UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

CURSO DE RELAÇÕES INTERNACIONAIS

ISABELA REGINA MELO DE SANTANA

O PROCESSO DE SECURITIZAÇÃO DAS FAKE NEWS: O REINO UNIDO NA PANDEMIA DE COVID-19

JOÃO PESSOA

2022

ISABELA REGINA MELO DE SANTANA

O PROCESSO DE SECURITIZAÇÃO DAS FAKE NEWS: O REINO UNIDO NA PANDEMIA DE COVID-19

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Relações Internacionais pela Universidade Federal da Paraíba.

Orientador: Prof. Dr. Augusto Wagner Menezes Teixeira Júnior.

JOÃO PESSOA

2022

Catalogação na publicação
Seção de Catalogação e Classificação

S232p Santana, Isabela Regina Melo de.
O processo de securitização das fake news : O Reino Unido na pandemia de Covid-19 / Isabela Regina Melo de Santana. - João Pessoa, 2022.
50 f.

Orientação: Augusto Wagner Menezes Teixeira Júnior.
TCC (Graduação) - UFPB/CCSA.

1. Securitização. 2. Segurança. 3. Pandemia. 4. Fake news. 5. Reino Unido. I. Teixeira Júnior, Augusto Wagner Menezes. II. Título.

UFPB/CCSA CDU 327

Elaborado por ANDRE DOMINGOS DA SILVA FERNANDES - CRB-15/00730

ISABELA REGINA MELO DE SANTANA

O PROCESSO DE SECURITIZAÇÃO DAS FAKE NEWS: O REINO UNIDO NA PANDEMIA DE COVID-19

Trabalho de Conclusão de Curdo apresentado ao Curso de Relações Internacionais do Centro de Ciências Sociais Aplicadas (CCSA) da Universidade Federal da Paraíba (UFPB), como requisito parcial para obtenção do grau de bacharel (a) em Relações Internacionais.

Aprovado(a) em, 12 de dezembro de 2022

BANCA EXAMINADORA

Prof. Dr. Augusto Wagner Menezes Teixeira Junior – (Orientador)
Universidade Federal da Paraíba - UFPB

Prof. Dr. Túlio Sérgio Henriques Ferreira
Universidade Federal da Paraíba - UFPB

Prof. Dr. Marcos Alan Shaikhzadeh Vahdat Ferreira
Universidade Federal da Paraíba - UFPB

AGRADECIMENTOS

Agradeço a Deus por sempre cuidar de mim e não poderia deixar de agradecer à minha família, minha mãe Joselita, meu pai Reginaldo e meu irmão Caio, por todo o apoio,vocês são o que há de mais importantes para mim.

Além disso, agradeço ao meu orientador, Augusto Teixeira, e aos meus professores da graduação, pelos ensinamentos e por serem uma inspiração para mim e meus colegas. Agradeço aos meus amigos, à Isabella, que fiz amizade desde o primeiro período da graduação e me acompanha até hoje, e às minhas amigas, Bianca e Maria Eduarda, por sempre me escutarem. Como também aos demais amigos da UFPB e de fora dela, os quais não citarei os nomes para não deixar de mencionar nenhum. Não poderia deixar de homenagear neste trabalho a Líderi e o GEESI, pelas experiências adquiridas para além da sala de aula. Meus agradecimentos às minhas avós, Conceição e Luzinete, e aos demais entes queridos, aos professores da escola e curso que me fizeram chegar nesse momento e cada um que de alguma forma torna meu dia melhor.

RESUMO

A Era da informação modificou as relações humanas após a década de 1980 e os avanços tecnológicos impactaram todos os setores da sociedade. Nesse sentido, o espaço cibernético surge como um novo e importante domínio para a segurança nacional e internacional e com ele, novas ameaças passam a desafiar os Estados. Em um contexto de crise, como da Pandemia de Covid-19, esses riscos se tornam mais evidentes e pressionam as autoridades a elaborar estratégias para enfrentá-los. Com isso, este trabalho visa estudar o movimento de securitização das *fake news* no Reino Unido no contexto da pandemia. Por meio de pesquisa qualitativa descritiva e exploratória, pretende-se fazer o uso da discussão da literatura sobre securitização para entender o cenário que levou a esse processo, como os agentes da política transformaram essa questão em um assunto de segurança e quais as medidas tomadas. Além disso, serão feitas considerações no tocante à percepção da população sobre essa nova ameaça.

Palavras-chave: securitização; segurança; pandemia; *fake news*; Reino Unido.

ABSTRACT

The Information Age changed human relations after the 1980s and technological advances impacted all sectors of society. In this sense, cyberspace emerges as a new and important domain for national and international security and with it, new threats begin to challenge States. In a context of crisis, such as the Covid-19 Pandemic, these risks become more evident and pressure authorities to devise strategies to face them. With this, this work aims to study the fake news securitization movement in the United Kingdom in the context of the pandemic. Through descriptive and exploratory qualitative research, it is intended to use the discussion of the literature on securitization to understand the scenario that led to this process, how policy agents turned this issue into a security issue and what measures were taken. In addition, considerations will be made regarding the population's perception of this new threat.

Keywords: securitization; safety; pandemic; fake news; United Kingdom.

SUMÁRIO

1 INTRODUÇÃO

A evolução tecnológica não apenas contribuiu para o desenvolvimento de novos aparelhos militares, mas também ampliou a definição de segurança. Em constante adaptação, a segurança adquiriu uma face mais complexa e transversal (CASTELLS, 2001).

Até as últimas décadas do século XX, os Estados buscavam operar em apenas quatro domínios físicos: a terra, o mar, o ar e o espaço sideral. Mas a década de 1990 marcou a emergência de estudos sobre um novo domínio: o ciberespaço (KUEHL, 2009). A criação da Internet modificou drasticamente a comunicação e facilitou a realização de diversas atividades humanas. Contudo, esse novo domínio apresentou novas ameaças à segurança dos Estados. O espaço virtual permitiu o aumento de diversos tipos de atividades delituosas como vírus e outras formas de código malicioso, que são frequentemente difundidos via rede global, o que destacou a necessidade de securitização do espaço cibernético, inclusive sua militarização (HJALMARSSON, 2013).

Atualmente, existem certas restrições (por exemplo, alianças, paridade militar e etc.) que impedem que Estados lancem hostilidades diretamente uns contra os outros. Com isso, a guerra indireta é a única opção para desestabilizar o adversário. Os chamados conflitos de quarta geração são mais fluidos, descentralizados e assimétricos do que as guerras do passado, correspondendo, portanto, ao estilo não convencional. Desse modo, marca-se a ênfase na guerra da informação e em operações psicológicas. Em vez de atacar diretamente os alvos em seu próprio território, os países utilizam as mídias sociais e tecnologias afins como um substituto às munições de precisão guiadas tal qual armas de “ataque cirúrgico” (KORYBKO, 2018).

Com o avanço da tecnologia no século XXI, as formas convencionais de conflito parecem menos atrativas por impor aos países limites e custos para o envolvimento em um conflito direto. Desse modo, o ambiente cibernético mostra-se uma alternativa propícia ao surgimento de diferentes formas de ameaça interna e externa, de modo que, é essencial para os Estados exercerem domínio sobre esse meio, com o objetivo de garantir a própria segurança (PORTELA, 2018).

Nessa esfera, a importância de estudar o processo de securitização das *fake news* se dá pois o próprio tema pressupõe o potencial ameaçador da propagação de notícias falsas à soberania do Estado. A desinformação, no contexto da pandemia iniciada em 2020, conseguiu desestabilizar sociedades e romper com a harmonia social. Além disso, a securitização de uma questão política dá credibilidade à necessidade de medidas urgentes e de mobilização de recursos para conter um suposto revés. Entretanto, além da emergência de ameaças no ciberespaço, como vírus e malwares, este ambiente tem sido utilizado com fins de afetar a opinião pública e governos através da manipulação de informações, muitas das quais conhecidas como fake news.

Essa tendência tornou-se evidente com o surgimento da pandemia de Covid-19 (*Coronavirus disease*), já que os últimos dois anos mostraram como informações falsas podem ser usadas para suscitar desconfiança, minar a ciência e ameaçar a vida. O constante uso do espaço cibernético para uma vasta gama de atividades sociais, econômicas, políticas e militares provocou alta dependência desse meio. Dessa forma, pessoas e governos tornam-se vulneráveis a fatores culminantes de insegurança e desestabilização nesse domínio.

O ambiente cibernético apresenta-se como um meio propício à disseminação de *fake news*. Características particulares desse domínio, tais quais anonimato, facilidade de ações e difusão de informações de maneira rápida, falta de barreiras físicas e pouca regulamentação evidenciam vulnerabilidades do Estado. Nesse contexto, as Fake News tornam-se uma arma não-cinética mais poderosa do que as tradicionais armas cinéticas e passam a se manifestar como potencial ameaça à segurança nacional em diversos países.

Em resposta a essa realidade, países como o Reino Unido tem ampliado suas capacidades de ação contra a desinformação, de modo que as *fake news* passaram a integrar o palco das discussões políticas e a se apresentar como um possível desafio à segurança do país. Tendo em vista esse contexto, potencializado pela pandemia de Covid-19, tem-se por problema de partida: “Como ocorreu o entendimento das *fake news* como ameaça à segurança britânica no contexto da pandemia?” A hipótese é de que a crise da pandemia de Covid-19 levou à aceleração do processo de securitização das *fake news*. Nesse sentido, partindo da teoria da securitização, o objetivo deste trabalho consiste em explicar como as *fake*

news passaram a ser entendidas como uma ameaça à segurança do Reino Unido. Nota-se, assim, que o estudo é voltado para analisar como o Estado, o ator securitizador para esta pesquisa, identifica o problema e age para construir uma narrativa que proponha o entendimento dessa questão como uma ameaça real.

Desse modo, o caso escolhido para entender o processo de securitização no meio online sob o contexto da pandemia foi o do Reino Unido por possuir um movimento securitizador claro, a partir de uma dimensão que utiliza a capacidade estatal e as forças armadas para lidar com o problema das *fake news.* Outrossim, o país reagiu rapidamente na pandemia através de políticas públicas em combate à desinformação e possui narrativas que evidenciam o desafio representado pelas notícias falsas.

O presente trabalho caracteriza-se essencialmente como uma pesquisa qualitativa descritiva e exploratória. Com isso, o Desenho de Pesquisa utilizado é um Estudo de Caso, o qual conta com análises de discursos e com uma metodologia baseada em três níveis de análise desenvolvidos por Balzacq (2010). Nesse sentido, o primeiro nível concentra-se nos atores e nas relações desempenhadas por eles. Em segundo lugar, serão analisadas as práticas e instrumentos, tais como a linguagem e recursos linguísticos. Por fim, será estudado o contexto e como o discurso adapta-se à ele.

Para examinar a dimensão de ciberespaço e a esfera informacional será utilizada a definição de Espaço Cibernético elaborada por Kuehl (2009), bem como as características descritas por Choucri (2012). A fim de obter um melhor entendimento desse domínio a partir da Teoria Realista serão aplicadas, essencialmente, as ideias de Kremer e Muller (2014), assim como Herz (1950) e Waltz (2002), sendo possível, portanto, compreender a condição de anarquia observada no ambiente cibernético. Tratando-se, enfim, dos desafios apresentados pelo espaço cibernético para a Segurança serão introduzidas as perspectivas de Sheldon (2012) e Nye (2008).

Além disso, se faz o uso da literatura de Klein e Wueller (2017), bem como Wardle e Derakhshan (2017), com o intuito de conceituar as *fake news* e distinguir os tipos de desordem de informação existentes. O trabalho também centra-se nas Teorias de Securitização formuladas por Buzan, Waever e Wilde (1998) e por Balzacq (2010) para compreender a securitização e seu encadeamento com a

pandemia. Ademais, se utiliza técnicas de análise de discurso a fim de verificar a presença da narrativa securitizadora nas falas de autoridades e documentos britânicos. No final, são apresentados dados, com o objetivo de verificar os resultados e inferir o sucesso ou fracasso da securitização.

Para isso, o estudo está dividido em 3 seções principais. A primeira visa compreender o espaço cibernético e contextualizar o ambiente em que age a possível ameaça. Desse modo, é trabalhado o conceito de ciberespaço, suas características, a abordagem teórica realista e os desafios para a segurança cibernética.

Alcançado o entendimento do espaço operacional em que se encontra a possível ameaça, é introduzido o tema da securitização. Nesta parte, são apresentadas duas visões distintas: a teoria proposta pela escola de Copenhague e a teoria de Balzacq. Em sequência, é justificada a escolha da abordagem utilizada nesta pesquisa. Em um segundo momento, é realizado considerações sobre a conceituação das *fake news* e analisada a sua capacidade de gerar consequências reais à sociedade, especialmente em situações de crise, como a pandemia.

