=1, 1, 0)* 0.07)+(IF(({2.11 Verifica-se que o
site omite acerca da partilha de dados com entidades externas? } =1, 1,
0)* 0.07))
```

▼ 3. Argumentos Recolha

3.1 Confirmação da não recolha de dados: → condicional

3.2 Limitação, adequação e relevância da recolha de dados: 20%

3.3 Inclusão de informações pessoais identificáveis: 5%

3.4 Inclusão de informações de contato: 5%

3.5 Inclusão de informações demográficas gerais: 5%

3.6 Inclusão do endereço IP do usuário: 5%

3.7 Inclusão de registros do comportamento de navegação: 5%

3.8 Inclusão de preferências específicas do utilizador: 5%

3.9 Inclusão da localização geográfica do utilizador: 5%

3.10 Inclusão de informações financeiras: 5%

3.11 Referência nos códigos-fonte "Pixel" 5%

3.12 Referência nos códigos-fonte "Tracking" 5%

3.13 Referência nos códigos-fonte "Analytics": 5%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Recolha

```
(  (IF({3.1 Confirmação da não recolha de dados}=1, 1, 0)* 0)+
  (IF({3.2 Limitação, adequação e relevância da recolha de dados} =1, 1,
0)* 0.20)+
  (IF({3.3 Inclusão de informações pessoais identificáveis}=1, 1, 0)* 0.0
5)+
  (IF({3.4 Inclusão de informações de contato}=1, 1, 0)* 0.05)+
  (IF({3.5 Inclusão de informações demográficas gerais} =1, 1, 0)* 0.05)+
  (IF({3.6 Inclusão do endereço IP do usuário} =1, 1, 0)* 0.05)+
  (IF({3.7 Inclusão de registos do comportamento de navegação}=1, 1, 0)*
0.05)+
  (IF({3.8 Inclusão de preferências específicas do utilizador}=1, 1, 0)*
0.05)+
  (IF({3.9 Inclusão da localização geográfica do utilizador }=1, 1, 0)*
0.05)+
  (IF({3.10 Inclusão de informações financeiras}=1, 1, 0)* 0.05)+
  (IF({3.11 Referência nos códigos-fonte "Pixel”}=1, 1, 0)* 0.05)+
```

```
  (IF({3.12 Referência nos códigos-fonte "Tracking" }=1, 1, 0)* 0.05)+
  (IF({3.13 Confirma-se a referência nos códigos-fonte do termo "Analytic
s”}=1, 1, 0)* 0.05)   )
```

▼ 4. Argumentos Finalidade

4.1 Confirma-se a omissão dos fins específicos da utilização de dados pessoais? → condicional

4.2 Os objetivos da utilização são identificados no momento da recolha de dados ou previamente: **35**%

4.3 É explicado de forma clara para que são utilizados os dados recolhidos: **30%**

4.4 Os dados são tratados com uma base legal e com interesse legítimo: **25%**

4.5 É especificada uma utilização secundária para outros fins que não a conclusão da interação atual: **10%**

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Finalidade

