O Público Não Quer a Verdade, Mas a Mentira que Mais Lhe Agrade: Fatores de Vulnerabilidade da Sociedade Portuguesa à Desinformação

Inês Narciso
Mestre em Criminologia pela Universidade de Leicester e doutoranda em Sociologia no ISCTE-IUL. Colaboradora do MediaLab do ISCTE-IUL.

Ana Costa
Licenciada em Criminologia pela Universidade do Porto e Mestre em Crime Global pela Universidade de Edimburgo.

Resumo

A complexidade da desinformação exige uma análise e uma resposta multidisciplinar, sustentada na identificação de fatores de risco e na sua mitigação. Para além dos contextos económico-sociais que permeiam a recetividade das populações à desinformação, como acontece atualmente em contexto de pandemia, identificaram-se três áreas de atuação preferencial onde as políticas públicas poderão ter um impacto direto e positivo: 1) no âmbito das caraterísticas da população, promovendo a literacia digital, sobretudo entre grupos mais vulneráveis; 2) nos índices de confiança destes grupos na comunicação social e nas instituições oficiais; 3) nas ações diretas destas instituições que visem conhecer o fenómeno para o regular de forma sustentada. Em Portugal, assiste-se a um desfasamento entre, por um lado, o desenvolvimento tecnológico das instituições e o uso cada vez mais frequente da Internet e, por outro lado, o conhecimento real dos utilizadores sobre os riscos e as vulnerabilidades da navegação *online* e particularmente nas redes sociais, nomeadamente sobre a desinformação. Apesar de os índices de confiança na comunicação social e nas instituições ligadas à ciência permanecerem elevados, apresenta-se como forte vulnerabilidade os baixos níveis relativamente às instituições governamentais. Por fim, reconhecendo esforços realizados no sentido de acompanhar algumas iniciativas europeias, em Portugal falta legislação e investimento em investigação sobre a desinformação e os projetos promovidos não têm ainda resultados práticos que façam face às vulnerabilidades detetadas. Perspetivar a evolução e agir para minimizar o potencial impacto desta ameaça contribuirão para proteger os portugueses e as instituições, salvaguardando competências e acesso a informação de qualidade que são condição necessária para uma democracia saudável.

Palavras-chave: Desinformação; Público; Mentira; Políticas Públicas; *Fake news.*

Abstract

The public does not want the truth, but the lies they like best: Factors of vulnerability to misinformation in Portuguese society

The complexity of desinformation requires a multidisciplinar analysis and response, based on identified risk factors and on actions designed to mitigate them. Beyond the social and economical contexts that might make people more susceptible to desinformation, as the current pandemic scenary, three areas were identified as specially relevant for political action due to the potential of generating direct and positive impact: 1) digital literacy should be promoted with a focus on the most vulnerable groups; 2) confidence levels on official media and institutions should be improved; 3) jointed action of different public and private entities must prioritize understanding and regulating desinformation in an efficient and ethical way.

In Portugal, the institutions have suffered a technological reform and developped in a significant digital way, and the number of internet users have grown substantially. However, the knowledge about the risks and vulnerabilities of internet use and, particularly, of social media does not meet the same standards. Although the portuguese population shows confidence in media and science institutions, the situation seems to be the opposite regarding the government.

Despite some efforts to follow european initiatives, Portugal is in need of legislation and investment in research about desinformation as the current projects seem not to have real effect on the vulnerabilities. It is the aim of this paper to help achieving real and positive results.

To foresee the evolution of desinformation and to act in order to minimize its impact will protect not only the portuguese people and institutions, but also the access to quality information and the hability to differentiate, which are essentials of a healthy democracy.

Keywords: *Disinformation; Public; Lies; Public policy; Fake news.*

Artigo recebido: 29.03.2021
Aprovado: 06.04.2021
https://doi.org/10.47906/ND2021.158.05

Introdução

A desinformação é um fenómeno que Portugal não pode desconsiderar, tomando uma posição de espetador do conflito híbrido que decorre entre outros países e no seio dos mesmos, em que conteúdo multimédia é disseminado *online* e operacionalizado como arma. Apesar das dificuldades de deteção e da ausência de limites geográficos da desinformação, já foram detetados sinais de politização de conteúdos desinformativos *online* em Portugal (Cardoso *et al.,* 2019), pelo que as instituições nacionais devem estar conscientes da problemática e preparar desde já uma resposta eficaz.

A "desordem informativa" (Wardle e Derakhshan, 2017, p. 10) que se verifica nos meios de comunicação é altamente complexa e o termo "notícias falsas" já se tornou totalmente desadequado para aludir ao fenómeno, pelo que se torna essencial entender que tipos de conteúdos são problemáticos, qual a motivação por trás da sua criação e como se disseminam. Paralelamente, é muito importante compreender que vulnerabilidades estão a ser exploradas e como nos podemos proteger enquanto indivíduos e sociedade, já que as consequências da exposição a conteúdos falsos ou maliciosos vão muito para além de gerar confusão, ceticismo e falta de confiança numa pessoa, instituição ou governo: podem influenciar os resultados de eleições, promover conflitos regionais, fortalecer vieses cognitivos, ou seja, pôr em causa a liberdade, a tolerância e a união, pilares da vida em sociedade e em democracia.

O presente artigo procura abordar a permeabilidade de Portugal à desinformação, numa avaliação sustentada de três áreas com influencia na sua produção, propagação e interação (Paisana *et al.,* 2020; Loos e Nijenhuis, 2020; Bayer *et al.,* 2019):

1) as caraterísticas sociodemográficas da população, a sua literacia digital e a consciencialização dos riscos da navegação *online;*
2) a relação e a confiança dos cidadãos nas instituições democráticas e o envolvimento da sociedade civil e
3) o papel das instituições governamentais, dos núcleos de investigação e desenvolvimento e a sua relação com o setor empresarial, traduzidas em cooperação multidisciplinar na caraterização e combate ao fenómeno, políticas públicas de sensibilização e legislação.

Esta avaliação será feita através da integração de dados quantitativos e qualitativos, com recurso a abordagem comparativa com dados internacionais, numa metodologia mista que procura traçar um enquadramento geral do atual panorama, identificando fragilidades e áreas de maior solidez. Como ponto de partida, efetua-se um balanço do conceito e da sua história recente, das estratégias, formas e origens

da desinformação e do seu potencial impacto, quer individual quer coletivo, assim como dos desafios inerentes à sua deteção e o tipo de respostas existentes, de onde emergem os fatores de influência analisados.

Definições/Termos Utilizados

A expressão *fake news* perdeu aplicabilidade nos modelos teóricos de desinformação por ser amplamente usada para atacar a imprensa, numa politização do termo que remeteu para segundo plano a legitimidade dos factos apresentados. Esta tendência, juntamente com a grande variedade de termos conexos como *clickbait*, rumores, dados falsos ou descontextualizados, teorias da conspiração, propaganda, entre outros, tem gerado necessidade de categorizar para um melhor entendimento e resposta ao fenómeno da desinformação.

Assim, tem sido amplamente divulgada a distinção de Wardle entre desinformação, "*mis*informação" e "*mal*informação" (Wardle e Derakhshan, 2017). Desinformação diz respeito a informação falsa disseminada deliberadamente com intuito de enganar, baralhar, influenciar. "*Mis*informação" é informação falsa disseminada sem se saber que não corresponde à verdade. Já "*mal*informação" refere-se a informação verdadeira cujo contexto é alterado maliciosamente ou a dados privados que são divulgados para humilhar/denegrir alguém. Todas vão contra os *standards* e a ética jornalística, mas, enquanto a desinformação e a "*mal*informação" são normalmente motivadas pelo lucro e pela influência política, ou simplesmente disseminadas para gerar confusão e problemas, a "*mis*informação" ocorre essencialmente pelo desejo de o indivíduo se mostrar como alguém informado, que quer ajudar, e pela vontade de pertencer a um grupo com ideias comuns.