A terceira seção, então, contextualiza a tentativa governamental de enquadrar as *fake news* como uma ameaça à segurança do Reino Unido e explica o desenvolvimento desse processo na pandemia. Para maior detalhamento, faz-se uma análise de discursos de autoridades britânicas a respeito do tema e das medidas tomadas pelo Governo do Reino Unido. Finalmente, são apresentados os resultados da securitização das *fake news* no plano britânico e averiguado o sucesso ou falha da securitização, a partir de dados da percepção dos civis acerca das notícias falsas.

2 ESPAÇO CIBERNÉTICO

A redução dos custos com tecnologia permitiu o ciberespaço tornar-se um meio acessível para um contingente maior de pessoas e uma fuga dos estresses cotidianos. Isso, em consonância com a sofisticação e diversificação dos aparelhos eletrônicos e com a facilidade de criar conexões em um ambiente livre de barreiras geográficas, marcam a tendência de uma transição do mundo físico para o virtual. Logo, o ciberespaço ganhou uma importância significativa à medida que praticamente todas as atividades tradicionais, sejam elas, sociais, políticas, institucionais, financeiras, de lazer e de trabalho realizadas por indivíduos, pelo Estado, empresas e Instituições, dependem cada vez mais do ambiente *online*. Contudo, apesar dos benefícios oferecidos pela internet, ela também apresenta novos perigos aos países e suas populações.

Esse capítulo tem por objetivo: 1) introduzir o conceito de espaço cibernético, bem como suas características e atores; 2) expor a visão realista a respeito desse domínio e 3) apresentar os desafios do ciberespaço à segurança nacional. Dessa forma, não se busca fazer uma análise técnica de aspectos referentes à Ciência da computação, mas utilizar o estudo desse domínio para avançar na discussão posterior sobre a utilização desse meio para a propagação de notícias falsas.

2.1 CONCEITO, CARACTERÍSTICAS E ATORES DO ESPAÇO CIBERNÉTICO

O termo “ciberespaço” ou “espaço cibernético”[1] ainda não tem uma definição globalmente aceita. Após fazer um levantamento de diversas definições utilizadas por instituições, empresas e autores, Kuehl (2009) elabora uma definição para o Ciberespaço:

> [...] um domínio global dentro do ambiente de informação cujo caráter distinto e único é enquadrado pelo uso da eletrônica e do espectro eletromagnético para criar, armazenar, modificar, trocar e explorar informações por meio de redes interdependentes e interconectadas usando tecnologias de informação e comunicação. (KUEHL, 2009, p. 4, tradução nossa)

[1] Para uma perspectiva distinta sobre o conceito de cibernética, ver Deutsch (1982).

A abordagem de Kuehl (2009) evidencia que apesar de ser amplamente utilizado como sinônimo de internet, o conceito de ciberespaço é mais complexo. Desse modo, a rede, os computadores e as informações digitais são elementos que compõem o espaço cibernético e tornam possível a interação humana nesse meio.

Essa definição é complementada pela descrição de *Cyberworld* como sendo qualquer realidade virtual contida em uma coleção de computadores e redes (DUGGAN; PARKS, 2012). Existem muitos mundos dentro do espaço cibernético, mas o mais relevante para este trabalho é a Internet.

Torna-se essencial, também, explicitar as diferentes camadas contidas no ciberespaço. Segundo o Plano de capacidade do conceito de operações ciberespaciais (ESTADOS UNIDOS DA AMÉRICA, 2010), enquanto o elemento físico compreende todos os componentes eletrônicos necessários para que a máquina funcione, a infraestrutura (cabeada, sem fio e óptica) dá suporte à rede e os conectores físicos (fios, cabos, radiofrequência, roteadores, servidores e computadores), o aspecto geográfico, por sua vez, compete a localização física dos elementos da rede, formando a primeira camada.

A segunda camada é a lógica, a qual abarca o componente de natureza técnica e corresponde às conexões lógicas que existem entre os dispositivos conectados a uma rede de computadores, denominados de “nós”. Por último, a camada social refere-se aos aspectos humanos. O componente *persona* é o sujeito que realmente está por trás daquela rede, já *cyber persona* é a identificação desse indivíduo na rede, como por exemplo, um endereço de e-mail. Ou seja, essa camada consiste no indivíduo sendo representado na *web*, por meio de uma ou mais *cyber personas* (ESTADOS UNIDOS DA AMÉRICA, 2010).

Esses são aspectos de importante conhecimento do Estado para a contenção de possíveis ameaças. Conhecer o espaço cibernético e suas camadas permite que essas ameaças sejam localizadas e que ações possam ser tomadas para a garantia da segurança neste domínio.

O surgimento de situações de insegurança no espaço cibernético se deve em grande medida às próprias características desse ambiente. Como visto anteriormente, o ciberespaço é um domínio singular. A combinação de elementos físicos e virtuais o fazem apresentar desafios diferentes dos já enfrentados em outros meios como terra, mar, ar e espaço sideral.

Essas características são importantes para o entendimento do espaço e dos fatores propulsores da insegurança, tais quais: **temporalidade**, capacidade de alterar a noção de tempo das pessoas, devido à velocidade com que as informações são trocadas; **fisicalidade**, o espaço cibernético não apresenta barreiras geográficas e não é necessário mudar de ambiente físico para que se possa divulgar informações; **permeação**, torna possível a infiltração em jurisdições e o rompimento de barreiras virtuais; **fluidez**, a capacidade de constante mutação; **participação**, permite o aumento da quantidade de pessoas que podem participar dos debates políticos; **atribuição**, existência de áreas de difícil detecção de atores malignos e **responsabilidade**, por ser complicado detectar agentes criminosos, torna-se impraticável responsabilizar esses indivíduos (CHOUCRI, 2012).

Nesse sentido, a temporalidade gera a instantaneidade com que as informações são passadas. Essa característica não é novidade dos aparatos tecnológicos atuais, mas o volume de informações hoje transmitidas a torna difícil de ser desconsiderada. A fisicalidade, por sua vez, provoca o efeito global da internet, viabilizando que as ameaças venham de ambientes externos. Além disso, o anonimato acaba por ser um fator que gera obstáculos à atribuição e responsabilização dos indivíduos, que podem se esconder por trás de sua *cyber persona*.

Para além das características citadas, é possível destacar os baixos custos financeiros que esse meio fornece, tanto para o acesso cotidiano da sociedade quanto para a própria atuação nociva.

Outro fator relevante desse meio é a sua multiplicidade de atores, tendo em vista que o ciberespaço propicia poucas barreiras para o acesso de novos agentes. Os usuários de redes podem ser indivíduos, organizações, grupos transnacionais ou até entidades nacionais (KUEHL, 2009). Contudo, com relação ao poder, os Estados obtêm maior vantagem nesse meio, pelos recursos, programas, treinamentos e relacionamentos disponibilizados. Além disso, entidades estatais detêm legalidade para o uso da força (BARNARD-WILLS; ASHENDEN, 2012).

No contexto da pandemia de Covid-19, observou-se distintos atores operando na crise a fim de espalhar desinformação, *fake news* e propaganda. Grande parte dessas ações são premeditadas e contém estratégias usadas em guerras psicológicas e de informação. Atores estatais, como a Rússia, empregam

um amplo espectro dessas abordagens de maneira notavelmente sofisticada. Sua forma de conduzir o conflito depende em grande medida de campanhas deliberadas de desinformação, combinadas com as ações das agências de inteligência. Com isso, ela tem por objetivo confundir o inimigo, bem como obter uma vantagem estratégica dentro das restrições orçamentárias da Rússia (RODARI, 2021).

Essa tendência foi identificada pela Otan (2020), a qual evidencia que os meios de comunicação, controlados pelo governo russo, como Sputnik ou RT (Russia Today), usaram uma estratégia de misturar notícias falsas com fatos reais para espalhar desinformação.

Assim como a Rússia, a China também foi acusada de contribuir para o cenário visto durante a pandemia:

> A China (uma potência global em crescimento) explorou as oportunidades geoestratégicas apresentadas pela crise global. Para a China, a desinformação e a dissimulação parecem servir a um propósito geopolítico estratégico mais amplo. Tendo sido (provavelmente) a fonte do COVID-19, ela parece ter emergido mais rapidamente da pandemia. Como tal, a campanha de informação dela parece basear-se em uma postura diplomática mais assertiva (ou seja, diplomacia “Wolf Warrior”), exploração de um mundo distraído para atingir ou avançar objetivos territoriais. (REDING; WELLS, 2022, p. 36, tradução nossa)

Além de países, grupos criminosos têm enxergado na pandemia uma oportunidade de obter vantagens. Enquanto os governos estão voltados para questões emergentes de segurança, economia e saúde, provocadas pela crise, grupos não estatais, como o ISIS (Islamic State of Iraq and Syria), declaradamente veem a pandemia global como uma oportunidade para enfraquecer ainda mais seus inimigos (BASSOU; TOBI, 2021).

Dessa forma, se demonstra os diferentes atores que podem compor o espaço cibernético. Vale destacar que, esse trabalho não visa responsabilizar sujeitos ou entidades a respeito da disseminação de notícias falsas, mas mostrar que tanto Estados, quanto grupos e indivíduos podem se aproveitar do contexto e das características do espaço cibernético para adquirir vantagens sobre eventuais inimigos.

Nesse sentido, dois aspectos importantes para a teoria realista ajudam no entendimento sobre a necessidade de garantia da segurança nesse meio, são eles: a anarquia e o Estado. Sob o ponto desta tradição teórica, o ambiente anárquico

torna a guerra uma condição latente e por isso os Estados devem se preocupar com a própria segurança para a sobrevivência. Sendo assim, investir em instrumentos militares de defesa possui um dever essencial na condição de anarquia (HERZ, 1950; FELICIANO, 2018).

Segundo Waltz (2002), a anarquia constrange os Estados a prezar pela própria segurança, estabelecendo relações de equilíbrio de poder entre si e definindo os meios e os fins de suas ações no ambiente internacional.

Além disso, o preceito realista do sistema internacional é encontrado também no ambiente cibernético. Segundo Kremer & Müller (2014, p.163)

> O espaço cibernético é um domínio artificialmente criado de informações e trocas econômicas. Como no caso das relações internacionais, o espaço cibernético é caracterizado pela condição de anarquia, a ausência de uma autoridade central.

Logo, a falta de uma governança central e a carência de regulamentação o tornam um ambiente fértil para riscos à soberania estatal. Faz-se necessário, então, que os Estados formulem estratégias com o objetivo de garantir o controle militar desse domínio. Dessa maneira, o Reino Unido, por exemplo, lançou em fevereiro de 2022 o documento que regula a Estratégia Nacional Cibernética (United Kingdom, 2022), com fins de estabelecer políticas e estratégias para aumentar suas capacidades no espaço cibernético.

Embora enfatizem apenas as formas tradicionais de poder, alguns autores realistas consideram o campo cibernético como um novo domínio operacional para a atuação dos Estados, em que estes deveriam projetar cada vez mais poder e ganhar mais influência em comparação com outros Estados (ACÁCIO; SOUZA, 2012).

Assim, por apresentar vulnerabilidades que oferecem riscos à segurança estatal, o ciberespaço é um ambiente que propicia a busca dos Estados por poder, tanto para ataque quanto para defesa, a fim de garantir sua preservação.

2.2 DESAFIOS PARA A SEGURANÇA CIBERNÉTICA

Percebe-se que as características do ciberespaço o tornam um ambiente de difícil manutenção da segurança. Além disso, o sistema livre e anárquico único da Internet pode representar um perigo em vez de uma oportunidade. Conforme

Schons (2007), diante da extensa quantidade de informações, a *Internet* sofreu impactos e a diminuição da capacidade de controle da ordem, tornando-se anárquica, inconsistente e caótica, manifestando o caos informacional visto atualmente.

Segundo Sheldon (2011), o espaço cibernético propicia o ataque em detrimento da defesa e isso se dá por um conjunto de fatores. Primeiro, as ações defensivas contam com um baixo aparato regulatório em um universo sem fronteiras e a filosofia de defesa cibernética atual busca principalmente identificar ameaças, mas encontra óbices para diminuir as fragilidades que as causaram. Além disso, as ações ofensivas só precisam ter sucesso uma vez para causar prejuízos, enquanto a defesa precisa ser constante[2]. Pela falta de barreiras geográficas, o invasor pode estar em qualquer lugar do globo e torna-se difícil conter uma ameaça quando não se localiza o alvo, desafiando, assim, a defesa do Estado.