```
(  (IF({4.1 Confirmação da omissão dos fins específicos da utilização de
dados pessoais.} =1, 1, 0)* 0)+
  (IF({4.2 Os objetivos da utilização são identificados no momento da rec
olha de dados ou previamente} =1, 1, 0)* 0.35)+
  (IF({4.3 É explicado de forma clara para que são utilizados os dados re
colhidos}=1, 1, 0)* 0.30)+
  (IF({4.4 Os dados são tratados com uma base legal e com interesse legít
imo. } =1, 1, 0)* 0.25)+
  (IF({4.5 É especificada uma utilização secundária para outros fins que
não a conclusão da interação atual }=1, 1, 0)* 0.05)   )
```

▼ 5. Argumentos Transparência

5.1 Não indica qualquer informação sobre os dados recolhidos. → **condicional**

5.2 Apresenta uma política de privacidade atualizada e documentada publicamente sobre os dados que recolhem? **15%**

5.3 A política de privacidade informa sobre quem retém os dados do utilizador? **10%**

5.4 A política de privacidade informa sobre porque utilizam os dados do utilizador? **10%**

5.5 Existe uma indicação do período de conservação dos dados? **10%**

5.6 A política de privacidade inclui os termos da divulgação dos dados? **10%**

5.7 A política de privacidade menciona como são protegidas as informações pessoais. **10%**

5.8 Disponibiliza pormenores sobre possibilidades de reidentificação. **5%**

5.9 A política de privacidade é facilmente acessível. **5%**

5.10 O interface do utilizador comunica e apoia os direitos da pessoa em causa através duma prática de gestão de dados aberta e facilmente disponível. **5%**

5.11 Os titulares dos dados são informados sobre seus direitos e têm acesso às informações através de notificação prévia à obtenção do consentimento. **5%**

5.12 A política de privacidade comunica de forma clara todas as informações essenciais sobre os dados recolhidos. **3%**

5.13 Permite que o utilizador tenha acesso às informações pessoais e possa fazer uma cópia de determinados dados. **4%**

5.14 As promessas e objetivos declarados permitem uma verificação independente (auditorias). **5%**

5.15 Existe menção a alterações da política de utilização na política de privacidade? **3%**

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Transparência

```
(  (IF({5.1 Omissão de qualquer informação sobre os dados recolhidos.}=1, 1, 0)* 0)+
  (IF({5.2 Apresenta uma política de privacidade atualizada e documentada publicamente sobre os dados que recolhem.}=1, 1, 0)* 0.15)+
  (IF({5.3 A política de privacidade informa sobre quem retém os dados do utilizador? }=1, 1, 0)* 0.10)+
  (IF({5.4 A política de privacidade informa sobre porque utilizam os dados do utilizador?}=1, 1, 0)* 0.10)+
  (IF({5.5 Existe uma indicação do período de conservação dos dados? }=1, 1, 0)* 0.10)+
  (IF({5.6 A política de privacidade inclui os termos da divulgação dos dados?}=1, 1, 0)* 0.10)+
  (IF({5.7 A política de privacidade menciona como são protegidas as informações pessoais.} =1, 1, 0)* 0.10)+
  (IF({5.8 Disponibiliza pormenores sobre possibilidades de reidentificação. }=1, 1, 0)* 0.05)+
  (IF({5.9 A política de privacidade é facilmente acessível.}=1, 1, 0)* 0.05)+
  (IF({5.10 O interface do utilizador comunica e apoia os direitos da pessoa em causa através duma prática de gestão de dados aberta e facilmente disponível.}=1, 1, 0)* 0.05)+
  (IF({5.11 Os titulares dos dados são informados sobre seus direitos e têm acesso às informações através de notificação prévia à obtenção do consentimento. }=1, 1, 0)* 0.05)+
  (IF({5.12 A política de privacidade comunica de forma clara todas as informações essenciais sobre os dados recolhidos. }=1, 1, 0)* 0.03)+
  (IF({5.13 Permite que o utilizador tenha acesso às informações pessoais e possa fazer uma cópia de determinados dados.}=1, 1, 0)* 0.04)+
  (IF({5.14 As promessas e objetivos declarados permitem uma verificação independente.}=1, 1, 0)* 0.05) +
  (IF({5.15 Existe menção a alterações da política de utilização na política de privacidade.}=1, 1, 0)* 0.03)  )
```

▼ 6. Argumentos Segurança

6.1 Existe referência à encriptação das informações recolhidas e processadas? 30%

6.2 Os dados pessoais estão barrados a quem não tem acesso ao seu tratamento? 10%

6.3 A entidade garante a proteção das informações pessoais contra o acesso não autorizado dos dados? 15%

6.4 A entidade garante a proteção das informações pessoais contra a perda acidental dos dados? 15%

6.5 A entidade garante a proteção das informações pessoais contra a danificação dos dados? 15%

6.6 A entidade garante a proteção das informações pessoais contra a destruição dos dados? 15%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Segurança