Dado que estas diferenças não influem na base deste trabalho e tal como outros autores optam por fazer (Tandoc *et al.*, 2018), de forma a tornar a leitura deste artigo mais fluída, serão utilizados os termos desinformação e conteúdos desinformativos para referir "dados que não correspondem à verdade/maliciosos". Importa desde já mencionar que estes conteúdos tomam diferentes formas – texto, imagem, vídeo, áudio – sendo que o mais comum é serem compostos, conterem texto sensacionalista e apelarem a sentimentos mais extremos (Shu *et al.*, 2020).

História Breve

Há várias décadas que a desinformação é utilizada para influenciar a opinião pública e/ou ganhar vantagem sobre oponentes. Durante a Guerra Fria, como recordam Shu *et al.* (2020), era frequente o uso de informação falsa ou manipulada, via

estacões de rádio clandestinas e artigos em formato de notícias, para persuadir ou gerar confusão. A propaganda tendia a ser mais abertamente manipuladora, com uma mensagem mais consistente, mais emocional que informativa (Wardle e Derakhshan, 2018).

A emergência da sociedade em rede resultou num mundo mais conectado, numa aparente democratização da informação, num acesso mais alargado às notícias, aos direitos e às diferentes perspetivas sobre a vida em sociedade, conduzindo à criação de comunidades de pertença mobilizadas em redor de ideologias anteriormente isoladas. O alcance da internet e o seu potencial de partilha ampla e rápida têm sido instrumentalizados para disseminar conteúdos desinformativos com essência de propaganda e servir agendas específicas, o que já resultou em inúmeros episódios de violência e conflitos que puseram e põem em risco vidas humanas. Com a utilização generalizada dos *smartphones,* por um lado, é cada vez mais conveniente ler notícias *online,* e a utilização generalizada das aplicações de mensagens, por outro lado, permite que a informação alterada ou falsa se espalhe de forma descontrolada (Shu *et al.,* 2020).

Desta forma, a desinformação está a ser disseminada por utilizadores isolados e/ou que não confirmam antes de partilhar; por jornalistas altamente pressionados para publicar mais e obter mais reações aos seus artigos; por comunidades *online* que tentam difundir as suas ideias ou atacar ideias rivais; e por campanhas altamente sofisticadas e organizadas que usam redes de *bots* e *troll factories*. Neste ecossistema informativo, sofremos uma sobreabundância de estímulos informativos que dificulta a identificação de fontes credíveis (Organização Mundial da Saúde, 2020) e que deixa o nosso cérebro exausto e mais facilmente influenciável.

Estratégias

Como afirma Waltzman (2017), dado que as pessoas passaram a ter a internet e as redes sociais como primeira fonte de notícias e informação, estas consubstanciam atualmente o vetor ideal de ataque pela informação. Conscientes desta tendência, tanto partidos políticos como grandes marcas e indústrias apostam em fazer passar a sua mensagem *online,* tirando o melhor partido possível do modo como os modelos de negócio dos sites e das redes sociais funcionam, e da falta de limites geográficos, éticos, de regulamentação e de responsabilização.

Os objetivos comerciais por detrás das redes sociais têm-nas levado a desenvolver algoritmos para conhecer os utilizadores, os seus gostos e padrões de comportamento, mas também vulnerabilidades cognitivas e dependências, de forma a puderem identificar aqueles que mais provavelmente reagirão e partilharão determinado conteúdo. Depois, direcionam esses mesmos conteúdos a estes "alvos".

Quando estes os partilham, existe uma maior probabilidade de os seus contactos confiarem e de partilharem sucessivamente porque surgem de alguém que conhecem. Os conteúdos vão sendo disseminados, promovidos por cadeias de confiança *peer-to-peer.*

Este tipo de funcionamento gera *filter bubbles* ou *echo chambers:* espaços *online* em que se partilham conteúdos específicos, relevantes para determinados utilizadores e que ao encontro das suas crenças, reforçando o seu ponto de vista (Pariser, 2011). Este processo de exposição repetida a uma ideia, sobretudo se tiver origem em fontes diferentes, pode não só reforçar as ideias já existentes como também a resistência a mudar de opinião mesmo que esteja comprovadamente errada. Ao sentir esse reforço, não só acreditamos mais como tendemos a partilhar tais conteúdos, uma vez que sentimos que elevam a nossa reputação e divulgam o nosso valor enquanto fonte credível.

De salientar que alguns autores defendem que vivemos uma altura de particular suscetibilidade à desinformação. Segundo explica Shu *et al.* (2020), em tempos de crise, as pessoas tendem a procurar informação através de fontes oficiais. Quando não encontram, têm tendência para procurar em redes não oficiais para satisfazer a necessidade de saber. Quanto mais incerteza sentirem, maior a probabilidade de aceitarem informação nova mesmo que não confirmada. Em paralelo, perante a ansiedade, frustração e irritação associadas à incerteza, a desinformação pode contribuir para aliviar a tensão emocional ao abordar as preocupações sentidas, gerando conforto na sensação de algo ter lógica e de se obter uma resposta. De facto, quando o ser humano tem medo, a sua capacidade de raciocínio crítico fica reduzida e ele torna-se mais facilmente influenciável. Estas condicionantes estão particularmente presentes em tempos de crise económica, social ou de potencial conflito.

Por fim, importa destacar que as desordens informativas têm ganhado terreno fazendo uso de contas, acessos e dados obtidos em ataques informáticos. Na guerra híbrida, assiste-se a uma estreita ligação entre os ataques e a propaganda *online,* servindo os primeiros como ferramenta de suporte para promoção de um único objetivo final. Esta instrumentalização por atores maliciosos, sobretudo em estruturas mais organizadas, torna necessária uma resposta participada por parte dos órgãos de defesa (Liederkerke e Zinkanell, 2020).

Motivações/Origens

Como já mencionado, a desinformação consubstancia uma tentativa de manipular a opinião em determinada direção, que pode ocorrer por motivos ideológicos, políticos, económicos, por reputação ou pela diversão de causar confusão. Pode ser realizada por indivíduos ou grupos de forma mais ou menos organizada, mas também por estruturas sofisticadas.

Pode ser coordenada direta ou indiretamente por Estados ou grupos de interesses, que agem sobre uma entidade ou população específica, durante determinado período de tempo, com recurso a ferramentas tecnológicas avançadas como *troll factories* e redes de *bots* que injetam de forma coordenada e sistemática conteúdos manipulados nas múltiplas plataformas. De forma altamente competente e dedicada, estas *cyber troops* (Bradshaw e Howard, 2019, p. 9) imitam o comportamento humano, geram atividade artificial, identificam, por um lado, os utilizadores mais suscetíveis e, por outro, os mais influentes, para maximizar a exposição e a credibilidade, mas essencialmente a probabilidade de gerar determinado comportamento (Shu *et al.*, 2020). Frequentemente existem redes de entidades envolvidas, algumas reais e outras que servem como *proxy,* que promovem a disseminação dos conteúdos e dificultam a responsabilização. Estas redes podem incluir grupos industriais privados, organizações da sociedade civil, subculturas da internet, grupos de jovens, coletivos de *hackers,* movimentos marginais, influenciadores digitais e voluntários apoiantes da causa (Bradshaw e Howard, 2019).

Relativamente à desinformação criada e disseminada por Estados, é de salientar o inventário global de Bradshaw e Howard, publicado em 2019, depois da monitorização e análise da manipulação das redes sociais por partidos e governos nos 3 anos anteriores, que identifica tendências, ferramentas, capacidades, estratégias e recursos dos diferentes países.