É notório que, apesar das vantagens estatais de desfrutar de poder, recursos e legitimidade para o uso da força, o exercício de defesa da esfera cibernética requer um esforço maior por parte de suas entidades militares do que por parte dos invasores. Segundo Araújo Jorge (2012), no ciberespaço, a ação ofensiva é mais rápida e barata do que a ação defensiva. Tal fato favorece o crescimento do número de invasores e tipos de crimes cibernéticos.

Uma abordagem para o desenvolvimento de ações defensivas por parte do Estado para proteger-se de ataques adversários é elaborada por Feliciano (2018):

> A Defesa Cibernética, para ser concretizada, requer que o Estado possua capacidade de atuação no espaço cibernético, isto é, desenvolva poder cibernético [...] de modo a garantir a proteção das infraestruturas críticas e sistemas militares, além de favorecer os Estados na realização de seus objetivos. (FELICIANO, 2018, p. 38)

Com efeito, o desenvolvimento de poder cibernético garante com que estratégias e ações mais eficazes sejam realizadas e alvos achem-se detectados e contidos. Contudo, os danos causados não competem apenas aspectos físicos.

Os governos tendem a se atentar sobretudo para os ataques de *hackers* à infraestrutura de tecnologia da informação de seu próprio aparato burocrático, entretanto existem fragilidades sociais que vão muito além dos aparelhos eletrônicos

[2] Essa condição se relaciona com a característica de temporalidade, que foi apresentada anteriormente (p.13).

do governo (NYE, 2008). Essas vulnerabilidades tornam-se ainda mais latentes em contextos de crise. No capítulo seguinte, abordaremos um desses problemas, o qual emergiu em meio ao surto de Covid-19 nos anos de 2020 e 2021.

3 SECURITIZAÇÃO E *FAKE NEWS*

A securitização é tanto uma teoria como um campo de estudo da denominada Escola de Copenhague representada por autores como Buzan, Waever e Wilde (1998). Para as abordagens realistas, os desafios de segurança e ameaças são tradicionais, como a guerra, corrida armamentista e terrorismo, por exemplo. Contudo, a teoria de securitização permite entender como são selecionados os problemas de segurança e que quando bem-sucedida, a securitização pode levar a mudanças na política.

Nesse sentido, desenvolvimentos na tecnologia *online* e digital proporcionam vantagens e auxílios expressivos para a sociedade. Contudo, eles também abriram espaços para que informações falsas encontrassem novas maneiras de se disseminar com facilidade. O potencial que as *fake news* possuem de causar danos não se dá unicamente por sua natureza inverídica, mas também por sua capacidade de se misturar com a realidade, afetando, portanto, o discernimento das pessoas de separar fatos reais e fictícios. Dessa maneira, os indivíduos acabam por tomar decisões que não teriam tido em caso de não exposição a essa informação.

Em vista disso, esse capítulo tem o intuito de: 1) apresentar o conceito de securitização por meio da teoria elaborada pela Escola de Copenhague e a definição alternativa de Thierry Balzacq como representante dos estudiosos da segunda onda e esclarecer a definição escolhida para esse trabalho, 2) fomentar o debate acerca do conceito de *fake news* e estabelecer sua relação com o poder e 3) apresentar alguns dados sobre a percepção da população a respeito das *fake news*.

3.1 REVISÃO DE LITERATURA (SECURITIZAÇÃO)

A Escola de Copenhague ampliou os estudos de segurança ao trazer pela primeira vez o tema da securitização. Para os precursores da Escola, Buzan, Wæver e Wilde (1998), a securitização acontece quando um ator apresenta uma questão como um problema de segurança. Sendo assim, essa questão deixa de ser apenas política e passa a ser assunto de interesse militar.

Isto posto, uma ameaça[3] é detectada quando se mostra capaz de causar um infortúnio considerável. Nesse sentido, o conceito de ameaça é caracterizado por se tratar de um risco à existência do objeto referente, especificamente. Nos casos dos setores político e militar trata-se de ameaças à existência do Estado, como é apresentado no realismo, por sua vez, no caso do setor social refere-se a algo que compromete a existência de um determinado grupo, sendo os três casos relacionados à sobrevivência.

Logo, a securitização é, para os autores, uma versão extrema da politização, de maneira que a prática da securitização vai variar de Estado para Estado, já que cada um irá elencar qual problema será considerado como ameaça existencial. A análise da securitização não pressupõe indicadores, pois, conforme a Escola de Copenhague, o mecanismo que os atores utilizam é a fala. Assim, a securitização, para obter sucesso, não pode ser imposta, e os seus agentes devem apropriar-se de argumentos para conseguir o consentimento do público sobre a ameaça por ele manifestada, sendo por meio desse exercício que se verifica o sucesso do processo.

Concomitantemente, são necessárias três etapas para a securitização: 1) ameaças existenciais; 2) ação de emergência e 3) efeitos nas relações por libertar-se das regras. De forma que, a percepção da ameaça implica em uma ação por parte do Estado, bem como uma mudança na sociedade, tornando a securitização uma construção social.

Outra característica da securitização é que ela é intersubjetiva, segundo os teóricos desse fenômeno:

> Nosso argumento é que a securitização, assim como a politização, deve ser entendida como um processo essencialmente intersubjetivo. Mesmo que alguém quisesse tomar uma abordagem mais objetivista, não está claro como isso poderia ser feito, exceto em casos em que a ameaça é inequívoca e imediata. (BUZAN; WÆVER; WILDE, 1998, p. 31, tradução nossa)

Essa perspectiva destoa das abordagens de segurança que até então destacavam seu caráter objetivo, ou seja, enfatizavam a existência de ameaças reais. Para Waltz (1959), o fenômeno da guerra, por exemplo, resulta do egoísmo inerente ao ser humano e é, portanto, inevitável. Para os autores da Escola de

[3] Para uma ampliação da discussão sobre ameaça e securitização, ler Viana e Silva (2013).

Copenhague, a securitização é determinada pelos atores dentro de uma comunidade política.

A Escola de Copenhague, ainda, tem como noção importante o objeto de referência, de forma que os estudos de securitização precisam compreender o ator (quem), as ameaças (quais questões) e os objetos de referência (para quem). O objeto é quem sofre a ameaça e para o qual as medidas urgentes serão tomadas pelo decisor, sendo normalmente representado pelo Estado. Não obstante, é preciso atentar-se sobre quais condições a securitização acontece e qual seu resultado, visto que, um processo bem-sucedido implica na aceitação do público-alvo e na não discordância por parte dos mesmos das medidas tomadas.

Contudo, uma das críticas levantadas por Huysmans (1998) a essa abordagem de Copenhague é que, não há uma distinção clara entre o que se encaixa dentro de um assunto de segurança e o que não se enquadra. Esse fator abre espaço para que muitas questões sejam classificadas como problema de segurança de forma indevida.

Nesse contexto, Balzacq (2010, p. 13) define securitização como sendo “[...] um conjunto de práticas inter-relacionadas, e os processos de sua produção, difusão e recepção que trazem ameaças”. Dessa forma, ele elabora uma visão mais ampla do processo que abrange contexto, circunstância, público e orador.

A segunda onda de estudiosos não entende a securitização simplesmente pela ótica da fala, de maneira que existem três atos transmitidos por fala. O primeiro ato é o locutório, a transmissão de uma mensagem. Por outro lado, os atos ilocucionários possuem a finalidade de adquirir convencimento de um público-alvo para a realização de uma determinada ação. Já os atos perlocucionários, são os efeitos consequentes, que têm o objetivo de modificar a visão que o público tem sobre uma questão específica (BALZACQ, 2005).

Em vista disso, uma das críticas de Balzacq à Escola de Copenhague é a concentração dessa perspectiva apenas nos atos ilocucionários. Para ele, a segurança deve ser pragmática e não resumida a um procedimento.

Nessa esfera, os estudos de securitização devem gerar suposições teóricas sobre intersubjetividade, contexto e práticas (BALZACQ, 2010). Para isso, ele parte de três pressupostos: 1) a centralidade da audiência; 2) a codependência de agência e contexto; 3) a força estruturante do dispositivo.

A primeira suposição é de que para que uma questão seja considerada securitizável, um público que tenha interesse na questão e que seja capaz de permitir que o ator securitizador tome medidas que concordem com as reivindicações desse ator. Logo, para obter um efeito perlocucionário, o orador deve sintonizar sua linguagem com a experiência do público, em falas, gestos e recursos visuais.

Por sua vez, o segundo pressuposto cria uma relação entre a linguagem e o conhecimento adquirido entre circunstâncias, anteriores e atuais, dessa forma, o discurso possui a capacidade de modificar o contexto. O agente securitizador precisa escolher o momento certo para que o público chegue a uma percepção estruturada comum de uma possível ameaça.

O terceiro pressuposto é que a securitização ocorre por meio de um conjunto de práticas subjetivas. Essas práticas normalmente são implementadas por meio de ferramentas de política, como por exemplo, os instrumentos regulatórios, que conseguem influenciar os comportamentos dos atores sociais, possibilitando, assim, que certas práticas reduzam a ameaça. Além disso, ferramentas de capacitação são utilizadas para impor disciplina externa a indivíduos e grupos sociais.

As duas abordagens teóricas, a Escola de Copenhague e a alternativa da segunda onda liderada por Balzacq (2010), concordam em alguns pontos fundamentais da segurança, mas representam modelos distintos de securitização. Os teóricos de Copenhague trouxeram contribuições importantes para o âmbito da segurança ao introduzir o conceito de securitização. Além disso, essa abordagem é bem fundamentada para analisar se um assunto é securitizado ou não e avaliar os impactos desse processo na sociedade. Entretanto, ao buscar entender o contexto em que ocorreu a securitização, a teoria de Balzacq mostra-se mais adequada para esse trabalho.

Na metodologia escolhida para essa pesquisa, Balzacq (2010) foca em três níveis de análise. Desse modo, ele não se concentra simplesmente nos agentes, mas também em atos e no contexto. No primeiro nível de análise encontram-se os atores, tanto aqueles favoráveis à securitização quanto os resistentes, as relações de poder entre eles, o objeto de referência e o sujeito de referência. O segundo nível de análise engloba as práticas, discursivas ou não, a linguagem, suas figuras e

recursos linguísticos, bem como os instrumentos para o processo. Enfim, o terceiro nível é o contexto, já que as ameaças surgem em uma determinada circunstância e o discurso é adaptado contextualmente, portanto, a análise deve situar-se socialmente e historicamente. O terceiro nível de análise, especialmente, será essencial para o capítulo posterior deste trabalho.

3.2 *FAKE NEWS*: CONCEITO E EMPREGO COMO INSTRUMENTO DE PODER

A despeito do fenômeno de falsificação política por meio da distorção de fatos e informações não ser uma prática nova, pouca atenção foi dada à análise conceitual. Nesse sentido, a emergência da expressão *fake news* no léxico político foi relevante para recolocar o tema na agenda. Conforme Quirós (2017), em meio ao cenário jornalístico dos últimos anos, as *fake news,* que em outros momentos poderiam ser chamadas de rumores, propagandas ou sátiras, causam impacto pela ampla divulgação e por encontrar uma audiência receptiva. Dessa forma, essas notícias têm ganhado força na sociedade através da legitimidade fornecida por aqueles que as compartilham.

Contudo, o termo *fake news* tem sido utilizado pela mídia para referir-se à propaganda enganosa, notícias fabricadas com o intuito de prejudicar a confiança em instituições, sites e páginas com diversos objetivos que misturam ficção e realidade e vídeos disseminados por civis com interesses particulares. Da mesma forma, políticos frequentemente usam a mesma terminologia para se referir às coberturas midiáticas que veiculam informações contrárias ao seu viés ideológico, sendo assim, o uso dessa terminologia de forma indiscriminada para designar distintos fenômenos dificultam a realização de análises com rigor acadêmico.

Nesse sentido, Wardle e Derakhshan (2017) abordam os três tipos de desordem da informação que servirão para o entendimento da abrangência do termo *fake news*, de modo que,cada uma das formas de desinformação se encaixa entre dois espectros: falsidade e dano (figura 1). O primeiro tipo presente no espectro da falsidade abrange as informações falsas criadas sem o intuito de causar prejuízo. Já o segundo, representa as informações falsas criadas de forma deliberada para prejudicar uma pessoa, grupo social, organização ou país e se enquadra na

interseção entre falsidade e dano. Por último, a informação maliciosa é baseada na realidade e usada para infligir prejuízo a uma pessoa, organização ou país e por isso encontra-se no segundo espectro.