```
(  (IF({6.1 Existe referência à encriptação das informações recolhidas e
processadas? } =1, 1, 0)* 0)+
  (IF({6.2 Os dados pessoais estão barrados a quem não tem acesso ao seu
tratamento?}=1, 1, 0)* 0.35)+
  (IF({6.3 A entidade garante a proteção das informações pessoais contra
o acesso não autorizado dos dados?}=1, 1, 0)* 0.30)+
  (IF({6.4 A entidade garante a proteção das informações pessoais contra
a perda acidental dos dados?} =1, 1, 0)* 0.25)+
  (IF({6.5 A entidade garante a proteção das informações pessoais contra
a danificação dos dados?}=1, 1, 0)* 0.05)+
  (IF({6.6 A entidade garante a proteção das informações pessoais contra
a destruição dos dados?} =1, 1, 0)* 0.10) )
```

▼ 7. Argumentos Responsabilidade

7.1 A organização responsável pelo tratamento de dados é identificada? 25%

7.2 O titular dos dados pode responsabilizar o serviço e contestar a conformidade dos dados obtidos? 15%

7.3 É mencionado o Direito de apresentar queixa a uma autoridade de controlo? 10%

7.4 A resolução do tratamento das queixas é prevista e assegurada? 10%

7.5 A entidade assume a proteção das informações pessoais contra o acesso não autorizado dos dados? 10%

7.6 A entidade assume a proteção das informações pessoais contra a perda acidental dos dados? 10%

7.7 A entidade assume a proteção das informações pessoais contra a danificação dos dados? 10%

7.8 A entidade assume a proteção das informações pessoais contra a destruição dos dados? 10%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Responsabilidade

```
(  (IF({7.1 A organização responsável pelo tratamento de dados é identificad
  (IF({7.2 O titular dos dados pode responsabilizar o serviço e contestar a
  (IF({7.3 É mencionado o Direito de apresentar queixa a uma autoridade de c
  (IF({7.4 A resolução do tratamento das queixas é prevista e assegurada?}=1
  (IF({7.5 A entidade assume a proteção das informações pessoais contra o ac
  (IF({7.6 A entidade assume a proteção das informações pessoais contra a pe
```

```
  (IF({7.7 A entidade assume a proteção das informações pessoais contra a da
  (IF({7.8 A entidade assume a proteção das informações pessoais contra a de
```

▼ 8. Argumentos Retenção

8.1 O período de conservação dos dados é especificado consoante a finalidade prevista? 30%

8.2 Os dados pessoais não são mantidos por mais tempo do que o necessário para os fins declarados? 40%

8.3 Os dados são destruídos de forma segura mediante pedido ou após o cumprimento dos objetivos? 30%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Retenção

```
(  (IF({8.1 O período de conservação dos dados é especificado consoante a
  (IF({8.2 Os dados pessoais não são mantidos por mais tempo do que o nec
  (IF({8.3 Os dados são destruídos de forma segura mediante pedido ou após
```

▼ 9. Argumentos Direito a ser esquecido

9.1 A possibilidade de apagar informações é abordada. 40%

9.2 A participação individual no direito de solicitar a remoção dos dados do contexto específico ou a quem foram divulgados é garantida. 60%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Direito a ser esquecido

```
(  (IF({9.1 A possibilidade de apagar informações é abordada.  }=1, 1, 0)
* 0.40)+
  (IF({9.2 A participação individual no direito de solicitar a remoção do
s dados do contexto específico ou a quem foram divulgados é garantida.}=
1, 1, 0)* 0.60) )
```

▼ 10. Argumentos Anonimização

10.1 É referido o tratamento de forma anónima (anonimização). 50%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Anonimização