Neste âmbito, a Rússia assume um lugar de destaque no processo de produção e distribuição de teorias da conspiração, em território nacional e no estrangeiro, escudando o Kremlin e barrando toda a informação alternativa, de forma altamente coordenada e a larga escala, com uma rede de entidades de media, incluindo desde jornais oficiais a páginas nas redes sociais e empresas de *trolls* (Avramov, 2018; Bennet e Livingston, 2018). Dentro da estrutura da Defesa, é reconhecida a existência da Information Operations Force, dando expressão real ao conceito de *hybrid warfare* (Hansen, 2017).

Por outro lado, segundo Wang, Rao e Sun (2020, pp. 1 e 3) na China vive-se uma *fakeness pandemic,* havendo mais de dois milhões de pessoas que são pagas para fazer comentários nas redes sociais (Bennet e Livingston, 2018). Em países como os EUA, a Alemanha, a Hungria, a Polónia e a Turquia, os ataques constantes à credibilidade da imprensa e a disseminação de desinformação *far-right* têm contribuído para polarizar a sociedade, para pânicos morais, episódios de violência e crimes de ódio (Bennett e Livingston, 2018).

Importa compreender que as cadeias de desinformação são muito complexas, raramente seguindo um fluxo único, podendo surgir de entidades organizadas, mas também de comunidades não estruturadas (Goode e Ben-Yehuda, 2009; Nielsen e Graves, 2017; Tiffen, 2019). Frequentemente existe um misto de atividade organizada, quer por Estados-Nação, *lobbys* económicos ou políticos ou outros grupos de interesse com reações espontâneas de indignação popular.

Impacto Individual e Impacto Coletivo

De forma a avaliar o risco associado à desinformação, importa compreender como a exposição ao fenómeno afeta a nível individual e social.
Enquanto alvos da *attention economy,* os utilizadores são manipulados para passar o máximo de tempo *online* em plataformas cujo modelo de negócio foca o lucro (Bennet e Livingston, 2018; Orlowski, 2020). Perspetivar esta tecnologia da persuasão a servir interesses políticos é especialmente preocupante, mas é inegável que a atual sobreabundância de conteúdos tanto pode influenciar em determinado sentido, como apenas confundir ou desviar a atenção, o que pode levar a fanatismos, mas também à desorientação, à desacreditação e ao total desinteresse pelo estado das coisas (Liedekerke e Zinkanell, 2020). De facto, se cada um passar a ter os seus factos, deixa de haver uma verdade e a necessidade de compromisso ou sequer de interação, crescendo a solidão e a alienação. Tal agrava a polarização social, as disputas entre grupos, a proliferação do racismo, etc., enfraquecendo a tolerância, a solidariedade, a coesão social, a segurança nacional e o próprio governo.
O declínio da credibilidade dos canais oficiais de notícias e a confusão gerada pelos não oficiais debilitam os processos de representação política e, consequentemente, o tecido social, alimentando a instabilidade e a vulnerabilidade da própria democracia. Nesta *post truth order,* em que os factos são menos relevantes para construir opiniões/tomar decisões do que as emoções, os estereótipos e as crenças pessoais (Wang, Rao e Sun, 2020, p. 14), importa notar que grupos com caraterísticas e experiências diferentes são expostos a informação diferente e afetados de forma díspar, sendo que este potencial para discriminação e abuso de poder evidencia como utópica a tese de que a internet constitui um acesso democrático a informação e oportunidades.

Dificuldades na Deteção

A prevalência das campanhas de desinformação, bem como o nível de exposição do público às mesmas são muito difíceis de quantificar. Apesar da reduzida evidência empírica, é indiscutível a existência em quantidade e influência ao ponto de distorcer o que é verdade e de impulsionar a dispersão de ideias marginais em plataformas e redes sociais com alcance global.
Algo que dificulta a deteção e a resposta à desinformação é o *deplatforming,* fenómeno mencionado por Rogers (2020) como o bloqueio de perfis por desrespeito de regras, normalmente seguido pela rápida transição dos mesmos para outras plataformas sem ou com menor moderação de conteúdos.
A deteção precoce de conteúdos desinformativos assume uma enorme importância para minimizar o número de pessoas influenciadas e, consequentemente, o dano

causado (Shu *et al.*, 2020), mas constitui um desafio especialmente complexo. Quanto a identificar quem é o agente, é discutido se será quem cria, quem publica ou quem partilha. Quanto a aferir a motivação, será altamente discutível num meio em que os agentes sociais são difíceis de identificar e cujo estudo aprofundado impõe evidentes limites éticos. De qualquer forma, será essencial rastrear os conteúdos, tentar bloquear as contas envolvidas ou diminuir o seu alcance. Também intervir na rede de disseminação parece relevante, tentando detetar os nódulos mais significativos e diminuir o ritmo da partilha e o potencial de influência. Adicionalmente, é possível incentivar os utilizadores a reportar conteúdos que suspeitem ser desinformação e, quando acima de determinado número de alertas, pressionar as plataformas a submeter a *fact-checking* e eventual remoção.
De salientar que importa estimular a Inteligência Artificial – *datamining, machine learning,* etc. –, a mesma que tornou possível meios de desinformação digital tão sofisticados como os *deepfakes,* os emuladores de voz, a escrita "falsa" que mimetiza figuras e plataformas conceituadas, a desenvolver formas de detetar de modo eficiente conteúdos desinformativos, gerar alertas, monitorizar e identificar os responsáveis.

Resposta

Os diferentes países têm tido respostas muito diversas à desinformação. No âmbito de um esforço inclusivo e colaborativo, Funke e Flamini (2020) elaboraram um mapa e um resumo do tipo de ação tomada por vários países, desde campanhas de literacia digital, constituição de *task forces* e elaboração de relatórios, passando por propostas de lei, investigação criminal, constituição de grupos de cibersegurança e de acordos entre o governo e empresas, até ameaças, detenções, bloqueios da internet, monitorização de *sites* e cobrança de impostos sobre as redes sociais, com grande disparidade no que toca à eficácia e ao impacto das mesmas nos direitos fundamentais.
Atendendo à dimensão transnacional da desinformação, ao seu impacto individual e coletivo e às dificuldades em identificar conteúdos desinformativos e os responsáveis pelos mesmos, estruturar uma resposta política eficiente implica integrar várias áreas profissionais e a sociedade civil, em estratégia compreensiva e coordenada a nível nacional, europeu e mundial, com especial incidência nos seguintes âmbitos:

Apostar na Educação/Literacia Digital

As condições educativas estão intimamente ligadas à literacia, tanto digital, como cívica e cultural, já que implicam a apreensão de referências que melhoram a experiência cognitiva e intelectual (Cardoso *et al.*, 2018b). Em particular, a Literacia Digital, a estratégia mais eficiente para combater a desinformação e o seu potencial de

manipulação inerente (Cardoso *et al.,* 2018b), deve incluir o conhecimento de como a informação é disponibilizada nas redes sociais e motores de busca, reconhecendo que há motivos pelos quais determinadas informações e notícias são apresentadas ou omitidas, e a capacidade de distinguir a informação através da verificação de factos. A investigação demonstra que a literacia informativa é a que mais contribui para a capacidade de identificar e não propagar conteúdos desinformativos (Jones-Jang *et al.,* 2019) e a sua aplicabilidade deve ser transversal a todas as faixas etárias para ter um impacto concreto.

Intimamente relacionada, refira-se a importância da consciência securitária na literacia digital com o objetivo de divulgar boas práticas no sentido de detetar riscos e de diminuir a exposição de dados. Como já referido, várias campanhas de desinformação usam a engenharia social – *honeypots* e *phishing* – para comprometer contas e perfis reais, que depois utilizam para promover a disseminação e credibilizar os conteúdos maliciosos (Liedekerke e Zinkanell, 2020). Paralelamente, conteúdos obtidos nestes ataques são reutilizados para campanhas de "malinformação", denegrindo e expondo potenciais setores estratégicos essenciais dos Estados.

