OUVIDOS NAS PAREDES DIGITAIS: A NOVA ERA DA ESPIONAGEM MÓVEL

Thales Alecssander Molina Pereira[1], Frederico Silva Moreira[1]

[1]Universidade Federal de Mato Grosso do Sul, Campo Grande, Brasil
(thales.alecssander@ufms.br)

Resumo: Este artigo aborda a evolução da espionagem de dados diante do avanço das tecnologias e dos meios de comunicação. Disfarçada sob diferentes interesses e estratégias discursivas, essa prática passou a atingir ambientes públicos e privados, ultrapassando barreiras físicas e informacionais. O estudo analisa a espionagem como instrumento de influência política, favorecimento econômico e atuação estratégica em contextos de guerra cibernética

Palavras-chave: Espionagem; Privacidade; Criptografia; Paredes Digitais; Cibersegurança

INTRODUÇÃO

O antigo ditado popular "as paredes têm ouvidos" nunca foi tão literal quanto na era da hiperconectividade. A prática da espionagem, historicamente associada a conflitos geopolíticos e à inteligência estatal, evoluiu significativamente. O que antes dependia de dispositivos rudimentares de amplificação mecânica e de relatos obtidos por terceiros, transformou-se em um fenômeno muito mais sofisticado.

Ultrapassando o imaginário popular retratado em obras temáticas e filmes como 007, Missão Impossível, Ponte dos Espiões, etc. Essas narrativas fortaleceram o gênero policial e de ação ao abordar a espionagem sob uma perspectiva heroica, marcada por conflitos físicos e psicológicos em prol da proteção de terceiros.

Entretanto, as paredes não possuem apenas ouvidos; elas possuem sensores, conexões e memória. Na era da espionagem digital, cada pacote de dados pode representar uma informação sensível, e cada dispositivo conectado à internet torna-se um potencial informante. Se antes a espionagem estava restrita a cenários de guerra ou alta política, hoje ela se encontra silenciosamente no bolso de bilhões de pessoas, disfarçada em permissões de aplicativos, vulnerabilidades de sistemas operacionais, microfones de alta sensibilidade, sensores piezoelétricos, interferometria a laser e técnicas de recuperação de áudio por sinais de Wi-Fi e sensores inerciais de *smartphones*.

Nesse contexto, a privacidade em ambientes confinados enfrenta desafios sem precedentes. O monitoramento deixou de depender da proximidade física e passou a ocorrer remotamente, permitindo a transmissão em tempo real de conteúdos acessados, além da captura de imagens e vídeos por meio de câmeras e *webcams*. Entramos em uma realidade na qual algoritmos conseguem decifrar sussurros em meio ao ruído digital, enquanto a privacidade se torna uma valiosa moeda de troca, muitas vezes utilizada contra o próprio indivíduo.

Esse fenômeno levanta questões fundamentais sobre vulnerabilidade, ética e legalidade em um mundo hiperconectado. Os *smartphones* deixaram de ser apenas ferramentas de comunicação e passaram a atuar como sofisticados sensores de vigilância. Sob uma aparência inofensiva, tecnologias de monitoramento ultrapassam barreiras físicas, alcançando ambientes privados e círculos de influência.

Nesse contexto, torna-se cada vez mais necessário compreender as ameaças existentes, que podem variar desde *malwares* simples, capazes de invadir celulares e computadores, até ataques de grande escala destinados a sobrecarregar e travar servidores, além de *spywares* silenciosos voltados à coleta contínua de informações.

Dessa forma, este artigo explora como a nova era da espionagem digital transcende a simples coleta de dados, transformando microfones, câmeras e sensores em agentes invisíveis capazes de monitorar a vida privada em tempo real.

MATERIAL E MÉTODOS

Para a elaboração deste artigo, adotou-se o método de revisão bibliográfica, por meio da análise crítica de livros, artigos científicos, documentos técnicos e demais publicações relacionadas ao tema da espionagem digital.

A pesquisa foi conduzida utilizando palavras-chave específicas em bases acadêmicas, como o Google

Acadêmico, com o objetivo de identificar estudos relevantes que serviram de fundamentação teórica e estrutural para o desenvolvimento do trabalho.