```
(  (IF({10.1 É referido o tratamento de forma anónima.}=1, 1, 0)* 0.50)
)
```

▼ 11. Argumentos Pseudonimização

11.1 É mencionado que os dados são pseudonimizados. 50%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Pseudonimização

```
(  (IF({11.1 É mencionado que os dados são pseudonimizados.}=1, 1, 0)* 0.
50)   )
```

▼ 12. Argumentos Correção

12.1 Existe a possibilidade de aceder aos dados de forma simples, rápida e eficiente. 15%

12.2 Existe notificação explícita dos meios pelos quais o utilizador pode solicitar a alteração de dados incorretos. 50%

12.3 A exatidão e o caracter exaustivo dos dados podem ser contestados e revistos. 25%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Correção

```
(  (IF({12.1 Existe a possibilidade de aceder aos dados de forma simples,
rápida e eficiente.} =1, 1, 0)* 0.15)+
  (IF({12.2 Existe notificação explícita dos meios pelos quais o utilizad
or pode solicitar a alteração de dados incorretos.}=1, 1, 0)* 0.50)+
  (IF({12.3 A exatidão e o caracter exaustivo dos dados podem ser contest
ados e revistos.} =1, 1, 0)* 0.20)
```

▼ 13. Argumentos Controlo

13.1 O utilizador pode optar por não participar na recolha ou no tratamento dos dados e não autorizar 20%

13.2 O utilizador tem de dar o seu consentimento para a recolha e o tratamento dos seus dados. 20%

13.3 O utilizador pode limitar a recolha, nomeadamente controlar a partilha com terceiros. 15%

13.4 O utilizador pode modificar o período de retenção. 5%

13.5 A descrição das escolhas que conduzem ao pedido de consentimento para recolha e tratamento dos dados é explicita e por isso permite um consentimento realmente informado para qualquer utilizador. 20%

13.6 As opções de utilização apresentam-se em interface fácil para qualquer utilizador. 20%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Controlo

```
(  (IF({13.1 O utilizador pode optar por não participar na recolha ou no
tratamento dos dados e não autorizar.}  =1, 1, 0)* 0.20)+
  (IF({13.2 O utilizador tem de dar o seu consentimento para a recolha e
o tratamento dos seus dados.}=1, 1, 0)* 0.20)+
  (IF({13.3 O utilizador pode limitar a recolha, nomeadamente controlar a
partilha com terceiros.}=1, 1, 0)* 0.15)+
  (IF({13.4 O utilizador pode modificar o período de retenção.} =1, 1, 0)
* 0.05)+
  (IF({13.5 A descrição das escolhas que conduzem ao pedido de consentime
nto para recolha e tratamento dos dados é explicita e por isso permite um
consentimento realmente informado para qualquer utilizador.}=1, 1, 0)* 0.
20)+
  (IF({13.6 As opções de utilização apresentam-se em interface fácil para
qualquer utilizador.} =1, 1, 0)* 0.20) )
```

▼ 14. Argumentos Divulgação

14.1 A entidade especifica a amplitude da divulgação dos dados, mencionando concretamente se o armazenamento é feito na UE. 20%

14.2 A entidade especifica a amplitude da divulgação dos dados, mencionando concretamente se existe transferência de dados pessoais para países terceiros fora da UE. 20%

14.3 Em caso de transferência de dados para fora da UE são garantidas medidas de proteção antes da divulgação de identificadores para o exterior. 20%

14.4 A comunicação de informações pessoais entre jurisdições geopolíticas é feita em conformidade com os requisitos legais, seguindo o princípio da limitação da utilização. 20%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Divulgação

