As redes sociais contemporâneas como ferramentas para operações de inteligência e contrainteligência: impactos na diplomacia

Autor
Juvenal Pelo Quicassa

Mestre, Especialista em Relações Internacionais.

Professor Assistente no Instituto Superior Politécnico do Kangonjo / e Instituto Superior Politécnico Internacional de Angola.

Pesquisador do Centro de Estudos e Pesquisas da Unipiaget (Benguela).

E-mail:
juvenalquicassa@gmail.com

Resumo

O presente artigo analisa como as redes sociais contemporâneas se tornaram ferramentas essenciais para operações de inteligência e contrainteligência, influenciando diretamente a diplomacia global. O estudo utiliza uma abordagem bibliográfica e comparativa para examinar casos recentes de espionagem digital e suas implicações para as relações internacionais. A pesquisa destaca que Estados e actores não estatais exploram plataformas como Facebook e Twitter para coletar informações estratégicas, influenciar processos políticos e monitorar adversários. Com a digitalização da espionagem, os Estados passaram a utilizar essas ferramentas para vigilância, manipulação de narrativas e até mesmo para operações de desinformação. Além disso, o estudo ilustra como a interconectividade global intensificou a vulnerabilidade diplomática, expondo países a ameaças cibernéticas e interferências externas. O artigo também discute a evolução da espionagem, desde os métodos tradicionais, como agentes infiltrados e interceptações telefônicas, até a era digital, onde big data, inteligência artificial e ataques cibernéticos desempenham papéis fundamentais. Casos como a interferência russa nas eleições americanas de 2016 e as operações de vigilância digital da NSA reveladas por Edward Snowden são analisados como exemplos do impacto crescente das redes sociais na inteligência global. Por fim, a pesquisa evidencia que a crescente influência das redes sociais na espionagem impõe desafios à segurança diplomática e exige novos paradigmas de governança da informação. A cooperação internacional e regulamentações mais rígidas podem ser caminhos para mitigar os riscos associados a essa nova realidade, garantindo maior transparência e segurança no uso das redes sociais para fins de inteligência.

Abstract

The present article analyzes how contemporary social networks have become essential tools for intelligence and counterintelligence operations, directly influencing global diplomacy. The study employs a bibliographic and comparative approach to examine recent cases of digital espionage and their implications for international relations. The research highlights that states and non-state actors exploit platforms such as Facebook and Twitter to gather strategic information, influence political processes, and monitor adversaries. With the digitalization of espionage, states have begun to use these tools for surveillance, narrative manipulation, and even disinformation operations. Additionally, the study illustrates how global interconnectivity has intensified diplomatic vulnerability, exposing countries to cyber threats and external interference. The article also discusses the evolution of espionage, from traditional methods such as infiltrated agents and telephone interceptions to the digital era, where big data, artificial intelligence, and cyberattacks play fundamental roles. Cases such as Russian interference in the 2016 U.S. elections and the NSA's digital surveillance operations revealed by Edward Snowden are analyzed as examples of the growing impact of social networks on global intelligence. Finally, the research highlights that the increasing influence of social networks on espionage poses challenges to diplomatic security and demands new paradigms of information governance. International cooperation and stricter regulations may be key strategies to mitigate the risks associated with this new reality, ensuring greater transparency and security in the use of social networks for intelligence purposes.

INTRODUÇÃO

Desde os tempos embrionários bem como no cenário contemporâneo das relações internacionais, a espionagem sempre desempenhou um papel fundamental na dinâmica dos fluxos de interações entre Estados, influenciando decisões estratégicas e moldando alianças e rivalidades. Historicamente, as actividades de inteligência eram tradicionalmente conduzidas por serviços secretos de alta especialização, operando sob um código rígido de sigilo.

No entanto, com o advento da era digital e a popularização das modernas redes

sociais enquanto ferramentas de conectividade e difusão de informação, o paradigma da espionagem passou por uma transformação significativa. Hoje, plataformas como Facebook, Twitter, Instagram e TikTok, inicialmente concebidas para interação social, têm sido utilizadas como ferramentas estratégicas e sigilosas para a coleta de informações, disseminação de narrativas políticas e monitoramento de adversários, ampliando o escopo das redes de espionagem interna e externa.

Desta feita, os Estados, bem como actores não estatais, têm procurado navegar nas redes sociais para fins de inteligência e contrainteligência, explorando vulnerabilidades tecnológicas e o vasto volume de dados disponíveis na esfera digital. Exemplos recentes, como as campanhas de desinformação em eleições e as denúncias de interferência estrangeira, demonstram como essas plataformas são instrumentalizadas para obter vantagens políticas e diplomáticas. Além disso, a interconectividade global que promove as redes sociais, permite que os governos monitorem dissidentes, influenciem a opinião pública internacional e conduzam operações encobertas sem a necessidade de agentes físicos infiltrados.

Diante desse cenário, este artigo procura examinar o impacto das redes de espionagem interna e externa nas relações diplomáticas, com um olhar específico sobre o papel das redes sociais modernas. A análise se baseia em estudos de caso e revisão bibliográfica, buscando compreender os desafios que a crescente digitalização da espionagem impõe à segurança diplomática e à estabilidade das relações internacionais. O objectivo é refletir sobre as implicações dessa nova realidade e discutir possíveis estratégias para mitigar os riscos associados ao uso estratégico das redes sociais no campo da inteligência global.

1. ABORDAGEM CONCEIPTUALISTA DA ESPIONAGEM

No âmbito das relações internacionais, a espionagem é uma prática antiga, mas que se mantém relevante e em constante evolução no mundo contemporâneo. É uma prática que contempla um conjunto de actividades destinadas à coleta, análise e utilização de informações sensíveis sobre governos, empresas, indivíduos e organizações.

Essas informações são obtidas de forma sigilosa e, muitas vezes, sem o consentimento dos alvos, com o objectivo de obter vantagens estratégicas, políticas, militares ou econômicas. Há uma variedade de autores que exploram conceitos digamos mais contemporâneos sobre a espionagem no século XXI, enfatizando seu papel na segurança nacional e nas Relações Internacionais.

Considerando a visão de Andrew (2009), podemos conceber a espionagem como sendo uma actividade que cinge-se na obtenção clandestina de informações sobre os interesses de um Estado ou entidade através de fontes humanas ou técnicas, cujo objectivo é garantir a segurança e os interesses nacionais.