Além das produções científicas, foram analisadas opiniões de especialistas, reportagens, jornais e revistas, visando ampliar a compreensão sobre os impactos e aplicações da espionagem digital na sociedade contemporânea. Os materiais selecionados contribuíram para a construção das seções do artigo e para a contextualização dos casos reais apresentados, proporcionando uma abordagem mais abrangente e fundamentada sobre a temática.

RESULTADOS E DISCUSSÃO

A história da espionagem

A prática da espionagem acompanha a história da humanidade desde a Antiguidade, estando diretamente relacionada à necessidade de sobrevivência, conquista territorial e manutenção do poder político e militar. Desde as primeiras civilizações organizadas, líderes e exércitos utilizavam mensageiros, observadores e informantes para obter informações estratégicas sobre adversários, rotas comerciais, recursos e possíveis ameaças.

Ao longo da história, diferentes povos aperfeiçoaram práticas de inteligência e contrainteligência. Civilizações como egípcios, gregos, romanos e chineses desenvolveram métodos de vigilância, infiltração e interceptação de informações para fortalecer seus impérios e antecipar ações inimigas. Um dos exemplos mais conhecidos encontra-se na obra A Arte da Guerra, na qual Sun Tzu (2006) destaca a espionagem como elemento essencial para o planejamento militar e para a obtenção de vantagens estratégicas em cenários de guerra.

Registros presentes no Velho Testamento, especialmente em Provérbios 24:3–7, datados de aproximadamente 1300 a.C., já ressaltaram a importância da estratégia, do conhecimento e da obtenção prévia de informações sobre o inimigo como fatores determinantes para o sucesso em conflitos e batalhas (BÍBLIA, 1993).

Nesse contexto, a espionagem consolidou-se como uma ferramenta estratégica voltada à coleta sigilosa de informações militares, políticas e territoriais, visando garantir vantagens táticas e fortalecer o poder das nações e exércitos. Com o passar dos séculos, essas práticas evoluíram juntamente com o avanço tecnológico, deixando de depender exclusivamente da ação humana e passando a incorporar sistemas eletrônicos, redes de comunicação e tecnologias digitais capazes de monitorar, processar e transmitir informações em escala global.

Até poucas décadas atrás, a espionagem era realizada principalmente por meios físicos e humanos, dependendo fortemente da atuação direta de agentes infiltrados, informantes e equipamentos analógicos. Os métodos mais comuns incluíam escutas telefônicas clandestinas (Figura 1), instalação de microfones ocultos em salas e objetos, fotografia secreta de documentos, interceptação de cartas e mensagens telegráficas, além do recrutamento de indivíduos que forneciam informações estratégicas em troca de dinheiro, proteção ou vantagens políticas.



Figura 1. Espionagem à moda antiga com gravadores.

Atualmente, a espionagem digital está presente de forma silenciosa nos dispositivos utilizados diariamente por bilhões de pessoas (Figura 2). *Smartphones* e aplicativos modernos utilizam permissões de sistema, sensores embarcados e coleta de dados para monitorar comportamentos, localização e interações dos usuários.



Figura 2. A espionagem através de *smartphones*.

Tecnologias como microfones de alta sensibilidade, sensores piezoelétricos, interferometria a laser e análise de sinais de Wi-Fi permitem captar vibrações, movimentos e até inferir sons sem a necessidade de gravação direta tradicional. Além disso, sensores inerciais de *smartphones*, como acelerômetros e giroscópios, podem ser explorados para identificar padrões de fala e movimentação.

Dessa forma, a vigilância contemporânea ocorre principalmente por meio da análise integrada de dados

digitais e algoritmos de inteligência artificial, tornando a ameaça à privacidade cada vez mais discreta e sofisticada.

Evolução do conceito de espionagem

Na contemporaneidade, a atividade da espionagem evoluiu para estruturas mais complexas. Sob a ótica de Andrew (2009), a espionagem define-se como a obtenção clandestina de informações relativas aos interesses de um Estado ou entidade, utilizando fontes humanas ou técnicas para salvaguardar a segurança nacional.