```
(  (IF({14.1 A entidade especifica a amplitude da divulgação dos dados, m
encionando concretamente se o armazenamento é feito na UE.}=1, 1, 0)* 0.2
0)+
  (IF({14.2 A entidade especifica a amplitude da divulgação dos dados, me
ncionando concretamente se existe transferência de dados pessoais para pa
íses terceiros fora da UE.}=1, 1, 0)* 0.20)+
  (IF({14.3 Em caso de transferência de dados para fora da UE são garanti
das medidas de proteção antes da divulgação de identificadores para o ext
erior.} =1, 1, 0)* 0.20)+
  (IF({14.4 A comunicação de informações pessoais entre jurisdições geopo
líticas é feita em conformidade com os requisitos legais, seguindo o prin
cípio da limitação da utilização.}
  =1, 1, 0)* 0.20)    )
```

▼ 15. Argumentos Funcionalidade

15.1 O site/app limita o aproveitamento dos serviços prestados se o utilizador não partilhar as informações solicitadas. → condicional

15.2 O site/app permite utilizar o serviço sem qualquer prejuízo caso o utilizador opte não participar na recolha de dados. 50%

15.3 O sistema aparenta incorporar a privacidade do utilizador durante a maior parte da sua utilização funcional. 30%

COBERTURA DO ATRIBUTO a partir da resposta aos argumentos - SOMA ATRIBUTO Funcionalidade