Complementando a ideia acima, Herman (1996), considera que a espionagem é uma das vertentes fundamentais da inteligência, sendo distinta das actividades de contraespionagem e segurança. Na perspectiva do autor, a espionagem envolve técnicas avançadas de coleta de informações, incluindo vigilância eletrônica, infiltração em redes de comunicação e recrutamento de agentes infiltrados.

O mesmo autor também chama atenção para a crescente digitalização da espionagem no século XXI, onde ataques cibernéticos e vigilância eletrônica tornaram-se ferramentas predominantes desse tipo de actividade.

Sintetizando as visões acima apresentadas, Johnson (2018), amplia o conceito de espionagem para incluir a "guerra da informação", onde segundo o autor, os governos e organizações privadas utilizam métodos clandestinos para influenciar a opinião pública, manipular as eleições e desestabilizar economias de partes adversárias. Dito isto, a espionagem

moderna vai além da coleta de informações sigilosas, abrangendo também operações psicológicas e de desinformação.

1. Espionagem na Era Digital e a Transformação dos Métodos

Com a explosão da globalização acompanhada com as novas Tecnologias da Informação e Comunicação (TICs), a espionagem sofreu uma transformação muito impactante. Tal evento não foi ignorado no âmbito da actualização dos novos métodos de espionagem, pois que, autores como Richard Aldrich (2010) e Eric O'Neill (2020), destacam que o campo da inteligência moderna se deslocou do tradicional uso de agentes infiltrados para uma abordagem mais cibernética e digital.

Ou seja, se anterior modelo de actividades de espionagem baseava-se no uso de agentes em campo para a coleta de informações de forma clandestina, hoje, com o eclodir das novas tecnologias, tal actividade ganhou um novo escopo de actuação.

Segundo Aldrich, (2010), a espionagem na era digital está cada vez mais interessada na interseção entre tecnologia e política, onde ataques cibernéticos, vigilância eletrônica e big data têm sido ferramentas essenciais para a obtenção de informações estratégicas. A título de exemplo, podemos citar a famoso caso das denúncias de Edward Snowden em 2013 sobre a Agência de Segurança Nacional (NSA) dos Estados Unidos, onde se verificou de forma nua como a vigilância digital tem se tornado em um elemento central das actividades de espionagem global.

O'Neill (2020), por sua vez, concebe que a espionagem cibernética não está apenas focada em coletar informações sigilosas ou estratégicas tal como pontua Aldrich, mas também na manipulação dos dados e influenciar eventos políticos e econômicos globais.

O caso das interferências russas nas eleições americanas de 2016 que determinou a primeira Administração Trump, documentado por investigações oficiais , se configura num dos grandes exemplos sobre como a espionagem nos moldes digital se tornou nos últimos anos, uma ferramenta de guerra híbrida.

Do ponto de vista tipológico, a actividade de espionagem pode ser dividida em diferentes categorias, tendo em conta a natureza do alvo em questão e dos métodos utilizados. Sobre este olhar, os autores Warner (2002) Jackson (2019), tipificam a espionagem moderna nas seguintes categorias:

a) Espionagem Militar: uma actividade focada na obtenção de informações sobre capacidades, estratégias e movimentações de forças armadas de Estados ou grupos adversários.

b) Espionagem Industrial e Econômica: um actividade mais voltada na obtenção de segredos comerciais e avanços tecnológicos de empresas concorrentes. De acordo com Schweizer (2015), as grandes potências como a China e Estados Unidos têm procurado empregar operações de espionagem para roubar segredos industriais e fortalecer as suas economias.

c) Espionagem Cibernética: tal como é apresentado por Schneier (2015), trata-se de uma actividade que vincula o uso de ataques de forma digitalizada para obter informações estratégicas, desestabilizar infraestruturas e manipular redes de comunicação. No escândalo da NASA, Edward Snowden revelou a magnitude das operações cibernéticas da referida agência americana, evidenciando como os Estados modernos na época contemporânea, dependem desse tipo de espionagem.

d) Espionagem Política: uma actividade que envolve a infiltração e manipulação de processos políticos estrangeiros, através da indexação de agentes. Johnson (2018), é bastante enfático ao evidenciar de forma abrangente sobre como os serviços de inteligência utilizam os seus agentes para influenciar eleições, recrutar políticos e minar governos adversários.

Face ao que fora apresentado, fica claro que espionagem, está longe de ser um considerado como apenas um fenômeno do passado, pois, tornou-se num dos pilares fundamentais da política internacional e da segurança global no século XXI.

Na medida em que novas tecnologias vão emergindo, os métodos que acompanham tal activadade, desde coleta e manipulação de informações continuam a evoluir, ampliando tanto as capacidades dos serviços de inteligência quanto os desafios éticos e jurídicos que enfrentam. Este facto leva-nos a crer que a espionagem é uma prática inevitável em um mundo interconectado, onde a informação é um recurso estratégico essencial. Seja na coleta de segredos militares, na espionagem cibernética ou na manipulação política, a inteligência clandestina continua a moldar as dinâmicas de poder entre Estados e corporações.

2. ESPIONAGEM E RELAÇÕES INTERNACIONAIS

A espionagem tem sido uma ferramenta essencial na formulação de políticas de segurança e estratégias de Estado desde os tempos antigos. Em um mundo onde a informação se constitui num elemento de poder, os serviços de inteligência desempenham um papel fundamental na manutenção do equilíbrio global. Desta maneira, compreender a evolução das redes de espionagem, o uso da espionagem como ferramenta de poder nas relações diplomáticas e casos históricos relevantes e suas consequências diplomáticas constituem temáticas importantes a serem exploradas.

Não é de todo novo, reconhecermos que a espionagem sempre foi parte integrante das relações entre os Estados, evoluindo ao longo da história e se adaptando às variadas mudanças tecnológicas e geopolíticas. Desde a Antiguidade, quando líderes políticos faziam recursos a informantes e espiões para monitorar rivais, até a era digital, onde os dados são coletados em uma escala massiva, a espionagem continua a ser um componente-chave da segurança nacional.

Olhemos o exemplo da antiga China, onde de facto,a espionagem era um componente essencial da guerra e da política. Sun Tzu, no século V a.C., no seu conceituado livro A Arte da Guerra, enfatiza a espionagem como uma ferramenta essencial para a vitória, destacando a importância do conhecimento do inimigo e do uso de agentes secretos, “se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas.”