Figura 1 – Diagrama de Venn da desordem informativa

Elaboração própria, de acordo com Wardle e Derakhshan (2017, p. 20).

Ainda conforme os autores, a desordem da informação passa por três fases: a criação, produção e distribuição. Nessas fases, é possível identificar os agentes, que podem ser oficiais ou não, com motivações financeiras, políticas, sociais ou psicológicas e participam das três etapas da desordem, seja de forma organizada, com o intuito de causar prejuízos, ou não.

Além disso, a mensagem é um elemento importante nesse processo, pois pode assumir formas e durações distintas de acordo com o intuito dos agentes e seu público-alvo, seja em texto ou oral, no formato de vídeo, imagem ou gráficos, por exemplo. Enfim, os receptores de informações normalmente não são passivos. Cada indivíduo que constitui uma audiência[4] possui status sociocultural, posições políticas

[4] Segundo Balzacq (2010), a audiência, para a Teoria de Securitização visa garantir a aprovação moral e formalizar o consentimento para que se efetue a securitização. De modo que, ela não é previamente estabelecida, mas funciona como uma categoria que se manifesta concomitantemente

e experiências pessoais e, assim, interpretam as informações de acordo com sua experiência.

Diante disso, há uma linha tênue entre desinformação e *fake news*. No entanto, a primeira possui o agravante de propositalmente disseminar a informação, na tentativa de causar confusão e afetar decisões e pessoas (AQUINO, 2021). Essa intenção é confirmada pela definição presente no Livro Branco de Danos *Online* do Governo britânico para a desinformação, como sendo a informação criada ou difundida com a intenção deliberada de enganar (UNITED KINGDOM, 2019a).

Nesse panorama, as notícias falsas são formações que imitam o conteúdo da mídia noticiosa em sua forma, mas não no processo organizacional ou na intenção, de modo que, os veículos disseminadores carecem de normas e processos editoriais que garantam a veracidade e credibilidade da informação (LAZER *et al*., 2018).

Uma outra definição é dada por Klein e Wueller (2017), como sendo a publicação *online* de declarações falsas de fatos. Contudo, é imprescindível o cuidado com definições abrangentes. Nesse caso, Gelfert (2018) chama atenção para o aspecto do alcance da notícia para que seja considerada *fake news:*

> Para que uma alegação seja considerada notícia falsa, ela deve de fato enganar um público relevante – embora o tamanho exato de uma audiência dependa do caso em questão – e deve fazê-lo em virtude da maneira como foi projetada para passar-se como notícia (pelo menos para o público-alvo relevante). (GELFERT, 2018, p. 103)

Desse modo, um erro cometido por um veículo com credibilidade que não espalhou falácias e afetou a opinião de uma grande quantidade de pessoas não se encaixa dentro da nomenclatura.

Ademais, outro conceito amplamente utilizado como sinônimo de *fake news* surgiu com a eclosão da pandemia de Covid-19. A palavra infodemia ganhou destaque nos recentes debates e significa o aumento no volume de informações relacionadas a um assunto específico, as quais podem se multiplicar em pouco tempo devido a um evento específico. Nesse contexto, as redes sociais são o meio para a disseminação de informações inverídicas como um vírus (ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE, 2020).

---

aos atores securitizadores em uma dinâmica intersubjetiva sobre quais contextos irão securitizar um determinado objeto de referência.

Logo, é comum que infodemia, desinformação e *fake news* sejam confundidas e que a utilização do último termo seja alvo de muitas críticas por autores atuais, principalmente devido a banalização e o uso indevido do mesmo.

Embora não exista consenso entre os autores e que haja muitas controvérsias acerca da intencionalidade do agente que fabrica *fake news*, o termo será utilizado nesse trabalho para se referir ao processo final de criação, produção e disseminação de notícias falsas, sem a checagem ou normas editoriais que tragam credibilidade à informação. Esse processo ocorreu por diferentes agentes, intencionais, em sua criação, como políticos e empresas com intuito de causar prejuízos, e não intencionais, pessoas que disseminaram as informações por terem sido vítimas desse processo.

Entender essa abordagem conceitual é imprescindível para que se possa avançar na discussão do porque as *fake news* tornaram-se uma ameaça à população britânica. De modo que elas podem ser vistas também como um instrumento de poder.

Nessa esfera, o poder é um assunto chave para os estudos de relações internacionais e ciência política. Conforme Robert Dahl (2001), o poder compreende na capacidade de conseguir que outra pessoa faça alguma coisa que anteriormente não seria feita. Em consonância, Morgenthau (2003) utiliza a definição desse elemento como a habilidade estatal de influenciar ou compelir outros Estados a agirem de uma maneira específica ou desistir de uma ação. Essas duas definições revelam a característica de influência do poder, em que, por meio de seu emprego, são tomadas decisões que resultam em uma determinada ação, elemento importante para esse trabalho, visto que abordaremos o poder cibernético.

Nessa esfera, Joseph Nye (2002) divide o poder em duas formas: o *soft power* e o *hard power*. A primeira consiste em compelir o outro a realizar seus interesses sem o uso da força, por meio da influência, cultura e política. A segunda, pelo contrário, se utiliza do poder coercitivo, sanções e forças militares para que o outro faça a sua vontade.

Com efeito, o poder cibernético concentra-se na criação, controle e comunicação de informações de computadores ou qualquer meio eletrônico e possui a capacidade de afetar muitos outros domínios (NYE, 2010).

Sendo assim, Nye apresenta três faces do poder no domínio cibernético:

Quadro 1 – Faces do Poder Cibernético

1° face	*Hard Power*: ataques de negação de serviço, inserção de *malware*, interrupções SCADA, prisões de blogueiros	*Soft Power*: campanhas de informação para modificar as preferências iniciais dos *hackers*, recrutamento de membros de organizações terroristas
2° face	*Hard Power*: *firewalls*, filtros e pressão sobre as empresas para excluir algumas ideias	*Soft Power*: ISPs e mecanismos de busca, se automonitorar, regras da ICANN sobre nomes de domínio, padrões de software amplamente aceitos
3° face	*Hard Power*: ameaças de punir blogueiros que divulgam material censurado	*Soft Power*: informação para criar preferências (por exemplo, estimular o nacionalismo e "*hackers* patrióticos"), desenvolver normas de repulsa (por exemplo, pornografia infantil)

Elaboração própria, de acordo com Nye (2010).

É possível observar que existem aspectos de *hard* e *soft power* nas três faces evidenciadas. A primeira é a capacidade de um ator convencer outros a fazerem algo contrário às suas próprias preferências. Por outro lado, a segunda face do poder é a definição de agenda ou a exclusão das estratégias, de maneira que pode ser legítimo (*soft power*) ou forçado (hard *power*). A terceira face, então, engloba a mudança das preferências iniciais de um ator por outro, para que ele não considere seguir determinada estratégia.

Dessa forma, as *fake news* constituem um mecanismo de inserção de informações por meio do espaço cibernético, de modo que adquiriram a capacidade de moldar o comportamento dos indivíduos. Nesse sentido, elas encontraram na internet um ambiente favorável para induzir a opinião pública. Essa última pode ser definida como resultado provisório da competição de discursos que têm lugar na esfera pública (Maia, 2008).

O poder sob domínio do ator capaz de moldar a opinião pública se dá porque além de fazer com que diferentes indivíduos pensem e atuem da mesma maneira, é possível alterar a agenda do Estado, visto que, a interação entre a

sociedade civil e os líderes de opinião, que se influenciam mutuamente, é a causa da agenda pública em nível nacional (SABĂU; ION; NEAG, 2016).

A opinião pública é um dos mais importantes fatores para a complexa formulação da agenda que irá nortear as prioridades e as decisões dos agentes políticos. Desse modo, os agentes disseminadores de informação em meios de comunicação adquirem a capacidade de interferir nas estratégias de agentes políticos. À vista disso, a pandemia foi o palco do disparo maciço de informações falsas para alcançar agendas políticas específicas.

3.3 DADOS SOBRE A PERCEPÇÃO DAS *FAKE NEWS* NA PANDEMIA

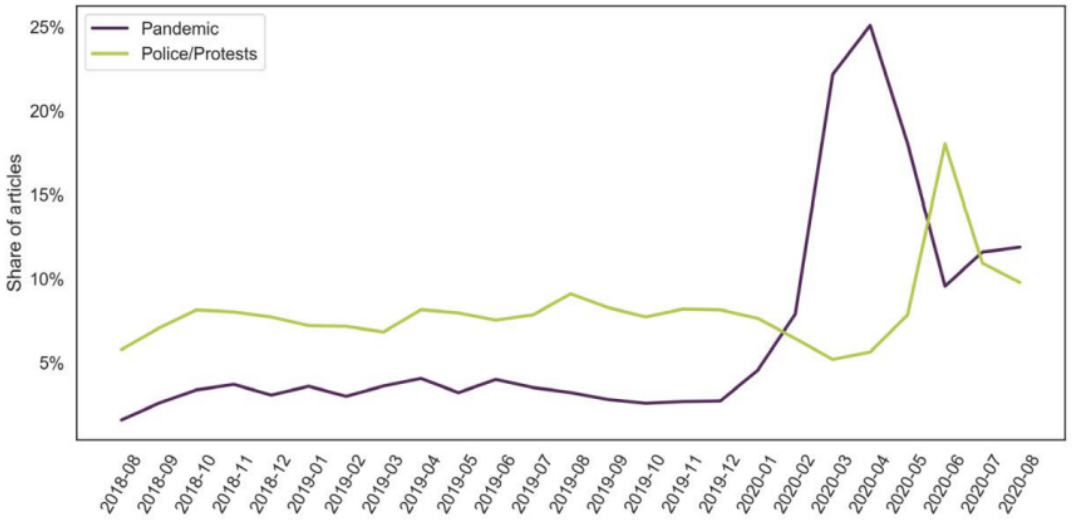
À medida que o Covid-19 se espalhava pelo mundo, também se espalhava uma epidemia de má informação e desinformação (HOLLOWOOD; MOSTROUS, 2020). Com efeito, a gênese da pandemia trouxe consigo o aumento de teorias da conspiração e veiculação de falsos métodos de prevenção e tratamento do vírus *SARS-CoV-2*.

Inicialmente, o desconhecimento sobre a origem do vírus e sua forma de agir no organismo fez com que as pessoas começassem a pesquisar mais sobre o assunto e se deparar com informações imprecisas sobre o tema. Contudo, com o andamento da situação, novas *fake news* e teorias surgiram, fazendo com que os indivíduos passassem a se automedicar e que métodos de tratamento perigosos direcionados a grupos específicos da população ameaçassem a vida das vítimas dessas falácias.

As plataformas digitais são simplesmente um meio para que pessoas e máquinas possam espalhar com maior velocidade as notícias falsas. De modo que, o Covid-19 não foi uma causa da desinformação que já existia, mas sim uma oportunidade para esses agentes perseguirem seus interesses.

Segundo dados do Ofcom (2021), a proporção de artigos de *websites* sobre a pandemia aumentou por volta de janeiro de 2020 e atingiu o pico em março, quando a Covid-19 foi declarada pandemia pela Organização Mundial da Saúde.

Figura 2 – Gráfico compartilhamento de artigos por assunto



Ofcom (2021)

No final de março de 2020, a agência realizou algumas pesquisas semanais com cerca de 2.000 pessoas, o intuito foi verificar os hábitos de consumo em relação às informações e notícias sobre a pandemia. Os resultados obtidos mostraram que durante a primeira semana do trabalho de campo realizado entre 27 e 29 de março de 2020, 46% dos entrevistados afirmaram que, na semana anterior à pesquisa, haviam encontrado informações ou notícias sobre o Covid-19 que consideravam falsas ou enganosas e 66% disseram que estavam vendo esse tipo de informação pelo menos uma vez por dia. Além disso, 40% das pessoas disseram achar difícil discernir os fatos reais das informações falsas (OFCOM, 2021).

Na semana trinta e três da pesquisa, entre 6 e 8 de novembro, 37% dos entrevistados disseram que, na semana anterior à pesquisa, haviam encontrado informações ou notícias sobre o Covid-19 que consideravam falsas ou enganosas. Os dados da agência mostraram uma diminuição gradual de um pico de 50% nas semanas três e cinco. Contudo, se observa que 40% das pessoas afirmaram achar difícil discernir as informações verdadeiras das falsas, dados iguais aos obtidos na primeira semana (OFCOM, 2021).

Os resultados da pesquisa apontam o perigo que as *fake news* possuem ao se misturar com fatos reais, de modo que essa diminuição da percepção de consumo das *fake news* pode ter sido autoalimentada pelas próprias notícias falsas.