```
(  (IF({15.1 O site/app limita o aproveitamento dos serviços prestados se
o utilizador não partilhar as informações solicitadas.}=1, 1, 0)* 0)+
  (IF({15.2 O site/app permite utilizar o serviço sem qualquer prejuízo c
aso o utilizador opte não participar na recolha de dados. }=1, 1, 0)* 0.5
0)+
  (IF({15.3 O sistema aparenta incorporar a privacidade do utilizador dur
ante a maior parte da sua utilização funcional.} =1, 1, 0)* 0.30)   )
```

ANEXO B

REGISTOS DAS OBSERVAÇÕES DOS TESTES

Acessibilidade	Unidade Amostral	Notas
Sem certificação	FCT - Fundação Tecnologia e Ciência	• Dúvidas em responder a 2.3, 3.12, 3.13, 8.1, 4.1, 5.5, 5.11, 6.1, 6.2 e 13.4. • As primeiras perguntas têm de considerar logo a informação que vem dos *cookies* - controlo, funcionalidade • Talvez faça sentido ter uma lista miniatura previamente visível de tudo o que podemos identificar para ir clicando • Incluir nas instruções iniciais o mecanismo de pesquisa por palavra "find" • Não sei se deve existir um botão "não consegui responder/ não tenho como saber/ não entendo a pergunta" comtemplado com a nota • Terminar com classificação de acuidade, cansaço e dificuldade na experiência do utilizador. • Dar a entender que as notas são opcionais. • Claramente a ordem deve se melhor estruturada, não somente em função da visita como da ordem lógica de expectativa. • Primeira experiência: longa, pouco intuitiva, maioritariamente intragável. • O site da Fundação Tecnologia e Ciência foi o mais demorado de observar (60 minutos)
Sem certificação	NOVA FCT - Faculdade de Ciências e Tecnologia	• Dúvidas em responder a 3.6. • Não sei em que resposta encaixar a informação *"Categoria 3 — Cookies de funcionalidade / Permitem armazenar algumas opções efetuadas pelo utilizador durante a navegação nas páginas web. A título de exemplo, podem armazenar o idioma seleccionado para garantir que as páginas são sempre apresentadas no idioma pretendido."* • Quando os sites são pouco claros ou omissos em relação às perguntas específicas, fica-se na dúvida sobre o que responder porque dá a sensação de que a opção de omissão devia estar mais disponível. • Observação paralela do site com o Privacy Rating. Resultou em categoria B. • Quando as políticas de privacidade omitem detalhes, o utilizador não pode inferir com certeza se sim ou não. Isso demostra a limitação desta ferramenta e conduz a outra solução. O critério quando não sabemos pode ser qual? Sim ou não? O resultado foi este mas não é fiável porque não defini esse critério quanto à omissão.
Selo ouro	Portal Mais Transparência	• No campo "diretórios a que pertence" escolher se estão lá colocados todos os diretórios possíveis, ou se é melhor mudar para resposta aberta. Neste caso seriam: Os 25 Portais + Procurados da AP, Administração Pública Central, Secretaria de Estado da Digitalização e da Modernização Administrativa • Dúvidas em responder a 1.1, 1.4, 2.6, e 3. • Acho que pode ser incluída a possibilidade de recolha de informações fiscais. • É chato fazer estas verificações. Fica-se na dúvida muitas vezes. Pela omissão não se sabe o que responder. Se não for omisso é super longo. É uma situação sem solução simples ou óbvia, o paradoxo da privacidade latente.
Selo prata	Portal da Defesa Nacional	Não tem Politica de Privacidade, nem disclaimer de *cookies* apesar de ter página sobre cookies. Demasiado esquisito e invulgar para ser analisado, passo a outro site para ver o selo prata.

Acessibilidade	Unidade Amostral	Notas
Selo prata	Polo de Inovação Digital AI4PA – Artificial Intelligence for the Public Administration	Não tem *cookies*, o que é interessante. Mas a política de privacidade remete para a da AMA, o que se calhar torna menos interessante de observar porque é genérica e serve muitas outras entidades. Vou considerar outra unidade amostral para este selo.
Selo prata	Certificado do Registo Criminal	• Dúvidas em responder **5.6, 5.8.** • É omisso relativamente à partilha de dados, apesar de se apresentar robusto na segurança. É um bom exemplo que como o utilizador pode ficar aparentemente descansado mas sem que todos os atributos estejam descritos preto no branco. • Na recolha, podemos não saber especificamente que dados são recolhidos, pode-se presumir que a finalidade poderá implicar que dados pessoais são recolhidos, mas não se sabe realmente quais são sem passar pelo processo de registo. O detalhe das informações recolhidas dos argumentos deste atributo fica sem resposta real se a funcionalidade do registo não for ativada na observação. • É cada vez mais notório que um utilizador comum pode não está grandemente apto para garantir a veracidade das respostas no percurso da observação dos atributos, pois não detém toda a informação relativa ao posicionamento da instituição. O interessante seria que este teste escrutinador pudesse ser respondido pelo DPO da instituição. • A política de privacidade do Certificado Registo Criminal rebate muito bem a discutível ameaça da inclusão da recolha do IP ao referir o tratamento desses dados por agregação: “ *Para efeitos estatísticos* ***são registados os endereços IP de todas as ligações ao Portal do Cidadão.