Fortalecer entidades oficiais de notícias e instituições democráticas

Um dos grandes desafios da atualidade é como materializar o apoio à criação de uma imprensa independente cuja sustentabilidade económica não dependa apenas da interatividade que o seu conteúdo gera (Rimscha, 2016). Tal tornaria mais evidente a distinção entre os órgãos de comunicação social estabelecidos e os meios alternativos cujo foco é a rentabilidade do seu conteúdo e não o seu valor informativo. Esse apoio deve-se também traduzir numa regulação eficaz assente nos direitos, liberdades e garantias de um Estado democrático.

Paralelamente é essencial que as instituições democráticas se pautem por políticas de comunicação mais transparentes, acessíveis e adequadas às preocupações manifestadas pela sociedade civil. Essas preocupações são muitas vezes traduzidas em desinformação, pelo que importa acompanhar o discurso público nas redes sociais, providenciar informação oficial de forma proactiva, consistente, exata e nos momentos certos, para prevenir especulação não só na perspetiva de identificar antecipadamente narrativas desinformativas, mas também para construir adequadas contranarrativas.

Promover a ação das instituições: cooperação, regulamentação e legislação

Respostas eficientes dependerão sempre do conhecimento holístico do fenómeno da desinformação, sendo complexa a variedade de atores e de interesses envolvidos.

Por muito que diferentes entidades continuem a desenvolver esforços para compreender, detetar, sinalizar, monitorizar e responsabilizar a aplicabilidade e o sucesso das suas propostas, dependerá sempre do suporte ativo das empresas privadas, sobretudo da internet, da sua transparência e vontade de adaptação, regulação e responsabilização. As entidades oficiais devem promover ações de pressão junto destas empresas, cujo modelo de negócio é propício à divulgação e promoção de conteúdos sensacionalistas/manipulativos, com normas e leis que assegurem a liberdade de expressão e dificultem o seu uso como espaços de propagação de desinformação.

Elencados estes três campos de atuação essenciais, importará projetar esta análise na realidade portuguesa e, mais do que almejar neutralizar esta ameaça, focar a ação na redução do seu impacto, detetando vulnerabilidades da população e do país que propiciem a produção, disseminação e efeitos da desinformação, e concebendo respostas dirigidas e concertadas entre as diferentes áreas. Será também relevante detetar os fatores de proteção e reforçá-los, de modo a maximizar a impermeabilidade dos portugueses aos conteúdos desinformativos.

A Realidade Portuguesa

No contexto da realidade portuguesa e numa tentativa de identificar os fatores de risco quanto à influência da desinformação, optou-se por destacar três áreas de análise, que se encontram obviamente interligadas e que correspondem à população e literacia digital, à relação do cidadão com as instituições e à ação das instituições.

Para responder à complexa análise destas áreas, identificaram-se questões essenciais, variáveis de análise e obtiveram-se dados, recolhidos através de distintos organismos e por diferentes metodologias, com amostras e contextos espaço-temporais diversos, no quadro nacional e internacional. Apesar de se fazer uso de dados quantitativos, a parte empírica do presente artigo pretende formular uma análise essencialmente qualitativa que evidencie fatores de risco próprios da realidade portuguesa, num primeiro esboço agregador desta matéria. A importância estratégica da análise destes *weak signals* já é prática regular como ferramenta de suporte à decisão e tem utilidade comprovada (Mendonça *et al.*, 2012), não obstante, sofre críticas de fragmentação e continua a revelar dificuldade de afirmação no setor académico.

Seguem, para cada área, as questões de partida, as variáveis de análise e o levantamento de dados quantitativos e qualitativos considerados para gerar respostas preliminares.

Áreas de análise	Pergunta	Variáveis de análise	Exemplos
População e literacia digital	A população portuguesa tem caraterísticas e hábitos que a tornam vulnerável?	Idade, nível de educação, religiosidade, utilização da internet e das redes sociais, literacia digital, consciência dos riscos, cuidados *online*	Dados demográficos, dados sobre utilizadores da internet, Índice de Digitalidade da Economia e da Sociedade, Relatórios OBERCOM e inquéritos do Instituto Nacional de Estatística
Relação do cidadão com as instituições	A desinformação e a mensagem inerente de que não se deve confiar nas instituições oficiais têm influência? Que mobilização podem gerar?	Índices de intervenção cívica e política, índices de confiança nas notícias e nas instituições, absentismo	Consumo e interação com notícias, petições públicas, associativismo, confiança, European Social Survey
Ação das instituições	Que esforços estão a ser tomados para mitigar a desinformação em Portugal?	Investimento em programas de sensibilização, em núcleos de cooperação e investigação, relação com grupos empresariais, regulação, legislação	Iniciativas de literacia digital, legislação específica, programa de governo, Orçamento do Estado, projetos de financiamento, relatório anual de Segurança Interna

População e Literacia Digital

1. População e caraterísticas demográficas

Segundo o Instituto Nacional de Estatística (INE) (2020), Portugal mantém tendência de envelhecimento demográfico, verificando-se um aumento da idade mediana da população residente de 43,1 para 45,2 anos, entre 2013 e 2018. Quanto ao grau académico da população residente em Portugal com 15 ou mais anos em 2019, a maioria tinha o nível secundário e pós-secundário (PORDATA, 2020). Segundo o Eurostat (2020), a população idosa portuguesa continua a ter uma taxa de escolaridade baixa, abaixo da média europeia, e Portugal distingue-se como um dos países com maior disparidade digital entre faixas etárias.

Uma vez que é a população mais envelhecida que tem maior propensão para ser alvo de desinformação, por serem faixas etárias com menos educação e menos

literacia digital, os dados convergem e apontam para maior permeabilidade dos portugueses ao fenómeno (Loos e Nijenhuis, 2020).

Quanto à religião, Shu *et al.* (2020) referiram que indivíduos com crenças religiosas, ilusórias ou dogmáticas, que não se baseiam em factos científicos, têm menos probabilidade de desenvolver pensamento aberto e analítico, pelo que será de ter em conta que mais de 90% dos portugueses são religiosos, segundo o censo realizado em 2011 (INE, 2012). Ainda seguindo o mesmo estudo 7% declarou não ter religião e 4% afirmou ter religião diferente da católica.

Quanto à nacionalidade dos cidadãos estrangeiros a quem foi concedido título de residência e com estatuto de residente em Portugal (INE, 2020), a brasileira era, com enorme destaque, em 2018, a mais representativa. A produção de desinformação tem um custo, pelo que a existência de grandes audiências unidas pela afinidade linguística favorece a migração de conteúdo. Dado o enorme impacto reportado da desinformação nos resultados da última eleição presidencial no Brasil (Resende *et al.*, 2018) e a identificação de conteúdo desinformativo de origem no Brasil sobre a COVID-19 a circular em Portugal, sobretudo associados ao WhatsApp, será importante considerar o peso da comunidade como transmissora inconsciente de conteúdo e práticas desinformativas por proximidade cultural e linguística.

2. Comportamentos *online* e literacia digital

Segundo o INE (2019), mais de 76% da população residente em Portugal entre os 16 e os 74 anos utiliza a internet, apesar de esta percentagem ser inferior à média UE-28. Não obstante, a percentagem dos que participam em redes sociais é superior à média UE e tem vindo a subir. O acesso à internet em mobilidade tem registado níveis idênticos à média europeia e também mantém tendência de crescimento.

Quanto às práticas digitais dos cidadãos, de acordo com o Índice de Digitalidade da Economia e da Sociedade (IDES, 2020), Portugal encontra-se bem abaixo da média europeia no que concerne ao capital humano e uso de internet, que correspondem às capacidades e utilização eficiente da internet por parte dos utilizadores no dia a dia, contrapondo com valores bastante positivos na digitalização das instituições e das estruturas de comunicação e conectividade. Cerca de 23% dos portugueses nunca usaram a internet, num valor bem acima da média europeia de 11% (Rocha, 2020).