Dessa forma, esse capítulo buscou fazer considerações acerca da definição das *fake news* e evidenciar seu potencial de moldar a opinião pública. Além disso, procurou-se mostrar, por meio de dados, que o crescimento do interesse da

população por pesquisar e compartilhar assuntos relacionados a pandemia aconteceu concomitantemente ao aumento da veiculação de falsas informações *online*, dificultando a percepção popular de quais conteúdos são verdadeiros ou não.

4 O CASO DO REINO UNIDO

Nos últimos anos, o debate político sobre *fake news* ganhou intensidade, especialmente com o Brexit no Reino Unido e as eleições presidenciais dos EUA em 2016, os quais acredita-se ter tido interferência da veiculação de falsas informações em seus respectivos resultados. De modo que, o The Guardian (2018) publicou investigações realizadas desde 2017 pela jornalista Carole Cadwalladr, as quais revelaram que a empresa de análise de dados Cambridge Analytica esteve por trás da campanha de Trump em 2016, bem como desempenhou um papel no referendo do Brexit, utilizando os dados coletados de 87 milhões de usuários do Facebook.

Essa tendência foi acentuada em 2020, quando os primeiros casos de contaminação pelo vírus SARS-CoV-2 no Reino Unido foram comprovados em membros de uma família de ascendência chinesa, hospedada no nordeste da Inglaterra. A primeira morte no Reino Unido ocorreu em março de 2020, posteriormente foi dada a confirmação da transmissão comunitária no país (OLIVEIRA; QUEIROZ, 2022).

Por outro prisma, a pandemia manifestou a necessidade do combate contra outro agente maligno que ameaçava a vida da população: a desinformação. Esse capítulo visa: 1) estudar como se deu o processo de securitização das *fake news* com suas bases em 2016 e agravado pelo contexto da pandemia de Covid-19, 2) apresentar ações de combate a esse problema tomadas pelo governo britânico e 3) Apresentar os resultados da securitização a partir da percepção dos britânicos sobre as notícias falsas.

4.1 SECURITIZAÇÃO DAS *FAKE NEWS*

Devido à recente notoriedade do tema, não existe um aporte teórico extenso sobre a securitização das *fakes news*. Contudo, os primeiros acontecimentos responsáveis pelo início dos estudos que vinculam propaganda e securitização foram os ataques de 11 de setembro e a invasão do Iraque. Nesse sentido, pode-se analisar o uso de informações falsas e um discurso de ódio direcionado à população pelos Estados Unidos para justificar a invasão do Iraque. Esse momento fundamentou o ambiente pós-verdade vivenciado nos dias atuais (HIGGOTT, 2003 apud ERGÜL, 2020).

No Reino Unido, as mídias sociais ganharam destaque nos debates políticos após as eleições sobre a permanência do Reino Unido na União Europeia em 2016. No ano seguinte, irrompeu no mundo o escândalo da *Cambridge Analytica* (CA), empresa que trabalhou fornecendo serviços de dados que apoiou a microssegmentação dos eleitores no contexto do referendo da UE.

Nesse sentido, o Comitê Digital de Cultura, Mídia e Esporte (DCMS) da Câmara dos Comuns divulgou o relatório final de uma investigação sobre desinformação que durou mais de 18 meses. O documento destaca a importância de refletir sobre os direitos de privacidade dos indivíduos e como suas escolhas políticas podem ser afetadas e influenciadas por informações *online*, além de abordar a interferência em eleições políticas no Reino Unido e em todo o mundo (UNITED KINGDOM, 2019b).

Além da *Cambridge Analytica*, o *Facebook* é responsabilizado por ter facilitado a manipulação política. Segundo o relatório, a empresa não se comprometeu em proteger os dados dos usuários e permitiu que os desenvolvedores de aplicativos tivessem acesso às informações dos mesmos, sem restrições, facilitando, portanto, o abuso de dados.

Assim sendo, o relatório adverte:

> Em comum com outros países, o Reino Unido é claramente vulnerável a campanhas secretas de influência digital e o governo deve conduzir análises para entender a extensão do direcionamento de eleitores, por *players* estrangeiros, durante as eleições passadas. (UNITED KINGDOM, 2019b, p. 94, tradução nossa)

Esse trecho admite a capacidade que o meio digital possui de afetar assuntos de interesse do Estado e destaca a necessidade de ações de combate à desinformação. À vista disso, a interferência de uma potência estrangeira nas eleições de um país pode ser considerada uma ameaça real. Com isso, o relatório e seus desdobramentos contribuem para o processo de securitização das *fake news,* já que provocou o debate sobre os perigos dessas informações para a democracia e sobre a guerra híbrida, gerando também mudanças nas legislações de diversos países e nos programas de grandes empresas que trabalham com dados.

Conquanto já existissem discussões sobre *fake news*, o Brexit em 2016 foi responsável por dar destaque para a necessidade de o Reino Unido colocar a

questão dentre as prioridades do Estado. Os acontecimentos apresentados aqui deram início ao quadro de securitização que foi agravado pela pandemia de Covid-19, tal qual estudado no próximo tópico.

4.2 A PANDEMIA E A SECURITIZAÇÃO DAS *FAKE NEWS*

Em 11 de março de 2020, a Organização Mundial da Saúde declarou a contaminação de Covid-19 como pandemia (WHO, 2020). Esse problema veio a se apresentar posteriormente, não apenas como uma ameaça à vida da população e à economia dos países, mas também trazendo implicações no âmbito da segurança e defesa. Conforme afirmado por Tedros Adhanom Ghebreyesus, diretor-geral da Organização Mundial da Saúde, na Conferência de Segurança de Munique, “Não estamos apenas lutando contra uma pandemia; estamos lutando contra uma infodemia" (ALJAZEERA, 2020).

A disseminação de informações falsas abrangeu diferentes fases da doença, desde a sua causa, contaminação e tratamento. Verral (2021) aponta os principais exemplos para cada uma das etapas, expostos no quadro 2 a seguir.

Quadro 2 – Principais temas de desinformação sobre a Covid-19

Causas (a história de origem)
Exemplos incluem os EUA liberando o vírus (CIA ou soldado); os chineses liberando o vírus; o vírus é uma desculpa para criar novas armas biológicas; criado para interferir nas eleições dos EUA; e como forma de criar dinheiro para as elites; “Big Pharma”; uma patente anterior para uma vacina dos EUA; fragmentos de um cometa; que foi criado por bioengenharia pelos EUA ou pela China; começou na Itália.
A propagação
Os exemplos incluem torres de sinal 5G; animais de estimação; banana; falta de seguro médico; variações de histórias de caixões e cadáveres; uma série de contextos ligando infecções intencionais conduzidas por certos países; e muitos países com seus próprios comentários sobre imigrantes e “estrangeiros”.
Prevenção e cura
Exemplos incluem o uso de solução salina; café; Prata coloidal; zinco; hidroxicloroquina; cloroquina; sal; luz solar; álcool; vitamina C; alimentos alcalinos; água tônica; lâmpadas ultravioleta; vapor de óleo de eucalipto; soluções minerais; bicarbonato de sódio; água sanitária para gargarejo; lavagem nasal; medicina ayurvédica; dietas veganas; banhos frios; vapor; pílulas de carbono; homeopatia; maconha; cocaína; sexo.

Elaboração própria, de acordo com Verrall (2021, p. 84)

Com relação à vacinação, a narrativa pró Kremlin obteve um papel significativo nas campanhas de desinformação e incentivo à não vacinação. Em relatório, a EUvsDisinfo (2020) detectou o compartilhamento de informações não confiáveis realizado pelo site Katehon por meio da republicação de um artigo contido no site americano LewRockwell.og, que já tinha republicado esse mesmo material de um site de medicina alternativa reconhecido por não possuir credibilidade. Posteriormente, foram identificadas várias fontes não confiáveis tentando sugerir que a pandemia seria uma invenção para que houvesse uma vacinação forçada a fim de estabelecer controle na população.

Com base nisso, Verrall (2021) explica que a técnica utilizada por Estados hostis e construções de narrativas como essa é chamada de Efeito Bandwagon. Nesse caso, o agente cria novas narrativas ou recicla as já existentes a fim de promover ruído por meio de engajamento, de maneira que, enquanto existir engajamento, o problema se perpetua. Essa técnica foi utilizada durante a pandemia para provocar desconfiança quanto à qualidade das vacinas do Reino Unido.

Quadro 3 – Técnicas de desinformação

Técnicas de engajamento	*Ad hominem; astroturfing; bandwagoning; butler lies; card stacking; cheerleading;* conspirações; dilema de falsidade; *flooding; laundering; gish gallop; transfer; strawman; misappropriation; ping pong; point and shriek; Potemkin village*; invasões; sátira, paródia e ridicularização; *shilling; sockpuppets; spiral of silence; symbolic action; tainting; totum pro parte; trolling; whataboutism; wolf cries wolf;* efeito woozle.
Ofício	**Contas** (contas falsas, contas antigas, contas sequestradas) • **Atribuição** (ocultar identidade, ocultar localização [IP], postar e excluir [fonte]) • **Personas** (voz, fala, texto, gesto [por exemplo, *deepfakes]* e outras imagens (por exemplo, fotos, símbolos, ícones, etc.) • **Conteúdo** (sites espelhados, crachás de verificação falsos, conteúdo impostor, documentos falsos ou editados, anúncios obscuros, vazamento contaminado [falso dentro da verdade], infográficos atraentes, compre métricas de mídia social) •**Comportamentos** (fazer amizade, espreitar, *phishing, trolling*)• **Redes** (acompanhamento mútuo, amplificar, *botnets*, nexo de agentes de influência).

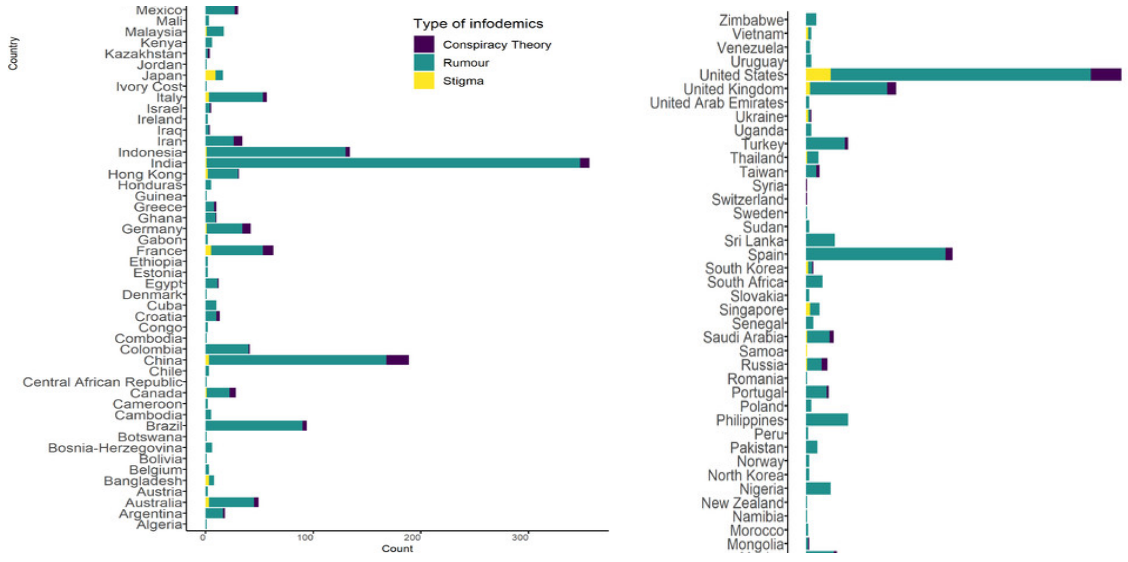
Elaboração própria, de acordo com Verrall (2021)

O contexto de crise trouxe implicações geoestratégicas ao se mostrar uma oportunidade de exploração de informações por atores envolvidos na zona cinzenta.

Um exemplo disso foram os três ataques integrados de desinformação sofridos pela OTAN (2020). Em primeiro lugar, uma carta falsa supostamente trocada entre o Secretário Geral da organização, Jen Stoltenberg, e o Ministro da Defesa da Lituânia, Raimundos Karoblis, para comunicar a retirada de tropas do país devido ao aumento da contaminação de Covid-19. Em seguida, foram criadas contas falsas para espalhar a desinformação e um vídeo foi publicado no *YouTube*. Por fim, a carta foi enviada para a sede da instituição. Essa situação foi percebida pela OTAN, exemplificando a necessidade de resposta rápida contra ataques inimigos à informação.