*** *Esta informação será utilizada* ***para efetuar análises estatísticas agregadas, não sendo estabelecida qualquer relação com os serviços e interações com os utilizadores.*** *O RCO monitorizará* ***toda a informação estatística relativa à utilização do serviço digital de forma agregada e anónima****. Os dados utilizados para este fim não contêm dados de identificação pessoal ou informação privada.*” • No caso da privacidade e segurança nos dados transmitidos ao Sistema de Informação de Identificação Criminal (SICRIM) parece ter enquadramento legal próprio: “ *sendo apenas pedidos e recolhidos os dados necessários para a prestação do serviço que estiver em causa na escolha do utilizador, os quais são tratados e conservados de acordo com as disposições legais constantes da Lei n.º 37/2015, de 5/5 e do Decreto-Lei n.º 171/2015, de 25/8.*” É suposto ter de ir lê-los para responder? Um utilizador comum não corresponderia a estar tarefa quase de certeza. • É no geral muito chato, aborrecido, e por vezes difícil de responder ao formulário inteiro, e de uma só vez.
Selo prata	Museu Nacional Ferroviário	O site do Museu Nacional Ferroviário foi o mais rápido de observar (apenas 7 minutos).
Selo bronze	Câmara Municipal de Águeda	• No caso de CMA especificavam que partilhavam dados mas não a terceiros, o que mostra que a exaustividade operacional dos argumentos também não foi alcançada. • Referencia a literacia ligada ao tema: “ *Assegurar a realização de ações de formação/informação/sensibilização, a quem procede ao tratamento de dados pessoais; / Implementar processos de monitorização, para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas, de modo a garantir a segurança do tratamento*”

ANEXO C (PI2)

TABELA DE CONSULTA PARA DIAGNÓSTICO DAS PRÁTICAS DE PRIVACIDADE ONLINE

1 VENDA

01. Confirma-se que o site não vende dados.
02. Os dados pessoais são vendidos ou alugados.
03. Alguns dados são vendidos a terceiros.
04. O site omite informações sobre a venda de dados.

2 PARTILHA

01. Confirma-se que o site não partilha dados.
02. A partilha das informações recolhidas é restrita à transação pretendida.
03. São fornecidas opções de controlo sobre a partilha de dados e manutenção da sua propriedade.
04. O tratamento dos meus dados inclui transmissões para amigos.
05. Os meus dados pessoais podem ser partilhados com outras empresas e fóruns públicos.
06. Os meus dados pessoais podem ser apresentados abertamente.
07. Prevê-se a partilha de informações para fins de anúncios.
08. As informações recolhidas com as minhas atividades são rastreadas por entidades externas.
09. As filiais e os terceiros já não estão vinculados às mesmas práticas de privacidade.
10. Alguns dos dados recolhidos deixam de ser propriedade do fornecedor de serviços.
11. Verifica-se que o site é omisso acerca da partilha de dados com entidades externas.

3 RECOLHA

01. Confirmação da não recolha de dados.
02. Limitação, adequação e relevância da recolha de dados.
03. Inclusão de informações pessoais identificáveis.
04. Inclusão de informações de contato.
05. Inclusão de informações demográficas gerais.
06. Inclusão do endereço IP do usuário.
07. Inclusão de registos do comportamento de navegação.
08. Inclusão de preferências específicas do utilizador.
09. Inclusão da localização geográfica do utilizador.
10. Inclusão de informações financeiras.
11. Referência nos códigos-fonte: *pixel*.
12. Referência nos códigos-fonte: *tracking*.
13. Referência nos códigos-fonte: *analytics*.

4 FINALIDADE:

01. Confirmação da omissão dos fins específicos da utilização de dados pessoais.
02. Os objetivos da utilização são identificados no momento da recolha de dados ou previamente.
03. É explicado de forma clara para que são utilizados os dados recolhidos.
04. Os dados são tratados com uma base legal e com interesse legítimo.
05. É especificada uma utilização secundária para outros fins que não a conclusão da interação atual.

5 TRANSPARÊNCIA:

01. Omissão de qualquer informação sobre os dados recolhidos.
02. Apresenta uma política de privacidade atualizada e documentada publicamente sobre os dados que recolhem.
03. A política de privacidade informa sobre quem retém os dados do utilizador.
04. A política de privacidade informa sobre por que utilizam os dados do utilizador.
05. Existe uma indicação do período de conservação dos dados.
06. A política de privacidade inclui os termos da divulgação dos dados.