Dessa maneira, é mister refletirmos que o seu papel enquanto ferramenta de influência nas relações internacionais evidencia o modo como o conhecimento antecipado das intenções e capacidades de adversários sempre foi uma vantagem crucial para Estados no âmbito do estabelecimento de suas relações.

A interseção entre espionagem e diplomacia constitui-se num ponto central na geopolítica moderna. Historicamente, tendo em vista a observação de Herman (1996), a espionagem tem assumido um papel dualista, enquanto instrumento de estabilidade e desestabilização. Ou seja, se por um lado ela permite que os Estados previnam ataques e ajustem suas estratégias com base em informações concretas, por outro, também tem sido um factor de crises diplomáticas e desconfiança internacional.

Dessa forma, a evolução da espionagem acompanha as mudanças da ordem internacional, adaptando-se aos desafios de cada época.

2.1 Espionagem como ferramenta de poder nas relações diplomáticas

A espionagem é um recurso essencial para os Estados na condução da diplomacia e na formulação de políticas externas. Conforme observado por Rid (2020), o objectivo central da inteligência é reduzir a incerteza no ambiente internacional, fornecendo informações críticas sobre as intenções e capacidades de outros Estados.

Por meio da coleta de informações privilegiadas, os Estados conseguem influenciar negociações internacionais, prever crises e mitigar ameaças potenciais. Essa ideia é complementada por Warner (2014), ao considerar que a espionagem não é apenas um instrumento defensivo, mas também uma ferramenta ofensiva utilizada para moldar a política internacional.

A espionagem está profundamente enraizada na geopolítica, sendo utilizada como instrumento de projeção de poder. Tal

perspectiva foi profundamente visível durante a Guerra Fria, onde os Estados Unidos e a União Soviética empregaram vastos recursos na coleta de informações estratégicas, influenciando decisões diplomáticas e militares. Em observância a isto, West (2017), descreve que, as agências de inteligência, como a CIA (do EUA) e a KGB (RÚSSIA), desempenharam um papel crucial na formulação das políticas externas de suas respectivas nações.

Devido a importância desse tipo de actividade que potencializa ações estratégicas por parte dos Estados, nos dias actuais, o equilíbrio de poder entre Estados é profundamente influenciado pela capacidade de conduzir operações de espionagem eficazes. No caso concreto da China e a Rússia, por exemplo, têm sido acusadas rotineiramente de realizar campanhas de ciberespionagem contra os Estados Unidos e a própria União Europeia, buscando cada vez mais vantagens econômicas e estratégicas. (DAWSON & RAHMAN, 2022).

Dessa forma, a espionagem tornou-se uma dimensão essencial da competição geopolítica moderna. De acordo com Buchanan (2020), a ciberespionagem é um dos desafios mais significativos da diplomacia contemporânea, pois dificulta a atribuição de responsabilidade e pode levar a retaliações inadvertidas.

Sobre essa premissa, tal como já fora referido nas seções anteriores, podemos olhar a suposta interferência russa nas eleições presidenciais dos EUA em 2016 e os ataques cibernéticos chineses contra empresas ocidentais para roubo de propriedade intelectual. (HARKNETT & GOLDMAN, 2017). Tais episódios evidenciam como a espionagem cibernética tem o potencial de desestabilizar relações diplomáticas e comprometer a segurança internacional.

Outro aspecto importante a ser mencionado é que a espionagem, além de fornecer informações valiosas para a tomada de decisão, também é empregada como instrumento de influência política. Operações de desinformação e propaganda são utilizadas para manipular opinião pública e enfraquecer adversários. Como argumenta Galeotti (2019), regimes autoritários frequentemente empregam campanhas de desinformação para minar a confiança nas instituições democráticas e ampliar sua influência global.

Além disso, a espionagem pode ser usada para obter alavancagem em negociações diplomáticas. A coleta de informações sobre a vida privada de líderes políticos (adversários de outras nações) tal como demonstra a história, tem sido usada rotineiramente para chantagem e coerção, alterando a dinâmica do poder internacional. (LEVINE, 2021).

Dito isto, vale reconhecermos que espionagem continua sendo uma ferramenta essencial de poder nas relações diplomáticas, desempenhando um papel crucial na segurança nacional e na formulação de políticas externas. Em um mundo cada vez mais interconectado, a espionagem não se limita apenas às práticas tradicionais, mas se expande para o ciberespaço, a desinformação e a guerra psicológica.

3. CASOS HISTÓRICOS RELEVANTES DE ESPIONAGEM E SUAS CONSEQUÊNCIAS DIPLOMÁTICAS

1. O Caso Dreyfus (1894-1906)

O caso Dreyfus não foi um episódio clássico de espionagem internacional como tal, mas sim uma acusação de traição dentro do exército francês. O capitão Alfred Dreyfus, judeu, foi falsamente acusado de fornecer segredos militares franceses à Alemanha (acusado de prática de espionagem). Sua condenação gerou um profundo racha na sociedade francesa e evidenciou o antissemitismo no Exército e na elite política. A revelação da falsificação de provas por parte da inteligência militar francesa levou a uma crise diplomática interna e externa, colocando a França sob escrutínio internacional.

Como aponta Hannah Arendt no seu livro As Origens do Totalitarismo (1951), a instrumentalização do antissemitismo na política europeia ganhou destaque nesse período, sendo o caso Dreyfus um exemplo emblemático da conexão entre preconceito racial e interesses de Estado.

A imprensa britânica, alemã e americana acompanhou de perto o desenrolar do caso. Durante aquele período, o jornal The Times de

Londres (EUA), frequentemente publicava editoriais críticos ao governo francês, destacando a injustiça cometida contra Dreyfus e questionando a credibilidade da República Francesa. Com base em Arendt (1951), a cobertura internacional colocou pressão sobre a França para revisar o processo, evidenciando a conexão entre justiça interna e prestígio externo.

A crise levou à queda do governo do primeiro-ministro francês Jules Méline e ao fortalecimento de líderes republicanos comprometidos com a revisão do caso, como Pierre Waldeck-Rousseau. A crise de confiança nas instituições militares impulsionou reformas dentro do exército e influenciou a separação definitiva entre Igreja e Estado na França (Lei de 1905), conforme detalhado por Maurice Agulhon em The French Republic 1879–1992 (1993).