As notícias falsas não só trouxeram consequências para as instituições, como também impactos sociais significativos, sendo responsáveis pelo agravamento da crise de saúde. Conforme pesquisa feita pelo American Journal of Tropical Medicine and Hygiene, em média 5.800 pessoas foram internadas em decorrência de *fake news* nas redes sociais e muitos morreram pela ingestão de metanol ou produtos à base de álcool por acreditar ser eficaz contra o vírus. A pesquisa mostra também que as teorias da conspiração provocaram o aumento do preço de produtos essenciais e a escassez de fornecimento de máscaras faciais, devido às compras causadas pelo pânico. Entre os países pesquisados, o Reino Unido possui destaque pelos rumores, estigmas e teorias da conspiração relacionados ao Covid-19 (ISLAM *et al.*, 2020).

Figura 3 – Rumores, estigmas e teorias da conspiração por país



Islam *et al.* (2020).

Nesse sentido, Ergül (2020) salienta:

> Os perigos potenciais das notícias falsas são vários e eficazes. Pode ser usada tanto em política interna quanto na política internacional. Com a ajuda do recente ambiente internacional, muitos atores se sentem ameaçados com elas e estão prontos para muitas coisas em princípio. Assim, as notícias falsas tornam-se abertas ao uso indevido e à securitização. (ERGÜL, 2020, p. 14, tradução nossa)

Esses perigos têm sido experimentados pelo povo britânico de forma cada vez mais latente. A secretária do Estado para Assuntos Internos do Reino Unido, Priti Prattel, destaca o papel polarizador que assumem as campanhas de desinformação:

> As campanhas de desinformação têm se tornado cada vez mais ferramentas para semear a discórdia, tentar interferir na democracia e perturbar o tecido da sociedade do Reino Unido por meio de divisão e polarização. (LUCA, 2021, p. 1)

Outra fala pode ser observada pela Ministra do Departamento de Cultura, Mídia e Esporte, o principal órgão do país para tratar de danos *online*, conforme afirma Caroline Dinenage (2021, p. 1): “Informações falsas ou confusas divulgadas *online* podem ameaçar a segurança pública e minar nossa democracia”.

Nesse caso, ela utiliza claramente a palavra “ameaça” para se referir aos efeitos da divulgação não apenas de mentiras, como também de mensagens que geram confusão. O contexto desta mensagem foi a criação da Estratégia de Alfabetização de Mídia, um plano que desenvolve esforços para o desenvolvimento de habilidades essenciais para fazer escolhas *online* e estimular o pensamento crítico, com foco em usuários vulneráveis, como os jovens.

Nessa esfera, o Reino Unido inclui na Estratégia Nacional Cibernética, elaborada em 2021 para 2022, a desinformação como ameaça a ser combatida:

> As ameaças que enfrentamos no ciberespaço e por meio dele cresceram em intensidade, complexidade e gravidade nos últimos anos. Ataques cibernéticos contra no Reino Unido são conduzidos por uma gama cada vez maior de atores estatais, grupos criminosos (às vezes agindo sob a direção dos estados ou com sua aprovação implícita) e ativistas para fins de espionagem, ganho comercial, sabotagem e desinformação. (UNITED KINGDOM, 2021, p. 9)

Nesse documento, o governo britânico coloca entre os objetivos das operações cibernéticas a defesa da democracia e eleições livres, justas e abertas, combatendo campanhas estatais de desinformação organizadas com destino a prejudicá-las. Podendo-se dizer, então, que o governo britânico é securitizador ao rotular as ações de desinformação como uma ameaça séria ao objeto referente: a democracia.

Durante a pandemia, o Parlamento do Reino Unido restabeleceu o Subcomitê de Danos e Desinformação *Online* por verificar a necessidade de acompanhar as informações sobre a crise. Além disso, foi inaugurada a Unidade de Contra-Desinformação e sua função foi fazer o monitoramento de possíveis riscos à informação durante a pandemia por meio de uma análise abrangente envolvendo o alcance desses problemas (VERRALL, 2021).

Além disso, a 77ª Brigada do Exército britânico atuou no combate à desinformação sobre o Covid-19, vale destacar que, esse grupo foi criado em 2015 para agir em situações de guerra psicológica e guerra de informação (YOUNG, 2020).

Outra campanha realizada pelo Reino Unido foi a “Don’t feed the beast” com vistas a ensinar o público a identificar notícias falsas com cinco etapas simples: 1) Verificar se a fonte da notícia é confiável; 2) Não ler apenas o título; 3) Verificar os fatos; 4) Analisar se as imagens ou vídeos parecem adulterados e 5) Prestar atenção em erros gramaticais (BANERJEE, 2020).

Concomitantemente, a Unidade de Resposta Rápida operou dentro do Cabinet Office para lidar com as narrativas falsas sobre o coronavírus. Ao identificar um problema, a equipe em parceria com os departamentos do Whitehall realizava a resposta adequada, seja por uma refutação direta nas redes sociais ou delegando às plataformas o dever de remover a postagem não confiável. Por volta de 70 casos semanais foram resolvidos pela unidade integrante da Célula Anti-Desinformação, liderada pelo Departamento de Cultura, Mídia e Esporte (UNITED KINGDOM, 2020).

Segundo o Centro Nacional de Segurança Cibernética:

> Exemplos de golpes incluem o direcionamento de pessoas que procuram comprar suprimentos médicos, aqueles que procuram conselhos de saúde e encorajar as pessoas a doar dinheiro para instituições de caridade falsas. (WOOLLACOTT, 2020, p. 1, tradução nossa)

Para isso, o Governo incumbiu ao NewsGuard o dever de classificar sites com base em critérios de credibilidade, entre eles: precisão de manchetes, comportamento anterior e abertura para publicar correções de erros e comunicados (WOOLLACOTT, 2020).

Nesse sentido, o secretário de Cultura, Oliver Dowden, se comunica de maneira claramente direcionada ao público:

> Precisamos que as pessoas sigam os conselhos médicos especializados e fiquem em casa, protejam o Serviço Nacional de Saúde e salvem vidas. É vital que esta mensagem chegue nas casas e que a desinformação e a má informação que as minam sejam derrubadas rapidamente. (UNITED KINGDOM, 2020, p. 1, tradução nossa)

Além disso, entrou em processo na Câmara dos Comuns o Projeto de Lei de Segurança *Online*. Com essa norma, o Reino Unido visa forçar as plataformas de mídia social a tomar medidas contra a desinformação e as empresas precisarão fazer avaliações de risco para conteúdo ilegal, dificultar a criação massiva de contas falsas e combater o uso de robôs em campanhas maliciosas (UNITED KINGDOM, 2022a).

A lei também visa a proteção do país contra a interferência estrangeira, sendo possível observar esse aspecto na fala da secretária do Estado para Cultura, Meios de Comunicação e Esporte, Nadine Dorries:

> A invasão da Ucrânia mostrou mais uma vez quão prontamente a Rússia pode e irá usar a mídia social como arma para espalhar desinformação e mentiras sobre suas ações bárbaras, muitas vezes visando as próprias vítimas de sua agressão. Não podemos permitir que estados estrangeiros ou seus fantoches usem a Internet para conduzir uma guerra *online* hostil sem impedimentos. (UNITED KINGDOM, 2022b, p. 1, tradução nossa)

Ao identificar o risco representado por ameaças externas de Estados hostis à Segurança do Reino Unido por meio do uso da informação, o país considera essencial continuar com atividades de defesa no meio cibernético.

Conforme o Ministro da Segurança Damian Hinds:

> As operações de informações on-line são agora uma parte essencial da atividade de ameaças de estado. O objetivo pode ser espalhar inverdades, confundir, minar a confiança na democracia ou semear a divisão na sociedade. (UNITED KINGDOM, 2022b, p. 1)

Quando uma questão deixa de estar presente apenas no debate político e passa a ser assunto de interesse de segurança do Estado, estratégias de mitigação precisam ser montadas e executadas. Dessa forma, a securitização de notícias falsas pelo Reino Unido buscou legitimar a aprovação de medidas para lidar com a ameaça urgente, desde o período pandêmico até as implicações para os próximos anos.

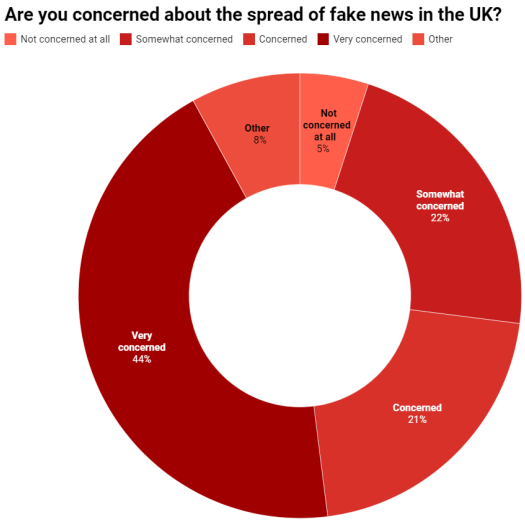
4.3 A SECURITIZAÇÃO COMO RESULTADO

Baseado na ideia da natureza da segurança, as análises de securitização devem buscar obter uma compreensão de quem securitiza, sob quais ameaças, para quem, com quais resultados e sob quais condições (BUZAN; WÆVER; WILDE, 1998). Diante disso, esse capítulo busca realizar uma análise dos resultados desse processo, com base em informações encontradas até o momento do presente trabalho.

As teorias de securitização não fornecem um modelo claro para averiguar o sucesso ou fracasso de um movimento securitizador. Contudo, um movimento de securitização, para ser bem-sucedido, precisa da aceitação do público da questão como uma ameaça (BALZACQ, 2010).

O problema das *fake news* tem sido um destaque no debate político mais amplo no Reino Unido. Um estudo feito com 2000 pessoas pela revista britânica Press Gazette revela que dois terços das pessoas entrevistadas se preocupam com a disseminação de *fake news* (KERSLEY, 2022).

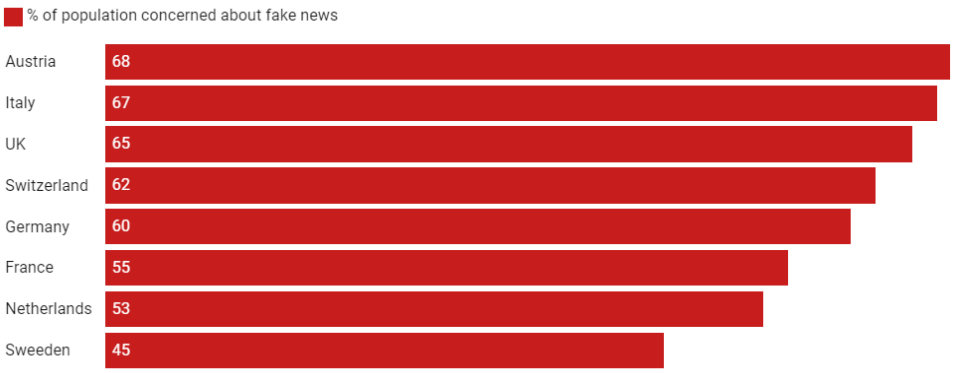
Figura 4 – Nível de preocupação dos britânicos com a disseminação de notícias falsas



Fonte: Kersley (2022).

Entre os países europeus, o Reino Unido assume o terceiro lugar dos oito países que mais se preocupam com o problema das *fake news* .

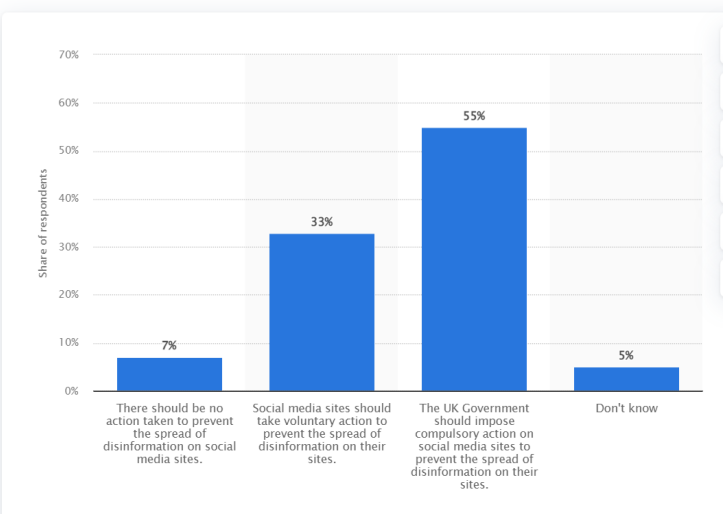
Figura 5 – Países europeus com mais porcentagem da preocupação sobre *fake news*



Fonte: Kersley (2022).