07. A política de privacidade menciona como são protegidas as informações pessoais.
08. Disponibiliza pormenores sobre possibilidades de reidentificação.
09. A política de privacidade é facilmente acessível.
10. A interface do utilizador comunica e apoia os direitos da pessoa em causa através duma prática de gestão de dados aberta e facilmente disponível.
11. Os titulares dos dados são informados sobre seus direitos e têm acesso às informações através de notificação prévia à obtenção do consentimento.
12. A política de privacidade comunica de forma clara todas as informações essenciais sobre os dados recolhidos.
13. O site permite que o utilizador tenha acesso às informações pessoais e possa fazer uma cópia de determinados dados.
14. As promessas e objetivos declarados no site permitem uma verificação independente.
15. Existe menção a alterações da política de utilização na política de privacidade.

6 SEGURANÇA:

01. Existe referência à encriptação das informações recolhidas e processadas.
02. Os dados pessoais estão barrados a quem não tem acesso ao seu tratamento.
03. A entidade garante a proteção das informações pessoais contra o acesso não autorizado dos dados.
04. A entidade garante a proteção das informações pessoais contra a perda acidental dos dados.
05. A entidade garante a proteção das informações pessoais contra a danificação dos dados.
06. A entidade garante a proteção das informações pessoais contra a destruição dos dados.

7 RESPONSABILIDADE:

01. A organização responsável pelo tratamento de dados é identificada.
02. O titular dos dados pode responsabilizar o serviço e contestar a conformidade dos dados obtidos.
03. É mencionado o direito de apresentar queixa a uma autoridade de controlo.
04. A resolução do tratamento das queixas é prevista e assegurada.
05. A entidade assume a proteção das informações pessoais contra o acesso não autorizado dos dados.
06. A entidade assume a proteção das informações pessoais contra a perda acidental dos dados.
07. A entidade assume a proteção das informações pessoais contra a danificação dos dados.
08. A entidade assume a proteção das informações pessoais contra a destruição dos dados.

8 RETENÇÃO:

01. O período de conservação dos dados é especificado consoante a finalidade prevista.
02. Os dados pessoais não são mantidos por mais tempo do que o necessário para os fins declarados.
03. Os dados são destruídos de forma segura mediante pedido ou após o cumprimento dos objetivos.

9 DIREITO A SER ESQUECIDO:

01. A possibilidade de apagar informações é abordada.
02. A participação individual no direito de solicitar a remoção dos dados do contexto específico ou a quem foram divulgados é garantida.

10 ANONIMIZAÇÃO:

01. É referido o tratamento de forma anónima.

11 PSEUDONIMIZAÇÃO:

01. É mencionado que os dados são pseudonimizados.

12 CORREÇÃO:

01. Existe a possibilidade de aceder aos dados de forma simples, rápida e eficiente.
02. Existe notificação explícita dos meios pelos quais o utilizador pode solicitar a alteração de dados incorretos.
03. A exatidão e o carácter exaustivo dos dados podem ser contestados e revistos.

13 CONTROLO:

01. O utilizador pode optar por não participar na recolha ou no tratamento dos dados e não autorizar.
02. O utilizador tem de dar o seu consentimento para a recolha e o tratamento dos seus dados.
03. O utilizador pode limitar a recolha, nomeadamente controlar a partilha com terceiros.
04. O utilizador pode modificar o período de retenção.
05. A descrição das escolhas que conduzem ao pedido de consentimento para recolha e tratamento dos dados é explicita e por isso permite um consentimento realmente informado para qualquer utilizador.
06. As opções de utilização apresentam-se em interface fácil para qualquer utilizador.

14 DIVULGAÇÃO:

01. A entidade especifica a amplitude da divulgação dos dados, mencionando concretamente se o armazenamento é feito na UE.
02. A entidade especifica a amplitude da divulgação dos dados, mencionando concretamente se existe transferência de dados pessoais para países terceiros fora da UE.
03. Em caso de transferência de dados para fora da UE são garantidas medidas de proteção antes da divulgação de identificadores para o exterior.
04. A comunicação de informações pessoais entre jurisdições geopolíticas é feita em conformidade com os requisitos legais, seguindo o princípio da limitação da utilização.

15 FUNCIONALIDADE:

01. O site/app limita o aproveitamento dos serviços prestados se o utilizador não partilhar as informações solicitadas.
02. O site/app permite utilizar o serviço sem qualquer prejuízo caso o utilizador opte por não participar na recolha de dados.
03. O sistema aparenta incorporar a privacidade do utilizador durante a maior parte da sua utilização funcional.