2. O Telegrama Zimmermann (1917)

Durante a Primeira Guerra Mundial, os serviços de inteligência britânica interceptou e decifrou um telegrama enviado pelo ministro das Relações Exteriores alemão, Arthur Zimmermann, ao México. No telegrama, a Alemanha prometia apoio militar ao México caso este declarasse guerra aos Estados Unidos. Os britânicos divulgaram o conteúdo do telegrama aos americanos, o que inflamou a opinião pública dos EUA e contribuiu decisivamente para a entrada do país na guerra ao lado da Tríplice Entente.

O telegrama foi enviado precisamente no dia 16 de janeiro de 1917, utilizando as redes diplomáticas alemãs, que passavam pelo sistema telegráfico submarino controlado pelo Reino Unido. Os britânicos naquela altura possuíam um programa avançado de interceptação de comunicações inimigas, baseado na famosa Room 40, a unidade de decifração do Almirantado britânico. Como destaca o historidador Kahn (1967), a Room 40 já vinha monitorando as comunicações alemãs desde o início da guerra e já havia quebrado vários códigos cifrados.

Os criptógrafos britânicos conseguiram decifrar a mensagem de Zimmermann, que continha a seguinte proposta ao México:

"Caso os Estados Unidos entrem na guerra contra a Alemanha, ofereceremos apoio financeiro e militar para que o México recupere os territórios do Texas, Arizona e Novo México."

O referido telegrama, para além de sugerir uma aliança militar a ser criada, indicava também que a Alemanha em breve daria início a uma guerra submarina, o que significava implicitiamente que embarcações americanas seriam alvos directos.

Após a decifração, conforme descrito por Nicholas Rankin no seu livro A Genius for Deception: How Cunning Helped the British Win Two World Wars (2009), os britânicos enfrentaram um dilema estratégico: se revelassem o conteúdo do telegrama aos Estados Unidos, os alemães perceberiam que seu código havia sido comprometido, levando-os a mudar suas cifras. Para contornar esse problema, a inteligência britânica simulou ter obtido o telegrama através de agentes no México. Essa manobra garantiu que os alemães não suspeitassem imediatamente da quebra de seus códigos. (RANKIN, 2009)

O telegrama foi enviado ao governo Norte Americano no dia 24 de fevereiro de 1917 e rapidamente divulgado à imprensa. A revelação causou indignação pública nos Estados Unidos, onde crescia o sentimento anti-alemão. (RANKIN, 2009)

Como destaca Tuchman (1958), a publicação da mensagem reforçou a percepção de que a Alemanha era uma ameaça directa à segurança americana. O impacto foi intensificado pela confirmação de sua autenticidade pelo próprio Arthur Zimmermann, que admitiu publicamente o conteúdo da mensagem em março de 1917.

Como resultado desses eventos, exatamente no dia 6 de abril de 1917, os Estados Unidos declararam guerra à Alemanha, marcando um ponto de virada no conflito. A entrada dos EUA trouxe um enorme impulso econômico e militar à Tríplice Entente, contribuindo significativamente para a derrota alemã datada em 1918.

3. O Caso Rosenberg (1950-1953)

O caso de Julius e Ethel Rosenberg (1950-1953) é também olhado como sendo um dos episódios mais controversos da história

durante o período da Guerra Fria, marcado pela interseção entre espionagem, política e o clima de medo gerado pelo anticomunismo nos Estados Unidos.

O final da Segunda Guerra Mundial consolidou o mundo bipolar, com os Estados Unidos e a União Soviética emergindo como superpotências rivais. A superioridade nuclear americana foi demonstrada com os bombardeios de Hiroshima e Nagasaki (1945), mas em 1949, os soviéticos surpreenderam o mundo ao testar sua primeira bomba atômica. Em decorrência a isto, tal como menciona Holloway (1994), a União Soviética alcançou esse avanço por meio de uma combinação de esforços científicos próprios e informações obtidas por espionagem.

Segundo o autor, os EUA responderam com uma intensa investigação para identificar os responsáveis pelo vazamento de segredos nucleares. Foi nesse contexto que os nomes de Julius e Ethel Rosenberg emergiram como suspeitos centrais. (HOLLOWAY 1994)

Os irmãos Julius Rosenberg de 35 anos e Ethel Rosenberg de 37 anos na altura, foram acusados de fornecer segredos nucleares à União Soviética, e em consequência a isto, ambos foram condenados à morte e executados em 1953 na cadeira elétrica na prisão de Sing Sing, tornando-se símbolos tanto da suposta traição interna quanto dos excessos do macarthismo . O caso ilustra o papel da inteligência na política internacional e como a Guerra Fria transformou a espionagem em um campo de batalha ideológico.

Do ponto de vista diplomático, esta ocorrência aumentou significativamente a tensão entre EUA e URSS no início da Guerra Fria, influenciado massivamente na expansão das operações da CIA e do FBI contra suspeitos de espionagem comunista, e como se não bastasse houve também o reforço da corrida armamentista nuclear entre as superpotências. (HOLLOWAY 1994)

Ainda no quadro da repercussão diplomática, tal como foi observado por Powers (1998), internacionalmente, a execução dos Rosenberg repercutiu de forma negativa para os EUA, sendo vista como um reflexo do autoritarismo do macarthismo, onde, enquanto os EUA se apresentavam como defensores da democracia, casos como esse revelavam um lado repressivo do sistema político americano.

Portanto, esses exemplos acima, demonstram claramente que a espionagem sempre foi um elemento fundamental das relações internacionais, muitas vezes sendo o catalisador para mudanças de alianças, guerras ou transformações na ordem global. Como demonstram os casos apresentados, suas consequências diplomáticas podem ser devastadoras, seja ao desmascarar planos inimigos, comprometer relações entre aliados ou alterar o equilíbrio de poder.

4. O PAPEL DAS AGÊNCIAS DE INTELIGÊNCIA NA ERA DIGITAL

O papel das agências de inteligência na era digital tem se tornado cada vez mais complexo e essencial diante dos constantes avanços tecnológicos e em especial, da própria expansão das redes digitais. O fluxo massivo de informações, a interconectividade global e a crescente ameaça cibernética têm sido ícone de transformação das operações de inteligência, exigindo novas abordagens e ferramentas para lidar com desafios emergentes.