As taxas de utilização da internet são significativamente mais elevadas para as pessoas que completaram o Ensino Superior (98,7%) e para aquelas que concluíram o Secundário (96,9%). A proporção de utilizadores de internet diminui de forma acentuada com a idade, não obstante a proporção de utilizadores no grupo etário dos 55 aos 64 anos ser 59,3% e 34,1% para a população com 65 ou mais anos de idade, não deixando de ser significativa (INE, 2019).

O mesmo inquérito concluiu que as atividades mais realizadas na internet se relacionam com a pesquisa de informações sobre bens e serviços, comunicação por *e-mail,* leitura de notícias *online,* participação em redes sociais e visualização de vídeos em serviços de partilha.

Em termos de dispositivos, se, em 2019 (INE, 2019), o dispositivo mais utilizado para aceder a notícias era o computador (portátil/de secretária), depois o *smartphone,* TV e *tablet,* em 2020 detetou-se uma ultrapassagem definitiva do *laptop* pelo *smartphone* quer em termos de utilização geral quer como principal dispositivo para consumo de notícias (Cardoso *et al.,* 2020). A grande desvantagem desta mudança é que o smartphone, pelas caraterísticas do aparelho, dificulta a visualização e transição entre conteúdos, tornando mais complicada a verificação do que recebemos e favorecendo a partilha rápida e imediata, sem considerar a sua veracidade.

Quanto às redes sociais, o Facebook mantém o estatuto de preferido dos portugueses, seguido do YouTube, tanto em termos gerais como para aceder a notícias. Contudo, 76,1% dos inquiridos responderam incorretamente à questão sobre como os conteúdos são apresentados no Facebook, o que evidencia desconhecimento sobre a utilização dos algoritmos que decidem que conteúdos apresentar individualmente e que geram consequentemente as referidas *filtered bubbles* de informação (Cardoso *et al.,* 2020).

Tal como referido supra, destaca-se ainda a crescente utilização das aplicações de mensagens, sobretudo do WhatsApp, que têm assumido um papel preponderante no quotidiano digital dos portugueses, em parte devido à crescente preocupação com a privacidade, tanto para o seu propósito original de comunicação como também para partilha de conteúdos noticiosos (INE. 2019). A relevância das plataformas de mensagens instantâneas neste contexto é inegável por se tratarem de espaços encriptados onde não existe um moderador que remove conteúdo impróprio, onde o mesmo se pode tornar viral sem conhecimento dos visados e considerando a impossibilidade de reportar ou remover ao contrário das redes sociais. Estas plataformas trouxeram a hipótese de comunicar via áudio através de pequenos clips de voz, o que veio permitir à população iliterada participar nas partilhas de conteúdo em aplicações móveis, com impacto já visivelmente gravoso, nomeadamente em linchamentos públicos de inocentes na Índia (Garimella e Eckles, 2020) mas ainda pouco estudado. Mais perto, em Espanha, um estudo realizado no início de 2020 por Salaverría *et al.* (2020), com base em três plataformas de *fact-checking,* concluiu que a desinformação analisada foi sobretudo disseminada pelas redes sociais quando comparado com fontes oficiais, com destaque para a plataforma de WhatsApp. Essencialmente, os conteúdos desinformativos eram em formato texto, de proveniência nacional e subordinados a temas políticos.

Particularmente quanto à interação com notícias *online,* 43% dos inquiridos referiram ter reparado em títulos ou vídeos, mas não ter tido qualquer interação.

Percentagens maiores, 57% e 51%, referiram ter feito gosto/partilhado uma notícia e ter clicado no *link* para saber mais sobre ela. Dezassete por cento afirmaram ter publicado uma notícia ou participado numa discussão privada ou pública sobre determinada notícia (Cardoso *et al.*, 2018b).

3. Consciencialização de riscos e cuidados securitários

Apesar de a televisão ainda manter um lugar fundamental quanto à produção e receção de notícias, constata-se que as redes sociais têm crescido quanto ao acesso e à visualização e em termos de importância no quotidiano (Cardoso *et al.*, 2020). A seguir aos canais de 24 horas de informação, a maior parte dos inquiridos reportou ter visualizado notícias via redes sociais, seguido de programas de televisão e *websites* e *apps* de jornais (Cardoso *et al.*, 2018b). Ainda assim, quando questionados especificamente sobre as notícias nas redes sociais, os portugueses desconfiam mais destas do que de notícias com origem em instituições e marcas noticiosas (Cardoso *et al.*, 2018b). Tal revela consciência de que nem toda a informação que circula *online* é verdadeira e há preocupação em saber o que é real e falso na internet. Segundo o *Relatório Reuters* (Cardoso *et al.*, 2020), Portugal é o segundo país cujos cidadãos mais se preocupam com a legitimidade de conteúdos digitais, cerca de 75%. Adicionalmente, o último relatório da *International Association for the Evaluation of Educational Achievement* (Fraillon *et al.*, 2018), com amostra focada apenas nas camadas mais jovens, evidenciou que os jovens portugueses têm uma capacidade acima da média europeia de avaliar a qualidade da informação que consultam na internet.
Neste âmbito, durante as suas atividades *online,* os portugueses procuram proteger a sua identidade *online,* limitando, por exemplo, o acesso aos conteúdos pessoais nas redes sociais, verificando a segurança dos *sites* visitados e não autorizando a utilização dos seus dados para fins publicitários. Menos frequentemente solicitam a remoção de informação pessoal em posse dos motores de busca (Cardoso *et al.*, 2018a). Quanto ao tipo de dados partilhados, enquanto 80,6% dos portugueses estão abertos a partilhar nome ou data de nascimento, os dados que menos partilham *online* são os dados de contacto como o número de telemóvel ou a morada (apenas 30,9%).
Através do *Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias* (INE, 2019) apurou-se que mais de 1/4 dos utilizadores privados de internet (27,6%) detetaram problemas de segurança nos 12 meses anteriores, sendo o incidente mais reconhecido o *phishing.* Por outro lado, 49% dos utilizadores de internet referiram ter limitado atividades na internet devido a preocupações com a segurança, principalmente em relação ao fornecimento de informação pessoal em redes sociais ou profissionais – 32,6% dos internautas –, na compra de produtos ou serviços (26%),

nas atividades bancárias (22,8%) e aquando do *download* de ficheiros (22,6%). Os portugueses com idades entre os 25 e os 34 anos e aqueles com estudos superiores são os que mais tendem a reconhecer que sofreram incidentes de segurança durante o uso da internet, facto que evidencia maior risco para a população mais envelhecida e com estudos inferiores. De facto, o Centro Nacional de Cibersegurança (2020) apurou que tanto os indivíduos como as empresas em Portugal, em 2019, reconheceram menos que sofreram incidentes de cibersegurança comparativamente com a UE.

A Relação do Cidadão com as Instituições: Confiança e Mobilização

Apesar da desconfiança acima reportada revelada quanto às notícias apresentadas nas redes sociais, os portugueses têm elevados níveis de confiança nas notícias e instituições noticiosas públicas e privadas em geral. No relatório elaborado por Cardoso, Paisana e Pinto Martinho (2020), numa parceria entre OberCom – Observatório da Comunicação ISCTE-IUL Media Lab e Reuters Institute for the Study of Journalism, Portugal destaca-se no conjunto dos 40 mercados analisados, como o país onde mais se confia em notícias a par da Finlândia.