Outra pesquisa realizada em 2020 e publicada em 2022 pelo Statista, sobre a opinião pública dos britânicos a respeito da desinformação, revela que 55% dos entrevistados disseram que o Governo do Reino Unido deveria impor ações compulsórias em sites de mídia social para impedir a disseminação de desinformação. Enquanto isso, 33% disseram que os sites deveriam tomar medidas voluntárias para impedir a disseminação de informação falsa em suas plataformas (DIXON, 2022).

Figura 4 – Opinião pública sobre como impedir a disseminação de desinformação nas mídias sociais Reino Unido em 2020



Fonte: Dixon (2022).

Esses dados sugerem a legitimação de medidas excepcionais para lidar com a ameaça urgente. De forma que a população britânica não parece apenas tolerar o movimento securitizador, mas apoiar que ações sejam realizadas para mitigar o problema, dessa forma, a securitização pode ser vista como bem-sucedida. Discussões futuras podem ser realizadas acerca das consequências diretas e indiretas desse processo para a sociedade e sua forma de lidar com a informação, assim, o Reino Unido pode servir como exemplo para outros países.

Esse capítulo buscou mostrar, portanto, a construção do problema das fake news como uma ameaça à segurança britânica e o seu agravamento pela emergência da pandemia de Covid-19, bem como os seus resultados para a população.

5 CONCLUSÃO

A presente monografia buscou analisar o processo de securitização das *fake news* no Reino Unido sob o contexto de pandemia do coronavírus. Fundamentado em Balzacq (2010), foi realizado o estudo do caso do Reino Unido a partir de três níveis da análise: os atores e suas relações, as práticas e recursos linguísticos e o contexto e suas implicações para o processo de securitização.

Durante o texto, se fez uso de análise de discursos para verificar a presença da narrativa securitizadora nas falas de autoridades e documentos britânicos. Como também, foram apresentados dados, com o objetivo de verificar os resultados do processo de securitização das *fake news* .

Nesse sentido, o arcabouço literário contou com a definição de Espaço Cibernético de Kuehl (2009) e suas características elencadas por Choucri (2012) para elucidar a dimensão de ciberespaço e a esfera informacional. Em outro momento, buscou-se introduzir a visão realista e a condição anárquica desse domínio, com a literatura de Kremer e Muller (2014), Herz (1950) e Waltz (2002). Além disso, as perspectivas de Sheldon (2012) e Nye (2008) foram apresentadas para o entendimento dos desafios apresentados pelo Espaço Cibernético.

Ademais, o trabalho buscou conceituar as *fake news* e distinguir os tipos de desordem de informação existentes através das definições de Klein e Wueller (2017), bem como Wardle e Derakhshan (2017). Com efeito, as Teorias de Securitização da Escola de Copenhague, representada por Buzan, Waever e Wilde (1998) e, especialmente, de Balzacq (2010), contribuíram para a compreensão do processo de securitização sob o contexto de crise do coronavírus.

Com efeito, o debate sobre a importância das mídias e do controle de informação começou a ganhar destaque na política britânica após a votação do Brexit em 2016 e o escândalo que envolveu a *Cambridge Analytica*. Contudo, os efeitos nocivos do compartilhamento de notícias falsas foram sentidos de forma mais direta pela população durante a crise de Covid-19.

Nesse sentido, o espaço cibernético oferece uma grande abertura para a desinformação e atuação de agentes malignos que encontram um meio livre de barreiras geográficas e com baixo aparato regulatório para agir no anonimato e espalhar informações falsas para o maior número de pessoas em um tempo curto.

Além disso, países e grupos paramilitares encontram no ambiente cibernético uma maneira de projetar ataques contra adversários sem um custo financeiro muito alto em comparação com ofensivas convencionais.

A pandemia expôs a vulnerabilidade de diversos países em lidar não apenas com uma crise sanitária e de saúde pública, mas com a ameaça da desinformação à vida da população e à segurança do Estado. As informações falsas abrangeram desde a causa do vírus até sua prevenção, tratamento e disseminação, com isso, pessoas foram internadas por ingestão de substâncias nocivas e o pânico causou o aumento de preços e escassez de máscaras e materiais de higiene.

O governo britânico não percebeu apenas os problemas internos causados por esse mal, mas identificou os riscos de ameaças externas ao país. A Rússia, por exemplo, comumente utiliza-se de estratégias de guerra psicológica e guerra de informação para atacar adversários da OTAN. Durante a pandemia, a narrativa pró Kremlin suscitou desconfiança quanto à vacina do Reino Unido.

Dessa forma, o país passou a lidar com as *fake news* não só como uma questão política, mas como um assunto de interesse militar e a partir disso realizou tentativas de transmitir para a população a percepção das notícias falsas como ameaça e tomou medidas de combate às mesmas.

Nesse contexto, várias autoridades britânicas apontaram em suas falas os riscos da desinformação à democracia e a característica polarizadora desse tipo de notícia. Além disso, o Subcomitê de Danos e Desinformação Online foi reestabelecido para fazer o monitoramento das informações e a campanha “Don’t feed the beast” foi lançada para conscientizar a população a não consumir conteúdo não confiável e identificar possíveis problemas.

A Unidade de Resposta Rápida também operou dentro do *Cabinet Office* para identificar informações danosas e realizar a refutação ou pedir para as plataformas de mídias sociais a remoção do conteúdo. Ademais, a estratégia nacional cibernética passou a incluir constantes operações de combate à desinformação como uma das prioridades.

Outra medida tomada foi o Projeto de Lei de Segurança Online que se encontra no momento deste trabalho em estágio de relatório na Câmara dos Comuns. Efetivamente, a população britânica enxerga nas *fake news* um problema e grande parte apoia ações excepcionais para lidar com esse impasse. Portanto, o

processo de securitização mostra-se bem-sucedido até então e isso implica em estratégias para a mitigação do problema. No entanto, vale fazer reflexões sobre os impactos futuros desse movimento e das medidas tomadas, na população.

Portanto, é possível confirmar a hipótese inicial do texto de que a crise da pandemia de Covid-19 levou à aceleração do processo de securitização das *fake news*. Tendo em vista que a pesquisa realizada nesta monografia mostrou um aumento do compartilhamento de informações falsas por parte da população na pandemia em meio às ações ofensivas de Estados contrários ao interesse britânico e as consequentes medidas defensivas tomadas por instâncias do Governo do Reino Unido. Esse caráter securitizador é observado não apenas nos discursos e documentos oficiais, como também por meio das políticas públicas e uso das forças armadas para combater a ameaça. Dessa forma, o êxito da securitização deve-se à aprovação moral da população com relação ao entendimento das *fake news* como uma ameaça ao país e ao não antagonismo no que se refere às medidas adotadas pelo Estado para o combate desse problema de segurança.

REFERÊNCIAS

ACÁCIO, D. P.; SOUZA, G. L. M. Segurança internacional no século XXI: o que as teorias de relações internacionais têm a falar sobre o ciberespaço? *In*: ENCONTRO ANUAL DA ANPOCS, 36., 2012, São Paulo. [**Anais**]. São Paulo: ANPOCS, 16 out. 2012. Disponível em: http://mail.anpocs.org/index.php/encontros/papers/36-encontro-anual-da-anpocs/gt-2/gt28-2/8169-seguranca-internacional-no-seculo-xxi-o-que-as-teorias-de-relacoes-internacionais-tem-a-falar-sobre-o-ciberespaco. Acesso em: 27 nov. 2022.

AQUINO, J. P. M. **Análise do conceito de fake news e de pós-verdade, bem como a resposta dada pelo direito**. 2021. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Escola de Direito de Brasília, Instituto Brasiliense de Direito Público, Brasília, DF, 2021. Disponível em: https://repositorio.idp.edu.br/handle/123456789/3428. Acesso em: 27 nov. 2022.

ARAÚJO JORGE, Bernardo Wahl G. de. 2012. **"Das guerras cibernéticas"**. XI Ciclo de Estudos Estratégicos da Escola de Comando e Estado-Maior do Exército (ECEME): 1–26 (Maio). Rio de Janeiro. Disponível em: https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjyypSNtNr7AhWIHrkGHXmtC4sQFnoECBAQAQ&url=https%3A%2F%2Fwww.academia.edu%2F3507313%2FDas_Guerras_Cibern%25C3%25A9ticas_&usg=AOvVaw3K-NOF2mPkKww4OdwxSTfc. Acesso em: ago 2022.

BALZACQ, T. The three faces of securitization: political agency, audience and context. **European Journal of International Relations**, [*s. l.*], v. 11, n. 2, p. 171-201, 2005. Disponível em: https://journals.sagepub.com/doi/10.1177/1354066105052960. Acesso em: 27 nov. 2022.

BALZACQ, T. **Securitization theory**: how security problems emerge and dissolve. Nova Iorque: Routledge, 2010.

BANERJEE, S. How we are fighting the spread of false coronavirus information online. **Government Communication Service**. [*S. l.*], 16 Apr 2020. Disponível em: https://gcs.civilservice.gov.uk/blog/how-we-are-fighting-the-spread-of-false-coronavirus-information-online/. Acesso em: 26 out. 2022.

BARNARD-WILLS, D.; ASHENDEN, D. Securing virtual space: cyber war, cyber terror, and risk. **Space and Culture**, [*s. l.*], v. 15, n. 2, p. 110-123, 2012. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/1206331211430016. Acesso em: 27 nov. 2022.

BASSOU, A.; TOBI, Y. (coord.). **Thriving on uncertainty**: covid-19-related opportunities for terrorist groups. [Barcelona]: European Institute of the Mediterranean, 2021. (Euromesco Policy Study, n. 21). Disponível em: https://www.euromesco.net/wp-content/uploads/2021/06/Thriving-on-Uncertainty-COVID-19-Related-Opportunities.pdf. Acesso em: 29 set. 2022.

BUZAN, B.; WÆVER, O.; WILDE, J. **Security**: a new framework for analysis. London: Roulder London, 1998. Disponível em: https://www.academia.edu/39047709/Buzan_Waever_and_De_Wilde_1998_Security_A_New_Framework_For_Analysis. Acesso em: 26 set. 2022.

CASTELLS, Manuel. **A sociedade em rede.** v.1. 5. ed. São Paulo: Paz e Terra, 2001. in A era da informação: Economia, sociedade e cultura.

CHOUCRI, N. The convergence of cyberspace and sustainability. **E-International Relations**. [*S. l.*], 20 Apr 2012. Disponível em: https://www.e-ir.info/2012/04/20/the-convergence-of-cyberspace-and-sustainability/. Acesso em: 27 nov. 2022.

DAHL, R. **Sobre a democracia**. Brasília: UnB, 2001.

DEUTSCH, Karl. **Análise das Relações Internacionais**. Brasília: Universidade de Brasília, 1982.

DINENAGE, C. Minister launches new strategy to fight online disinformation. [Entrevista cedida ao] **Deparment for Digital, Culture, Media & Sport**. London, 14 July 2021. Disponível em: https://www.gov.uk/government/news/minister-launches-new-strategy-to-fight-online-disinformation. Acesso em: 27 nov. 2022.

DIXON, S. Public opinion on how to stop the spread of disinformation on social media UK 2020. **Statista**. [*S. l.*], 28 Apr 2022. Disponível em: https://www.statista.com/statistics/1115732/opinion-on-preventing-disinformation-on-social-media-uk/. Acesso em: 20 out. 2022.

DUGGAN, D. P.; PARKS, R. Principles of cyberwarfare. **IEEE Security & Privacy Magazine**, [*s. l.*], v. 9, n. 5, p. 30-35, 2012.

ERGÜL, M. M. **Securization of fake news**. 2020. Thesis (Master of Sciences in International Relations) – The Graduate School of Social Sciences, Middle East Technical University, Ancara, Turkey, 2020.

ESTADOS UNIDOS DA AMÉRICA. Department of the Army. **Cyberspace operations concept capability plan 2016-2028**. Washigton, DC: Department of the Army, 2010. Disponível em: https://irp.fas.org/doddir/army/pam525-7-8.pdf. Acesso em: jul. 2022.

EUVSDISINFO. **Vaccine hesitancy and pro-kremlin opportunism**. [*S. l.*], 20 Apr 2020. Disponível em: https://euvsdisinfo.eu/vaccine-hesitancy-and-pro-kremlin-opportunism/#. Acesso em: 20 out. 2022.

Exposing Cambridge Analytica: 'It's been exhausting, exhilarating, and slightly terrifying. **The Guardian,** 2018. Disponível em:

https://www.theguardian.com/membership/2018/sep/29/cambridge-analytica-cadwalladr-observer-facebook-zuckerberg-wylie. Acesso em: ago. 2022.