Devido as possibilidades que a era digital garante as sociedades e aos Estados em particular, a coleta de dados para fins estratégicos em diferentes domínios do interesse dos Estados, tem sido uma das principais actividades das agências de inteligência. Esta ideia é profundamente defendida por Rid (2020), que na sua obra, aborda que a espionagem desta era contemporânea depende fortemente da interseção entre a tecnologia e informação. Dito isto, é através da vigilância eletrônica, monitoramento de comunicações e análise de grandes volumes de dados, que as agências conseguem de facto identificar as potenciais ameaças e antecipar os riscos à segurança dos Estado.

O outro aspecto importante adicional ao papel das agências de inteligência na presente era digital, além da coleta de informações, é sem dúvidas a famosa guerra cibernética, que cada vez mais tem se tornado numa dimensão estratégica fundamental para as agências.

Em observância a isto, os autores Singer e Friedman (2014), consideram que constantemente os Estados financiam os hackers para realizar um conjunto de ataques contra infraestruturas, obter de forma ilícita informações sigilosas e desestabilizar os potenciais adversários. Os mesmos autores complementam dizendo que o ciberespaço é hoje um dos principais campos de batalha da geopolítica, onde os Estados disputam informações e exercem influência através de ataques sofisticados.

Outro aspecto a considerar é que as agências de inteligência também desempenham um papel crucial no combate à desinformação. Muitas plataformas digitais como redes socias do Facebook e Twitter têm sido usadas pelos Estados e ate mesmo grupos com vontades hostis para disseminar a variedade de informações falsas (fake news) e consequentemente manipular reações públicas e até mesmo eleições. (BENKLER, FARIS & ROBERts, 2018).

Podemos aqui olhar o caso que levou a investigação sobre a interferência russa nas eleições americanas em 2016, tal facto demonstrou claramente o poder das redes sociais para influenciar a opinião pública, expondo a vulnerabilidade das democracias frente a essa nova forma de guerra informacional.

Entretanto, o papel das agências de inteligência na era digital também levanta questionamentos éticos e desafios do ponto de vista regulatório. Dito isto, reconhece-se inequivocamente que o uso de ferramentas de monitoramento em massa (usadas muitas vezes pelas agências de inteligência para combater a desinformação e obter dados) pode gerar conflitos com os direitos fundamentais, como o direito á privacidade e liberdade individual, no caso concreto do nosso país consagrado no art.º 32 da constituição da república de Angola.

Outro ponto a discutir é que o próprio direito internacional ainda encontra inúmeras dificuldades para gerar ou estabelecer parâmetros claros para a actuação dessas agências sem comprometer a segurança global. E tal facto é destacado por Zuboff (2019), o qual considera que o avanço da vigilância digital desafia os limites da democracia e exige maior transparência na governança dos dados.

5. AS AGÊNCIAS DE INTELIGÊNCIA ANGOLANAS

As agências de inteligência angolanas, assim como as mais variadas agências de alta notoriedade ao nível mundial, desempenham um papel crucial quer no âmbito da segurança nacional, quer na proteção das instituições do Estado bem como na estabilidade política do país.

Dentre elas, destacam-se o Serviço de Inteligência e Segurança do Estado (SINSE), o Serviço de Inteligência Militar (SIM) bem como o Serviço de Inteligência Externa (SIE), os quais são apontados como os principais órgãos responsáveis por essas actividades, actuando no combate às ameaças internas e externas, incluindo até mesmo o terrorismo, a espionagem e crime organizado.

Vale destacar que desde a independência do país, datada em 1975, os serviços de inteligência do Estado Angolano têm sido moldados por vários factores que estão intrinsecamente ligados aos contextos políticos e de segurança do país. Olhemos por exemplo o contexto da guerra fria e da própria guerra civil angolana como um dos episódios ilustrativos (1975-2002), onde verificou-se de facto que as agências de inteligência tiveram um papel essencial na luta contra movimentos da oposição e de determinados grupos considerados rebeldes, bem como na manutenção do poder do Movimento Popular de Libertação de Angola (MPLA).

Tendo em conta o considerável apoio recebido pelos seus diversos aliados soviéticos , os serviços de inteligência do Estado angolano utilizou um conjunto de técnicas de contraespionagem e vigilância para garantir a supremacia do governo central.

Com os episódios que marcaram de facto a pacificação (2002) do país e a transição para um Estado mais institucionalizado e multipartidário, as referidas agências de inteligência acabaram por ganhar novos desafios em termo. Face a isto, a questão da segurança econômica e a proteção de infraestruturas estratégicas, como o sector

petrolífero e mineiro, acabaram por se tornarem prioridades, visto que o crescimento econômico de Angola atraiu diversos interesses externos.

Esta na verdade foi uma jogada estratégica defendida por Goldsmith (2018), o qual pontua que nos países em desenvolvimento, as agências de inteligência são frequentemente mobilizadas para garantir a estabilidade política e econômica, em vez de se focarem exclusivamente em ameaças tradicionais.

No entanto, no contexto da espionagem, as agências supracitadas têm adaptado as suas estratégias para enfrentar ameaças modernas, incluindo a questão da vigilância digital. Há uma variedade de Relatórios que indicam que, em 2013 , o SINSE adquiriu da empresa italiana Hacking Team uma tecnologia de foco na espionagem denominado “Remote Control System (RCS)”, capaz de decodificar senhas, acessar e obter documentos e interceptar conversas via Skype e outras redes de interação digital. Essa aquisição sugere um esforço do SINSE para aprimorar suas capacidades de vigilância no ambiente digital, acompanhando a tendência global de monitoramento cibernético.

Actualmente, o papel das agências de inteligência em Angola também se estende à segurança cibernética e à proteção contra influências externas no ambiente digital. Tendo em vista acentuado nível de conectividade e da dependência das tecnologias da informação, os serviços de inteligência angolana têm procurado se adaptar a estas novas dinâmicas, modernizando gradualmente as suas técnicas de monitoramento para lidar com os crimes cibernéticos e a disseminação de desinformação nas redes sociais.

Nesse contexto, trazendo aqui a visão de Rid (2020), a guerra informacional tornou-se uma das principais frentes da inteligência moderna, especialmente em regimes que buscam manter a coesão interna.

Entretanto, desafios como a transparência e a necessidade de controle democrático sobre as agências de inteligência permanecem em pauta gerando vários debates e opiniões públicas diversas. Questões éticas são levantadas principalmente em matérias ligadas aos direitos fundamentais, o que reforça a ideia de que a operacionalização dessas estruturas de inteligência deviam ter uma vigilância independente que pudesse monitorar os modos operandos e justificativas das agências.