Esta elevada confiança dos portugueses de que as instituições noticiosas divulgam informação íntegra, precisa e honesta contrapõe-se com a sua relação com as instituições governamentais, nomeadamente os órgãos políticos e de justiça. De facto, pequenos estudos pontuais têm apontado que os portugueses confiam na grande maioria das instituições oficiais, na investigação científica e nos *media* tradicionais, não sucedendo o mesmo com as estruturas de governação política (European Social Survey, 2018a; European Social Survey, 2018b). Esta ideia parece corroborar os trabalhos já realizados sobre a caraterização da desinformação em Portugal, cujos dados empíricos apontam para uma prevalência de temas associados à corrupção e uma menor presença de temas xenófobos como temas virais no conteúdo desinformativo que circula nas redes sociais portuguesas (Cardoso *et al.*, 2019).

Além do sentimento de confiança, importará perceber como se mobilizam os portugueses no que toca ao que consomem na internet. Através do INE (2019), apurou-se que quase 25% dos utilizadores de internet terão tido uma intervenção cívica ou política na internet: 17% terão publicado opiniões ou comentários e 15,4% terão participado em consultas ou votações para a decisão de questões cívicas ou políticas. É interessante salientar que esta proporção, embora tenha reduzido quanto a 2017, mantém-se superior ao registado para a UE-28. Até que ponto esta mobilização *online* tem correspondência no mundo real de forma a conduzir os portugueses a levar a cabo ações concretas decorrentes do impacto dos conteúdos desinformativos visionados e poderá constituir uma ameaça? Recentes protestos contra as medidas restritivas aplicadas pelo governo no âmbito da pandemia da COVID-19 resultaram de

iniciativas de páginas e grupos de Facebook em que circulam conteúdos que contestam a utilidade das máscaras, a segurança dos testes e o valor sanitário das medidas. Em Portugal têm surgido nestas manifestações várias dezenas de pessoas, enquanto noutros países iniciativas equivalentes têm juntado milhares.

Como mencionado supra, a confusão criada pelos canais não oficiais de notícias e a diminuição da autoridade dos oficiais gera dúvida e instabilidade, que podem afetar valores-base e a capacidade de raciocínio. Se a nível individual tal pode desorientar, manipular e alienar, à escala coletiva pode fragilizar os processos de representação política, a coesão social e a tolerância, propiciando conflitos e divisões e mesmo contestação e resistência às forças e serviços de segurança, às Forças Armadas e ao governo, o que põe em causa a Segurança Nacional e o funcionamento democrático da sociedade.

Neste âmbito, entende-se que, além da relação entre os portugueses e os media em geral, importa cuidar a relação dos mesmos com as instituições estatais que consubstanciam o último reduto da segurança, da lei e da ordem, com profissionalismo e transparência, para minimizar os efeitos da desinformação na sua imagem, autoridade e valor.

A Ação das Instituições: Investigação, Sensibilização e Legislação

As instituições nacionais têm procurado acompanhar aquilo que são as diretrizes europeias e de desenvolvimento sustentável das Nações Unidas. Tem havido um forte investimento no acesso mais democrático à internet e na digitalização das infraestruturas, que se têm revelado no IDES (2020). No entanto, a nível da literacia digital, pese embora o investimento nas camadas mais jovens, há ainda um longo caminho a percorrer na formação da restante população, sobretudo nas zonas rurais e nas classes sociais mais desfavorecidas, grupos demográficos que correspondem exatamente aos que menor confiança demonstram nas instituições (Coelho, 2017; Gil, 2019). Esta dicotomia resulta numa vulnerabilidade acrescida, visto que o desenvolvimento tecnológico das estruturas administrativas não é acompanhado pela formação dos quadros a operar nas mesmas e dos seus utilizadores.

As iniciativas de investigação e as campanhas de sensibilização e os projetos existentes têm resultado na sua maioria de financiamento europeu, num quadro mais macro do projeto europeu, como o INCoDe.2030 e existem poucas e descentralizadas referências exclusivamente nacionais de apoio institucional de combate e estudo da desinformação, de campanhas de sensibilização e de investimento em literacia digital. Os projetos existem, mas muitas vezes falta a materialização final para chegar aos grupos que dela mais necessitam, focando-se sobretudo na prestação de serviços digitais e menos na criação de uma cultura digital que atenue em vez de reforçar

desigualdades entre os dois grupos (Aires *et al.*, 2018; Gomes, 2019; Gil, 2019). Do ponto de vista da criação de fundos e núcleos de investigação, não se conhece até ao momento nenhum projeto exclusivo sobre esta matéria a nível nacional.

Em termos legais, existe ainda um significativo atraso em acompanhar o desenvolvimento do setor tecnológico, pese embora uma recente recomendação de aplicação de algumas medidas do quadro europeu (Resolução de Assembleia de República, n.º 50/2019). A regulamentação das plataformas dificilmente seria viável num quadro nacional e decorrem de momento iniciativas europeias nesse sentido, como o *Digital Services Act*, mas não deixa de ser relevante destacar a forte discrepância entre as medidas legais vigentes em Portugal e a relevância que estas desordens informativas têm no quotidiano dos portugueses.

Muitas vezes a desinformação materializa-se em campanhas de difamação pessoal, ou encontra-se associada a outros fenómenos de desordem informativa como o *revenge porn*[1] ou o *doxxing*,[2] e no uso de ferramentas como sistemas automáticos de propaganda e perfis privados, todos eles ainda não regulados do ponto de vista legal e alguns com impacto profundo a nível pessoal. A impunidade com que muitas vezes estes fenómenos se alastram no espaço virtual, com enorme dificuldade por parte das instituições competentes em garantir a aplicabilidade da lei, resulta numa crescente descredibilização das instituições, agravando as vulnerabilidades elencadas anteriormente.

Tanto o Centro Nacional de Cibersegurança (2020), como o *Relatório Anual de Segurança Interna* (RASI) respeitante a 2019 (Sistema de Segurança Interna, 2020) documentaram um aumento dos crimes/denúncias relacionados com a informática, sem que seja possível discernir até que ponto se relacionam com a disseminação de conteúdos que consubstanciem desinformação.

Também o governo português quer no seu Programa quer no Orçamento do Estado determina estratégias que deverão ser aplicadas de forma valorizar a cibersegurança. Importará perceber se tais destaques oficiais se refletem ou não no investimento concreto em capital humano, além de tecnológico, formado para este tipo de averiguações, projetos e iniciativas.

Conclusão

O presente artigo procurou efetuar um enquadramento da atual problemática da desinformação, focando alguns dos fatores facilitadores da sua propagação com o objetivo de promover respostas eficazes de mitigação do problema. Nesse sentido,

1 A publicação não consensual de imagens íntimas obtidas no foro de um momento privado.

2 Divulgação propositada de dados privados sobre uma entidade com o objetivo de a prejudicar.

destacaram-se três áreas de análise. No âmbito da primeira área da análise, as caraterísticas da população como consumidora e propagadora de desinformação, destacou-se a importância da literacia digital, sobretudo nas camadas menos jovens, através de uma maior consciencialização do funcionamento da internet e dos seus riscos, ao invés de um foco apenas na digitalização dos serviços do Estado, esperando uma aprendizagem quase autodidata dos utilizadores através da necessidade de aprendizagem, o que acentua desigualdades e não promove o uso consciente da internet, contribuindo para o aumento do número de utilizadores da plataforma que têm dificuldades em compreender os seus riscos, nomeadamente a desinformação.

Num segundo plano de análise, a relação desta população com as estruturas oficiais, nomeadamente o Estado e a Comunicação Social, é essencial compreender como a desconfiança nas instituições, as preocupações latentes e o medo do desconhecido promovem um terreno fértil à desinformação. No panorama atual em que figuras de relevo atacam diariamente e descredibilizam agências noticiosas, o termo *fake news* não só se banalizou como acaba por minar a confiança em fontes fidedignas e comprometer a passagem de mensagens importantes. O comprometimento dos atuais modelos de negócio dos grandes grupos de imprensa reduziu a qualidade informativa e conduziu ao crescimento do *clickbait* e da produção de conteúdo em massa. Assim, o fortalecimento de uma imprensa independente assente num modelo económico menos permeável às regras de capitalização do conteúdo *online* impõe-se como um dos primeiros passos essenciais.