FELICIANO, R. A. **A incorporação do poder cibernético ao militar**: análise estadunidense do governo Obama. 2018. Monografia (Bacharelado em Relações Internacionais) – Departamento de Relações Internacionais, Centro de Ciências Sociais Aplicadas, Universidade Federal da Paraíba, João Pessoa, 2018. Disponível em: https://repositorio.ufpb.br/jspui/bitstream/123456789/13934/1/RAF26.03.2019.pdf. Acesso em: 27 nov. 2022.

GELFERT, A. Fake news: a definition. **Informal Logic**, [*s. l.*], v. 38, n. 1, p. 84-117, 2018. Disponível em: https://informallogic.ca/index.php/informal_logic/article/view/5068. Acesso em: 27 nov. 2022.

GHEBREYESUS, T. A. We need to work together to tackle the coronavirus 'infodemic'. [Entrevista cedida a] Muhammad Jawad Noon. **Aljazeera**. [*S. l.*], 23 Oct 2020. Disponível em: https://www.aljazeera.com/opinions/2020/10/23/we-need-to-work-together-to-tackle-the-coronavirus-infodemic. Acesso em: 21 out. 2022.

HERZ, J. H. Idealist internationalism and the security dilemma. **World Politics**, [*s. l.*], v. 2, n. 2, p. 157-180, Jan 1950. Disponível em: https://www.jstor.org/stable/2009187. Acesso em: 3 nov. 2022.

HJALMARSSON, O. **The securitization of cyberspace**: how the web was won. 2013. Essay (Course of Political Science) – Department of Political Science, Lund University, Lund, Sweden, [2013]. Disponível em: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=3357990&fileOId=3357996. Acesso em: 27 nov. 2022.

HOLLOWOOD, E.; MOSTROUS, A. The infodemic: fake news in the time of C-19. **Tortoise**. [*S. l.*], 23 Mar 2020. Disponível em: https://www.tortoisemedia.com/2020/03/23/the-infodemic-fake-news-coronavirus/. Acesso em: 27 nov. 2022.

HUYSMANS, J. Revisiting Copenhagen: or, on the creative development of a security studies agenda in europe. **European Journal of International Relations**, [*s. l.*], v. 4, n. 4, p. 479-505, 1998. Disponível em: https://journals.sagepub.com/doi/10.1177/1354066198004004004. Acesso em: 5 nov. 2022.

ISLAM, S. *et al.* Covid-19-related infodemic and its impact on public health: a global social media analysis. **The American Journal of Tropical Medicine and Hygiene**, [*s. l.*], v. 103, n. 4, p. 1621-1629, 10 ago. 2020. Disponível em: https://www.ajtmh.org/view/journals/tpmd/103/4/article-p1621.xml?tab_body=contributor-notes-display. Acesso em: 20 out. 2022.

KERSLEY, A. Two-thirds of british people worry about the spread of fake news. **Press Gazette**. [*S. l.*], 8 Mar 2022. Disponível em: https://pressgazette.co.uk/news/british-fake-news/. Acesso em: 6 out. 2022.

KLEIN, D.; WUELLER, J. Fake news: a legal perspective. **Journal of Internet Law**, [*s. l.*], v. 20, n. 10, p. 5-13, Apr 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958790. Acesso em: 15 ago. 2022.

KORYBKO, Andrew. **Guerras Híbridas**: Das revoluções coloridas aos golpes. Expressão Popular. São Paulo, 2018.

KREMER, J.; MÜLLER, B. **Cyberspace and international relations**: theory, prospects and challenges. Nova Iorque: Springer, 2014.

KUEHL, D. T. From cyberspace to cyberpower: defining the problem. *In*: KRAMER, F. D.; STARR, S.; WENTZ, L. K. (coord.). **Cyberpower and national security**. Washington, DC: NDU Press, 2009. p. 1-17.

LAZER, D. M. J. *et al.* The science of fake news: addressing fake news requires a multidisciplinary effort. **Science**, [*s. l.*], v. 359, n. 6380, p. 1094-1096, 9 Mar 2018. Disponível em: https://www.science.org/doi/10.1126/science.aao2998. Acesso em: 20 ago. 2022.

LUCA, A. Reino Unido quer criminalizar fake news espalhadas por governos hostis e vazamento de informações. **MediaTalks**. [*S. l.*], 15 maio 2021. Disponível em: https://mediatalks.uol.com.br/2021/05/15/espalhar-fake-news-pode-dar-prisao-no-reino-unido/. Acesso em: 22 out. 2022.

MAIA, R. **Deliberação e mídia.** In R. C. M. Maia (ed.), Mídia e deliberação (pp. 93-110). Rio de Janeiro: Editora FGV, 2008.

MORGENTHAU, H. J. **Política entre as nações**: a luta pelo poder e pela paz. Brasília: UNB, 2003.

NYE, J. S. **O paradoxo do poder americano**: por que a única superpotência do mundo não pode prosseguir isolada. Tradução: Luiz Antônio Oliveira de Araújo. São Paulo: UNESP, 2002.

NYE. J. S. Cyber insecurity. **Project Syndicate**. [*S. l.*], 10 Dec 2008. Disponível em: https://www.project-syndicate.org/commentary/cyber-insecurity-2008-12. Acesso em: 16 out. 2022.

NYE, J. S. **Cyber power**. Cambridge: Harvard, 2010.

OFCOM. **Understanding online false information in the UK**. [*S. l.*]: Ofcom, 27 Jan 2021. (Economist discussion paper series, n. 2). Disponível em:

https://www.ofcom.org.uk/__data/assets/pdf_file/0027/211986/understanding-online-false-information-uk.pdf. Acesso em: 5 set. 2022.

OLIVEIRA, S. C.; QUEIROZ, L. F. **O Reino Unido diante da covid-19**: hesitação política e capacidade de resposta de um sistema de saúde universal. [Salvador]: Fiocruz, 2022.

ORGANIZAÇÃO PAN-AMERICANA DE SAÚDE. **Entenda a infodemia e a desinformação na luta contra a covid-19**. Washington, DC: PAHO, 2020. (Série Kit de Ferramentas de Transformação Digital, Ferramentas de conhecimento, n. 9). Disponível em: https://iris.paho.org/handle/10665.2/52054. Acesso em: 19 out. 2022.

OTAN. North Atlantic Treaty Organization. **Russia's top five myths about NATO & covid-19**. [*S. l.*]: PDD, Apr 2020. 1 ficha técnica, color. Disponível em: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/2004-Factsheet-Russia-Myths-COVID-19_en.pdf. Acesso em: 5 jun. 2022.

PORTELA, Lucas Soares. Geopolítica do espaço cibernético e o poder: o exercicio da soberania por meio do controle. **Revista Brasileira de Estudos de Defesa.** v. 5, nº 1.2018, p. 141-165. Disponível em: 75081-Texto do Artigo-1491-311410-10-20190402.pdf. Acesso em: dez. 2022.

QUIRÓS, Eduardo A. **A era da pós verdade: realidade versus percepção.** Uno, São Paulo, v. 27, n. 1, p.36-37, mar. 2017. Disponível em: http://www.revista-uno.com.br/wp-content/uploads/2017/03/UNO_27_BR_baja.pdf. Acesso em: nov. 2022.

READING, D. F.; WELLS, B. Cognitive warfare: NATO, covid-19 and the impact of emerging and disruptive technologies. *In*: GILL, R.; GOOLSBY, R. (coord.). **Covid-19 disinformation**: a multi-national, whole of society perspective. Switzerland: Springer, 2022. p. 25-45.

RODARI, Adriano. Russia’s [un]controlled disinformation. **Duodecim Astra**, 2021,, p. 98-120. Disponível em: https://www.coleurope.eu/sites/default/files/uploads/page/11%20Adriano%20Rodari%20-%20Russia%E2%80%99s%20%28un%29Controlled%20Disinformation%20%28Duodecim%20Astra%29.pdf. Acesso em: ago. 2022.

SABĂU, C. G.; ION, V.; NEAG, M. National security and public opinion. *In*: SCIENTIFIC RESEARCH AND EDUCATION IN THE AIR FORCE, 2016, Romania. [**Proceedings**]. Brasov: ARACIS, 2016. Disponível em: https://www.afahc.ro/ro/afases/2016/SOCIO/SABAU_ION_NEAG.pdf. Acesso em: 27 ago. 2022.

SCHONS, C. H.. O volume de informações na internet e sua desorganização: reflexões e perspectivas. Informação & Informação, Londrina, v.12, n.1, jan./jun. 2007. Disponível em: . Acesso em: 26 nov. 2014.

SHELDON, J. B. Deciphering cyberpower: strategic purpose in peace and war. **Strategic Studies Quarterly**, [*s. l.*], v. 5, n. 2, p. 95-112, Summer 2011. Disponível em: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-2/Sheldon.pdf. Acesso em: 27 nov. 2022.

UNITED KINGDOM. Government. Secretary of State for Digital, Culture, Media & Sport. Secretary of State for the Home Deparment. **Online harms white paper**. London: Crown, Apr 2019a. (CP n. 57). Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf. Acesso em: 27 nov. 2022.

UNITED KINGDOM. House of Commons. Digital, Culture, Media and Sport Committee. **Disinformation and 'fake news'**: final report. London: House of Commons, 18 Feb 2019b. (Eighth Report of Session 2017-19). Disponível em: https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf. Acesso em: 15 ago. 2022.

UNITED KINGDOM. Cabinet Office. Deparment for Digital, Culture, Media & Sport. **Government cracks down on spread of false coronavirus information online**. London, 30 Mar 2020. Disponível em: https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online. Acesso em: 27 nov. 2022.

UNITED KINGDOM. **Policy paper**: national cyber strategy 2022. London: Crown, 2021. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1085304/National_Cyber_Strategy_2022_-_GOV.UK.pdf. Acesso em: 27 nov. 2022.

UNITED KINGDOM. Deparment for Digital, Culture, Media & Sport. **Internet safety laws strengthened to fight russian and hostile state disinformation**. London, 5 July 2022a. Disponível em: https://www.gov.uk/government/news/internet-safety-laws-strengthened-to-fight-russian-and-hostile-state-disinformation. Acesso em: 27 nov. 2022.

UNITED KINGDOM. UK Parliament. **Government Cyber Security Strategy**: Building a cyber resilient public sector. London, 2022. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf. Acesso em: jul. 2022.
UNITED KINGDOM. UK Parliament. **Online safety bill**. [London], 25 Nov 2022b. (Originated in the House of Commons, Sessions 2021-22, 2022-23). Disponível em: https://bills.parliament.uk/bills/3137. Acesso em: 15 out. 2022.

VERRALL, N. Covid-19 disinformation, misinformation and malinformation during the pandemic infodemic: a view from the United Kingdom. *In*: GILL, R.; GOOLSBY, R. (coord.). **Covid-19 disinformation**: a multi-national, whole of society perspective. Switzerland: Springer, 2021. p. 81-112.

VIANA E SILVA, Caroline Cordeiro. **Segurança internacional e novas ameaças : a securitização do narcotráfico na fronteira brasileira**. 2013. 126 f. Dissertação (Mestrado)- Curso de Ciência Política, Universidade Federal do Paraná, Curitiba, 2013.

WALTZ, Kenneth N. 1959. **Man, the state and war:** A theoretical analysis. New York: Columbia University Press.

WALTZ, Kenneth. **Teoria das Relações Internacionais**. Lisboa: Gradiva, 2002.

WARDLE, C.; DERAKHSHAN, H. **Information disorder**: toward an interdisciplinary framework for research and policy making. [Estrasburgo, FR]: Council of Europe, 2017. (Council of Europe report, DGI (2017)09). Disponível em: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c. Acesso em: 27 out. 2022.

WHO. WHO **Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020**. [*S. l.*], 11 Mar 2020. Disponível em: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. Acesso em: 20 out. 2022.

WOOLLACOTT, E. UK government launches unit to deal with fake coronavirus. **Forbes**. [*S. l.*], 30 Mar 2020. Disponível em: https://www.forbes.com/sites/emmawoollacott/2020/03/30/uk-government-launches-unit-to-deal-with-fake-coronavirus-news/?sh=2d6c3b606ab3. Acesso em: 15 ago. 2022.

YOUNG, G. Defence chief says 77th brigade is countering covid misinformation. **The National**. Buckinghamshire, 22 Apr 2020. Disponível em: https://www.thenational.scot/news/18398012.defence-chief-says-77th-brigade-countering-covid-misinformation/. Acesso em: 15 out. 2022.