No caso concreto do Estado angolano, já é música de longas datas a discussão em torno do equilíbrio entre segurança nacional e respeito aos direitos civis, o qual continua sendo um desafio, despertando novas visões cada vez mais reformistas para tornar a actuação da inteligência mais eficiente e alinhada com princípios democráticos. Embora que, numa perspectiva do realismo clássico pontuado por Maquiavel, os interesses do estado estão acima da moral comum, é imperioso que se justifiquem os meios e as ocasiões que tais interesses sobrevalorizem os direitos fundamentais.

Deste modo, em síntese, vale-nos afirmar que as agências de inteligência angolanas desempenham um papel fundamental na defesa do Estado, mas também enfrentam a necessidade de adaptação aos novos desafios contemporâneos. A modernização dos serviços, o reforço da segurança digital e a implementação de mecanismos de supervisão mais transparentes serão decisivos para garantir que a inteligência continue a servir aos interesses nacionais sem comprometer os direitos fundamentais dos cidadãos.

6. REDES SOCIAIS COMO FERRAMENTA DE INTELIGÊNCIA E CONTRAINTELIGÊNCIA

As redes sociais tornaram-se hoje num universo privilegiado para o fluxo de informações em escala global, desempenhando assim um papel bastante preponderante na comunicação contemporânea. No entanto, apesar de vulgarmente serem olhadas apenas para uso cotidiano de interação social virtualmente, tais redes também podem se consolidar em ferramentas estratégicas para operações de inteligência e contrainteligência constituindo-se nisto, o nosso foco e análise e reflexão.

Já não é nenhuma novidade, ou pelo menos até a data presente, que muitos

Estados, corporações e até mesmo certos indivíduos têm utilizado as famosas plataformas como Facebook, Twitter, Instagram e TikTok não apenas para disseminação de informações, mas também para coleta de dados, análise comportamental, disseminação de desinformação ou fake news e até mesmo influência política. A ascensão da tecnologia digital bem como a presença acentuada das redes sociais no mundo, reformularam consideravelmente o ambiente informacional, tornando-o um campo fértil para actividades de monitoramento, manipulação e defesa cibernética.

Dito isto, os serviços de inteligência, isto no contexto das redes sociais, estão associadas às suas capacidades de obterem e interpretar as informações relevantes a partir dos dados disponíveis nessas plataformas e consequentemente fazerem com elas uma gestão e posteriormente uso estratégico. Esta linha de pensamento é reforçada por Zuboff (2019), que destaca que a economia da vigilância tornou-se um pilar fundamental do capitalismo digital, onde as redes sociais coletam massivamente dados dos usuários para prever e influenciar comportamentos.

Um facto bastante curioso que levanta inquietações e questões alvo de reflexão do presente estudo é o facto de, para se tornar parte dessas plataformas (ter acesso) a condição sine qua non é fazer inscrição com seus dados pessoais para aceite naquela comunidade virtual. Ao reconhecermos esta factualidade, estamos a admitir que os dados compartilhados voluntariamente pelos usuários, que vão desde postagens e curtidas até localização e padrões de interação, fornecem um volume vasto de informações passíveis de análise e uso potencialmente estratégicos para quem recolhe e detém tais dados.

Hoje, com a evolução das técnicas de mineração de dados e inteligência artificial aprimoraram-se a capacidade de mapear perfis, prever comportamentos e identificar tendências sociopolíticas. Essa realidade faz com que as redes como Facebook se tornem verdadeiros bancos de dados para governos e corporações interessados em compreender o comportamento de massas e indivíduos específicos, e consequentemente minar informações nas redes para conduzir tais massas ou manipular opinião publica.

O facto acima detalhado é confirmado pelo pesquisador Andrejevic (2020), o qual aponta que o uso desses dados pode ser decisivo para campanhas eleitorais, estratégias de marketing e até mesmo para operações de segurança nacional.

Face a isto, é chamado aqui um dos conceitos interessantes a temática, no caso, a contrainteligência. Na perspectiva de Olson (2006), a contrainteligência, por sua vez, refere-se às estratégias desenvolvidas para impedir ou mitigar a obtenção de informações sensíveis por agentes adversários através do recurso a espionagem sabotagem, subversão ou outras ameaças promovidas pelos serviços de inteligência estrangeiros.

Considerando que o actual ambiente digital promove de forma voluntaria a alta exposição dos indivíduos e estruturas institucionais, as operações de contrainteligência nas redes sociais envolvem desde campanhas de desinformação até a criação de perfis falsos para enganar e desviar tentativas de monitoramento.

Olhemos por exemplo a visão de Rid (2020), o qual afirma que a guerra de informação moderna envolve não apenas a coleta, mas também a manipulação de dados, criando realidades paralelas que favorecem determinados grupos. Entretanto, os Estados que percebem as ameaças cibernéticas provenientes de potências estrangeiras ou grupos opositores, normalmente e de forma antecipada, fazem recurso aos métodos avançados para proteger sua soberania nos moldes digitais, adotando práticas que variam desde regulamentações mais rígidas até estratégias ofensivas para neutralizar adversários no ciberespaço-selvagem. Não é sem razão que temos vistos países a criarem várias legislações de regulação e até mesmo de proibição de uso de certas redes sociais.

Pese embora haja várias redes sociais no interior do ciberespaço, o Facebook é um exemplo um pouco mais feliz para uma análise da dualidade entre inteligência e contrainteligência no ambiente digital. Sua estrutura algorítmica favorece a segmentação

detalhada de públicos, permitindo que informações sejam direcionadas de maneira extremamente precisa.

Em função disto, muitos governo, empresas privadas e grupos, procuram explorar essas variáveis para fins de vigilância e manipulação da opinião pública. Um dos grandes exemplos disto foi o caso que gerou escândalo da Cambridge Analytica , evidenciaram a capacidade das redes sociais de influenciar processos democráticos por meio do direcionamento seletivo de conteúdos.

Tal como foi discutido por Cadwalladr (2019), o uso intensivo de dados pessoais para previsões comportamentais levanta questões sobre privacidade, ética e a própria natureza da democracia contemporânea.