Paralelamente, as instituições democráticas devem pautar-se pela transparência, correspondendo e incentivando ações da sociedade civil que questionem as suas decisões e processos de trabalho, com uma comunicação acessível, clara e verificável. Adicionalmente, importa criar estratégias de acompanhamento mais regular de conteúdo sobre os principais eixos estratégicos democráticos, a fim de identificar antecipadamente narrativas desinformativas, estudar as preocupações latentes em que se sustentam e construir contranarrativas nos princípios elencados supra.

No último plano de análise, destacou-se a importância da regulamentação e da proatividade institucional em mitigar algumas das vulnerabilidades identificadas nos dois pontos anteriores. É essencial um maior investimento em investigação multidisciplinar sobre as macro e micro realidades em que a desinformação surge, numa abordagem prática que compreenda as narrativas subjacentes e os agentes sociais que permitiram a sua propagação. Uma legislação que exija uma maior responsabilidade das plataformas é também fulcral para garantir que a aplicabilidade das leis não termina na passagem para o virtual e que, dessa forma, não é minada a confiança das vítimas nas instituições.

Transversalmente aos fatores referidos, importa destacar o momento vivido mundialmente que poderá ter um efeito particularmente potenciador da desinformação.

A pandemia da COVID-19 pode ser considerada um período de crise, como mencionado por Shu *et al.* (2020), marcada pela ansiedade, medo e incerteza, fatores que propiciam a procura e aceitação de informação não oficial, não confirmada, para obter alguma resposta e assim algum alívio da tensão e da falta de controlo sentidas. A maior instabilidade e a menor capacidade de raciocínio crítico consubstanciam vulnerabilidades que potenciam a influência da desinformação.

Transposta esta reflexão para a realidade portuguesa, identificaram-se fatores que manifestam maior vulnerabilidade, o que visa informar decisores e promover medidas no sentido de os colmatar. Segue quadro agregador dos fatores identificados como fatores de risco/vulnerabilidades, fatores neutros e fatores de proteção, de forma a antecipar e delinear respostas sustentadas ao fenómeno da desinformação.

Fatores de Risco/Vulnerabilidades	**Fatores Neutros**	**Fatores de Proteção**
Tendência de envelhecimento da população	Aumento do acesso à internet em mobilidade	Frequência do ensino superior a crescer
Prevalência do nível de Ensino Secundário e Básico	Percentagem maior que a da UE no que toca a intervenção cívica e política *online*	São os jovens e população com maior nível de ensino quem mais utiliza a internet
População maioritariamente religiosa	Incidentes de cibersegurança podem ou não relacionar-se com disseminação de conteúdos desinformativos	Televisão mantém papel central na visualização de notícias
Facilidade de migração de conteúdo desinformativo		Confiança nas notícias em geral, mas desconfiança quanto às apresentadas nas redes sociais
Aumento acelerado dos utilizadores da internet, também nas faixas etárias mais vulneráveis		Preocupação em distinguir real de falso
Grande percentagem de utilizadores das redes sociais		Preocupação com dados partilhados *online*
Aumento da utilização das redes sociais e das *apps* de mensagens para aceder a notícias		Limitação de atividades *online* para evitar incidentes de cibersegurança
Facebook é a rede preferida e os utilizadores tendem a desconhecer algoritmos de seleção dos conteúdos		Confiança nas instituições oficiais e de investigação científica

Fatores de Risco/Vulnerabilidades	Fatores Neutros	Fatores de Proteção
Aumento da utilização do *smartphone* em geral e para aceder a notícias		Investimento na digitalização de infraestruturas
Aqueles entre os 25 e os 34 anos e com estudos superiores são os que mais reconhecem incidentes de cibersegurança		Iniciativas e campanhas de sensibilização, sobretudo decorrentes do âmbito UE
Os portugueses reconhecem menos que a média UE quando sofrem incidentes de cibersegurança		Programa de Governo e Orçamento do Estado salientam cibersegurança e ciberdefesa
Desconfiança nos órgãos políticos e de justiça		RASI destaca e alerta para a desinformação
Literacia digital desigual na população		
Iniciativas e campanhas de sensibilização pouco materializadas e adequadas		
Atraso da regularização de setores *online*		
Aumento do número de crimes relacionados com a informática/ /invasão de privacidade, de denúncias e de condenados		
Imprensa economicamente frágil e dependente da viralização de conteúdo para sobrevivência		

O quadro supra pretende traduzir a realidade da permeabilidade à desinformação, que se evidencia desfasada, com um evidente desenvolvimento de determinados setores e um atraso significativo relativamente a outros pontos. Destaca-se a importância de reconhecer os fatores de proteção como casos de sucesso e replicar as *lessons learned* de forma a fazer face aos fatores de vulnerabilidade. Um maior desenvolvimento desta avaliação de risco, no sentido de focar outros países e as respetivas realidades nacionais, concebendo modelos específicos de intervenção para cada variável, surge como uma potencial proposta para seguimento do presente trabalho.

Bibliografia

Aires, L., Santos, R., Guardia, J., Lima, C. e Correia, J. (2018). Mediating towards digital inclusion: the monitors of internet access places. *Observatorio (OBS*) Journal 12*(2): 196-213. http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-59542018000200012

Assembleia da República (2019). Resolução da Assembleia da República n.º 50/2019. *Diário da República* n.º 66/2019, Série I de 2019-04-03: 1826-1826. https://dre.pt/web/guest/pesquisa/-/search/121942395/details/maximized

Avramov, K. (2018). By Another Way of Deception: The Use of Conspiracy Theories as a Foreign Policy Tool in the Arsenal of the Hybrid Warfare. *Information & Security: An International Journal 39* (2): 151-161. https://doi.org/10.11610/isij.3913

Bayer J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A. e Uszkiewicz, E. (2019). *Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States.* European Parliament. LIBE Committee, Policy Department for Citizens' Rights and Constitutional Affairs. https://ssrn.com/abstract=3409279or http://dx.doi.org/10.2139/ssrn.3409279

Bennett, W. e Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication 33* (2): 122-139.

Bradshaw, S. e Howard, P. (2019). *The Global Disinformation Disorder:2019 Global Inventory of Organised Social Media Manipulation.* Working Paper 2019.2. Oxford, UK: Project on Computational Propaganda. http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Cardoso, G., Baldi, V., Pais, P., Paisana, M., Quintanilha, T. e Couraceiro, P. (2018b). *As* Fake News *numa Sociedade Pós-Verdade. Contextualização, potenciais soluções e análise*. OberCom. https://obercom.pt/wp-content/uploads/2018/06/2018-Relatorios-Obercom-Fake-News.pdf

Cardoso, G., Narciso, I., Moreno, J. e Palma, N. (2019). *Online Desinformation During Portugal's 2019 Elections.* MEDIALAB & Democracy Reporting International. https://democracy-reporting.org/wp-content/uploads/2019/10/Portugal-First-Post-Election-Report-Social-Media-2019.pdf

Cardoso, G., Paisana, M. e Pinto-Martinho, A. (2020). *Digital News Report 2020 Portugal.* OberCom — Reuters Institute for the Study of Journalism. https://obercom.pt/wp-content/uploads/2020/06/DNR_PT_2020_19Jun.pdf

Cardoso, G., Paisana, M., Quintanilha, T. e Pais, P. (2018a). *Literacias na Sociedade dos Ecrãs.* OberCom. https://obercom.pt/wp-content/uploads/2018/03/OberCom2018-Literacias-na-Sociedade-dos-Ecra%CC%83s.pdf