Por outro lado, tal como já fizemos referência no início deste tópico, o TikTok é também outra rede social de forte manuseio das agências de inteligência para despoletar quer actos e espionagem quer actos de desinformação e manipulação. No entanto, é importante distinguirmos que TikTok emergiu como uma plataforma distinta, tanto pela sua base de usuários quanto pelo seu modelo de funcionamento.

Diferentemente do Facebook, que construiu seu império a partir de conexões interpessoais e compartilhamento de conteúdos, o TikTok opera com um sistema algorítmico altamente responsivo, baseado no consumo de vídeos curtos e na rápida adaptação aos interesses do usuário. Isso o torna uma ferramenta poderosa para disseminação de narrativas, especialmente entre públicos mais jovens e menos expostos aos meios tradicionais de comunicação.

Disto isto, nos últimos anos, foi notório a crescente preocupação com a influência chinesa na plataforma, o que fez com que muitos países como os Estados Unidos chegassem a discutir medidas de restrição e monitoramento, demonstrando como as redes sociais podem se tornar arenas de disputa geopolítica. Nesta linha de ideia, Mozur (2021), assinala que a possibilidade de coleta massiva de dados e a imprevisibilidade do alcance viral de conteúdos específicos fazem com que o TikTok seja considerado uma ameaça por governos que priorizam a soberania digital e a segurança nacional.

Outro detalhe importante que vale ser mencionado é que a dinâmica entre inteligência e contrainteligência nas redes sociais não se limitam apenas à questões de vigilância estatal. Isto porque as Organizações não governamentais, os grupos activistas e até indivíduos comuns adotam estratégias para proteger suas informações ou, ao contrário, ampliar sua capacidade de persuasão e mobilização.

O fenômeno das fake news e a criação de narrativas artificiais têm bastante acentuação junto dessa plataforma através das recentes IA (inteligência artificial). Tal como enfatiza Wardle (2020), a propagação de conteúdos fabricados ou distorcidos pode gerar instabilidade social, alterar percepções e até influenciar políticas públicas, e tem sido bastante comum, vermos no TikTok a publicação de vários vídeos falsos de entidades e até mesmo discursos audiovisuais criados pelas IA.

Portanto, o ambiente selvagem que o ciberespaço das redes socias proporciona, implica elevados desafios na agenda geopolítica global, gerando diversas adaptações e tendências inovadores dos serviços de inteligência dos mais variados países.

7. OS DESAFIOS DA REGULAÇÃO DAS REDES SOCIAIS NO CONTEXTO DA ESPIONAGEM

Devido a natureza das redes sociais e o seu nível de alcance em termos de usuários e actividades nelas desenvolvidas por tais usuários, desde pessoas individuais e colectivas, faz com que a regulação dessas plataformas apresenta desafios significativos, uma vez que envolve um equilíbrio delicado entre segurança nacional, liberdade de expressão e soberania digital.

Um dos principais desafios regulatórios que podemos apontar reside exatamente na identificação e no combate à disseminação de desinformação promovida pelos actores estrangeiros. A referência dessa afirmação pode ser demonstrada nas investigações realizadas sobre a interferência eleitoral nos

Estados Unidos e na Europa, onde verificou-se claramente as ações de determinados governos estrangeiros a utilizarem as plataformas como Facebook e Twitter para influenciar eleições e dividir a sociedade. (RID, 2020).

O problema é que, ao tentar regular esse fenômeno, os governos frequentemente enfrentam resistências ligadas à liberdade de expressão e de acesso a informação. Face a isto, a coleta massiva de dados por meio das redes sociais acaba sendo um pivô bastante preocupante no que toca a espionagem e segurança nacional.

Em rezões disto, em 2020, os Estados Unidos da América ameaçaram a banir o TikTok devido a preocupações com a influência do governo chinês sobre a empresa, alegando riscos à segurança nacional. (MOZUR, 2021). Esse caso ilustra como a regulação de redes sociais muitas vezes se confunde com disputas geopolíticas e preocupações com soberania digital.

Outro grande desafio que também pode ser apontado é a questão da harmonização de regulações em um cenário global. Ou seja, é visivelmente notório nos últimos anos, o modo como os Estados adotam abordagens próprias, para regular as redes sociais, emancipando de forma nua uma divergência de regulações.

Enquanto a União Europeia tem implementado leis como o Regulamento Geral sobre a Proteção de Dados (GDPR) para restringir a coleta e o uso de informações pessoais, outros países, como é o caso da China e da Rússia, optaram por um controle mais rigoroso sobre o conteúdo e as actividades das empresas de tecnologia. Essa fragmentação regulatória pode dificultar a cooperação internacional em matéria do combate à espionagem digital e à manipulação de informação.

Um aspecto muito interessante que vale ser mencionado, reside no papel que as grandes empresas de tecnologia exercem na regulação das redes sociais. Por um lado, essas empresas criam e implementam políticas de privacidade e segurança para proteger seus usuários. Mas por outro, o modelo de negócios dessas empresas baseia-se essencialmente na coleta de dados para publicidade direcionada, o que cria incentivos para minimizar as restrições regulatórias.

Esse comportamento é discutido por Zuboff (2019), o qual aponta que o capitalismo de vigilância transforma os dados pessoais em mercadoria, tornando as grandes plataformas digitais actores-chave no cenário da espionagem contemporânea.

Portanto, em resposta a esses desafios, muitos Estados têm procurado regulamentar as redes sociais por meio de legislações específicas em colaboração com as próprias plataformas digitais. No entanto, a eficiência dessas medidas depende da capacidade dos Estados de impor regras claras e de garantir transparência no funcionamento dos algoritmos. O debate sobre a regulação das redes sociais no contexto da espionagem continua a evoluir, refletindo as tensões entre segurança, privacidade e liberdade digital em um mundo cada vez mais interconectado.

CONSIDERAÇÕES FINAIS

A crescente interconectividade das redes sociais redefiniu o cenário da espionagem e da inteligência global, tornando-se uma ferramenta indispensável para Estados e actores não estatais. Como analisado ao longo deste estudo, as plataformas digitais não apenas facilitaram a coleta e análise de informações estratégicas, mas também criaram novos desafios para a segurança diplomática e a estabilidade das relações internacionais. A manipulação de narrativas, a disseminação de desinformação e a vigilância cibernética emergiram como práticas recorrentes, transformando o ambiente digital em um campo de disputa entre diferentes interesses geopolíticos.