Centro Nacional de Cibersegurança. (2020). *Relatório Cibersegurança em Portugal. Riscos e Conflitos.* Observatório de Cibersegurança. https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2020__observatoriocibersegurança_cncs.pdf

Coelho, A. (2017). *Os seniores na sociedade em rede: dinâmicas de promoção da inclusão e da literacia digitais em Portugal.* CIES e-Working Papers 213/2017. http://hdl.handle.net/10071/14535

European Social Survey. (2018a). *Media and Social Trust* (Core – all rounds). https://www.europeansocialsurvey.org/data/themes.html?t=media

European Social Survey. (2018b). *Justice and fairness* (ESS9 2018). https://www.europeansocialsurvey.org/data/themes.html?t=justfair

Eurostat. (2020). *Ageing Europe – statistics on social life and opinions.* https://ec.europa.eu/eurostat/statistics-explained/index.php/Ageing_Europe_-_statistics_on_social_life_and_opinions#Education_and_digital_society_among_older_people

Fraillon, J., Ainley, J., Schulz, W., Friedman, T. e Duckworth, D. (2018). *Preparing for Life in a Digital World. IEA International Computer and Information Literacy Study 2018 International Report.* The International Association for the Evaluation of Educational Achievement. http://iave.pt/images/FicheirosPDF/Estudos_Internacionais/ICILS/ICILS_2018_Relat%C3%B3rioInternacional.pdf

Funke, D. e Flamini, D. (2020). *A guide to anti-misinformation actions around the world.* POYNTER. https://www.poynter.org/ifcn/anti-misinformation-actions/

Garimella, K. e Eckles, D. (2020). Images and Misinformation in Political Groups: Evidence from WhatsApp in India. *The Harvard Kennedy School Misinformation Review 1* (5).

Gil, H. (2019). A literacia digital e as competências digitais para a infoinclusão: por uma inclusão digital e social dos mais idosos. *Revista de Educação a Distância e Elearning 2* (1): 79-96. http://hdl.handle.net/10400.11/6490

Gomes, M. (2019). *O eGovernment em Portugal: literacia digital e dificuldades de difusão de políticas públicas.* Tese de doutoramento. Lisboa: ISCTE-IUL. http://hdl.handle.net/10071/19551

Goode, E. e Ben-Yehuda, E. (2009). *Moral Panics: The Social Construction of Deviance* (2.ª edição). Wiley Blackwell.

Hansen, F. (2017). *Russian hybrid warfare: A study of disinformation.* Danish Institute for International Studies, report 06. http://hdl.handle.net/10419/197644

Índice de Digitalidade da Economia e da Sociedade de 2020. Portugal. (2020). Comissão Europeia. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66950

Instituto Nacional de Estatística (2019). *Sociedade da Informação e do Conhecimento – Inquérito à Utilização de Tecnologias da Informação e da Comunicação pelas Famílias – 2019.*

Instituto Nacional de Estatística (2020). *As Pessoas 2018.*

Instituto Nacional de Estatística. (2012). *Censos 2011. XV Recenseamento geral da população. V Recenseamento geral da habitação. Resultados Definitivos. Portugal.*

Jones-Jang, S., Mortensen, T. e Liu, J. (2019). Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don't. *American Behavioral Scientist.*

Liedekerke, A. e Zinkanell, M. (2020). Deceive and Disrupt: Disinformation as an emerging cybersecurity challenge. *AIES Studies 13.* https://www.aies.at/download/2020/AIES-Studies-2020-13.pdf

Loos, E. e Nijenhuis, J. (2020). Consuming Fake News: A Matter of Age? The Perception of Political Fake News Stories in Facebook Ads. In: Gao Q., Zhou J. (eds) *Human Aspects of IT for the Aged Population. Technology and Society.* HCII 2020. Lecture Notes in Computer Science, vol 12209. Springer, Cham.

Mendonça, S., Cardoso, G., Caraça, J. (2012). The strategic strength of weak signal analysis. *Futures* 44 (3): 218-228.

Nielsen, R. e Graves, L. (2017). *"News you don't believe": Audience perspectives on fake news.* Reuters Institute for the Study of Jounalism. https://ora.ox.ac.uk/objects/uuid:6eff4d14-bc72-404d-b78a-4c2573459ab8

Organização Mundial de Saúde (2020). *Novel Coronavirus (2019-nCoV) Situation Report-13.* https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf?sfvrsn=195f4010_6

Orlowski, J. (Director) (2020). *The Social Dilemma* (Documentary). Netflix.

Paisana, M., Pinto-Marinho, A. e Cardoso, G. (2020). Trust and fake news: Exploratory analysis of the impact of news literacy on the relationship with news content in Portugal. *Communication & Society* 33 (2): 105-117.

Pariser, E. (2011). *The Filter Bubble: What The Internet Is Hiding From You.* Penguin Books.

PORDATA. (2020). População residente com 15 e mais anos: total e por nível de escolaridade completo mais elevado. https://www.pordata.pt/Portugal/Popula%C3%A7%C3%A3o+residente+com+15+e+mais+anos+total+e+por+n%C3%ADvel+de+escolaridade+completo+mais+elevado-2101

Resende, G., Messias, J., Silva, M., Almeida, J., Vasconcelos, M. e Benevenuto, F. (2018). *A System for Monitoring Public Political Groups in WhatsApp. WebMedia '18: Proceedings of the 24th Brazilian Symposium on Multimedia and the Web:* 387-390.

Rimscha, M. (2016). Business Models of Media Industries: Describing and Promoting Commodification. In *Managing Media Firms and Industries:* 207-222.

Rocha, C. (2020). Governo lança plano estratégico para "acelerar" Portugal no mundo digital. *Dinheiro Vivo,* 5 de março. https://www.dinheirovivo.pt/economia/governo-lanca-plano-estrategico-para-acelerar-portugal-no-mundo-digital-12687321.html

Rogers, R. (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication* 35(3): 213-229. https://doi.org/10.1177/0267323120922066

Salavérria, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I. e Erviti, M. (2020). Desinformación en tempos de pandemia: tipologia de los bulos sobre la Covid-19. *El profesional de la información 29* (3). https://doi.org/10.3145/epi.2020.may.15

Shu, K., Bhattacharjee, A., Alatawi, F., Nazer, T., Ding, K., Karami, M. e Liu, H. (2020). Combating Disinformation in A Social Media Age. *Wires Datamining and Knowledge Discovery 10* (6). https://doi.org/10.1002/widm.1385

Sistema de Segurança Interna (2020). *Relatório Anual de Segurança Interna 2019*.

Tandoc Jr., E., Lim, Z. e Ling, R. (2018). Defining "Fake News". A typology of scholarly definitions. *Digital Journalism 6*(2): 137-153. https://doi.org/10.1080/21670811.2017.1360143

Tiffen, R. (2019). Moral Panics. In H. Tumber e S. Waisbord (Eds.), *The Routledge Companion to Media and Scandal*. Routledge.

Waltzman, R. (2017). *The weaponization of information.* https://www.armed- services.senate.gov/imo/media/doc/Waltzman_04-27-17.pdf

Wang, M., Rao, M. e Sun, Z. (2020). Typology, Etiology, and Fact-Checking: A Pathological Study of Top Fake News in China. *Journalism Practice.*

Wardle, C. e Derakhshan, H. (2017). I*nformation Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.* https://rm.coe.int/information-disorder--toward-an-interdisciplinary-framework-for-researc/168076277c

Wardle, C. e Derakhshan, H. (2018). Thinking about "information disorder": formats of misinformation, disinformation, and malinformation. In I. Cherilyn e J. Posetti (Eds.), *Journalism, fake news & disinformation: handbook for journalism education and training:* 44-56. https://unesdoc.unesco.org/ark:/48223/pf0000265552