A digitalização da espionagem revelou que a informação se tornou um recurso estratégico central no século XXI, onde big data, inteligência artificial e ataques cibernéticos desempenham papéis fundamentais na obtenção e manipulação de dados. Casos emblemáticos, como a interferência russa nas eleições americanas de 2016 e as operações de vigilância da NSA, demonstram que as redes sociais não são apenas espaços de socialização, mas também arenas para

conflitos informacionais que podem impactar a política global.

Diante desse cenário, a governança da informação e a regulamentação das redes sociais surgem como desafios cruciais para os Estados. Medidas como a adoção de marcos regulatórios mais rígidos, o fortalecimento da cooperação internacional e o desenvolvimento de tecnologias de segurança digital são essenciais para mitigar os riscos associados à espionagem digital. Além disso, a transparência das plataformas e a conscientização dos usuários sobre a manipulação de dados podem contribuir para a construção de um ambiente digital mais seguro e confiável.

Portanto, o impacto das redes sociais na espionagem moderna exige uma abordagem equilibrada entre inovação tecnológica, proteção da soberania digital e respeito aos princípios democráticos, garantindo que a inteligência global não comprometa os direitos individuais e a estabilidade das relações internacionais.

REFERÊNCIAS BIBLIOGRÁFICAS

1.AGULHON, Maurice. A República Francesa: 1879–1992. Blackwell, 1993.

2.ALDRICH, Richard J. GCHQ: A história não censurada da mais secreta agência de inteligência britânica. HarperPress, 2010.

3.ANDREJEVIC, Mark. Mídia automatizada. Routledge, 2020. Disponível em: https://doi.org/10.4324/9780429492413. Acesso em: 21 jul. 2025.

4.ANDREW, Christopher. A Defesa do Reino: A história autorizada do MI5. Allen Lane, 2009.

5.ARENDT, Hannah. Origens do totalitarismo. Harcourt, Brace & Co., 1951.

6.BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. Propaganda em rede: Manipulação, desinformação e radicalização na política americana. Oxford University Press, 2018.

7.BUCHANAN, Ben. O hacker e o Estado: Ciberataques e o novo normal da geopolítica. Harvard University Press, 2020.

8.CADWALLADR, Carole. O grande hack: Como o escândalo da Cambridge Analytica foi desvendado. The Guardian, Londres, 17 mar. 2019. Disponível em: https://www.theguardian.com/news/series/cambridge-analytica-files. Acesso em: 21 jul. 2025.

9.DAWSON, Laura; RAHMAN, Tariq. Ciberespionagem e rivalidades geopolíticas no século XXI. Journal of Cybersecurity and International Affairs, v. 8, n. 1, p. 45–67, 2022.

10.GALEOTTI, Mark. Precisamos falar sobre Putin: Por que o Ocidente o interpreta mal – e como corrigi-lo. Ebury Press, 2019.

11.GOLDSMITH, Andrew. Agências de inteligência e cooperação internacional: Poder e restrição em um mundo globalizado. In: JOHNSTON, Angus; WOOD, David (org.). Inteligência e a função do governo. Routledge, 2018. p. 95–114.

12.HARKNETT, Richard J.; GOLDMAN, Emily O. A busca pelos fundamentos do ciberespaço. Journal of Cybersecurity, v. 3, n. 1, p. 1–12, 2017. Disponível em: https://doi.org/10.1093/cybsec/tyx001. Acesso em: 21 jul. 2025.

13.HERMAN, Michael. O poder da inteligência em tempos de paz e guerra. Cambridge University Press, 1996.

14.HOLLOWAY, David. Stalin e a bomba: A União Soviética e a energia atômica, 1939–1956. Yale University Press, 1994.

15.JACKSON, Peter. Inteligência e Estado: Uma perspectiva global. Routledge, 2019.

16.JOHNSON, Loch K. Vigiando os espiões: A responsabilidade da inteligência nos Estados Unidos. Oxford University Press, 2018.

17.KAHN, David. Os decifradores de códigos: A história abrangente da comunicação secreta desde os tempos antigos até a internet. Macmillan, 1967.

18.LEVINE, Robert A. Vigilância e poder: A política global da informação. Palgrave Macmillan, 2021.

19.MOZUR, Paul. Por dentro da dança perigosa do TikTok com Pequim. The New York Times, Nova York, 25 jun. 2021. Disponível em: https://www.nytimes.com/2021/06/25/technology/tiktok-china-data.html. Acesso em: 21 jul. 2025.

20.O'NEILL, Eric. Dia cinzento: Minha missão secreta para expor o primeiro espião cibernético da América. Crown Publishing Group, 2020.

21.OLSON, James M. Jogo justo: Os dilemas morais da espionagem. Potomac Books, 2006.

22.POWERS, Richard G. Não sem honra: A história do anticomunismo americano. Yale University Press, 1998.

23.RANKIN, Nicholas. Um gênio da decepção: Como a astúcia ajudou os britânicos a vencer duas guerras mundiais. Oxford University Press, 2009.

24.RID, Thomas. Medidas ativas: A história secreta da desinformação e da guerra política. Farrar, Straus and Giroux, 2020.

25.SCHNEIER, Bruce. Dados e Golias: As batalhas ocultas para coletar seus dados e controlar seu mundo. W. W. Norton & Company, 2015.

26.SCHWEIZER, Peter. Impérios secretos: Como a classe política americana esconde a corrupção e enriquece familiares e amigos. Harper, 2015.

27.SINGER, Peter W.; FRIEDMAN, Allan. Cibersegurança e ciber-guerra: O que todos precisam saber. Oxford University Press, 2014.

28.TUCHMAN, Barbara W. O telegrama Zimmermann. Macmillan, 1958.

29.WARDLE, Claire. Compreendendo a desordem informacional. In: IRETON, Cherilyn; POSETTI, Julie (org.). Jornalismo, 'fake news' e desinformação: Manual para educação e treinamento em jornalismo. UNESCO, 2020. p. 19–36. Disponível em: https://en.unesco.org/fightfakenews. Acesso em: 21 jul. 2025.

30.WARNER, Michael. Inteligência e segurança nacional: Um manual de referência. ABC-CLIO, 2014.

31.WEST, Nigel. MI6: Operações do Serviço Secreto de Inteligência Britânico, 1909–1945. Weidenfeld & Nicolson, 2017.

32.ZUBOFF, Shoshana. A era do capitalismo de vigilância: A luta por um futuro humano na nova fronteira do poder. PublicAffairs, 2019.