Entretanto, o cenário do século XXI impõe novos desafios. Johnson (2018) expande esse conceito ao incluir a "guerra da informação", onde a espionagem transcende a mera coleta de dados para abranger operações psicológicas e de desinformação. Nesse contexto, as redes sociais tornaram-se o universo privilegiado para esse fluxo de informações.

Embora vistas apenas como espaços de interação cotidiana, plataformas como Facebook, Instagram e TikTok consolidaram-se como ferramentas estratégicas de inteligência e contra inteligência. Como reforça Zuboff (2019), a "economia da vigilância" tornou-se um pilar do capitalismo digital, onde a coleta massiva de dados, muitas vezes cedidos voluntariamente pelos usuários em atos de inscrição "*Sine qua non*" (sem a qual não), permite prever e influenciar comportamentos de massa.

Essa realidade transforma dados triviais, como curtidas e localização, em ativos estratégicos. Andrejevic (2020) aponta que a mineração desses dados, otimizada por Inteligência Artificial (IA), é hoje decisiva para campanhas eleitorais e segurança nacional, dos quais fornece dados cruciais para as táticas e terrenos para serem usadas em momentos mais oportunos.

O caso da Cambridge Analytica, que foi uma consultoria política britânica que obteve indevidamente dados de cerca de 87 milhões de usuários do Facebook para criar perfis psicológicos e influenciar comportamentos eleitorais, notadamente na campanha de Donald Trump em 2016 e no referendo do Brexit, foi discutido por Cadwalladr (2019). É o exemplo mais emblemático de como o direcionamento seletivo de conteúdo pode minar processos democráticos.

Paralelamente, o TikTok emerge como uma nova fronteira geopolítica. Diferente do modelo de conexões do Facebook, seu algoritmo responsivo de vídeos curtos facilita a disseminação de narrativas virais. Segundo Mozur (2021), a possibilidade de coleta massiva de dados por essa plataforma é vista como uma ameaça à soberania digital de diversas nações, especialmente diante da influência chinesa.

Face à tamanha exposição, a contrainteligência assume um papel vital. Na perspectiva de Olson (2006), ela refere-se às estratégias para mitigar a espionagem e a subversão estrangeira. No ambiente digital, isso envolve desde regulamentações rígidas até a criação de "realidades paralelas" e perfis falsos para desviar o monitoramento adversário, técnica que Rid (2020) descreve como a manipulação ativa para favorecer determinados grupos.

Por fim, essa dinâmica não se restringe aos Estados; indivíduos e grupos ativistas também operam nesse campo fértil de monitoramento e defesa. Como enfatiza Wardle (2020), a propagação de conteúdos fabricados (*fake news*) via IA tem o poder de gerar instabilidade social e alterar percepções públicas, consolidando as redes sociais como as novas arenas da disputa pelo poder global.

Espionagem cibernética - casos reais

Guerra Fria

Um dos maiores passos para evolução da espionagem digital deriva de "A Coisa", um episódio muito célebre da guerra fria. Tratava-se de um dispositivo de escuta passivo escondido dentro de uma réplica de madeira do Grande Selo dos Estados Unidos, presenteado à embaixada americana em Moscou. O objeto foi pendurado na parede do escritório do embaixador, na Casa Spaso, onde permaneceu por sete anos.

Criado pelo inventor russo Léon Theremin, o dispositivo não utilizava pilhas ou fios (passivo), o que o tornava indetectável pelos métodos de varredura convencionais da época. Ele funcionava apenas quando ativado por ondas de rádio enviadas de fora do edifício, transmitindo o áudio das conversas.

Caso Snowden

Em 2013, Edward Snowden, ex-analista da NSA, revelou ao mundo a existência de programas de vigilância em massa operados pelo governo dos EUA, como o PRISM. Os documentos vazados demonstraram a interceptação sistemática de dados de milhões de cidadãos e líderes globais, provocando um debate internacional sem precedentes sobre a soberania digital, os limites da espionagem estatal e o direito fundamental à privacidade na era da internet (Quicassa, 2026). Atualmente, Snowden vive na Rússia, onde recebeu cidadania, enquanto permanece acusado de espionagem em solo americano.

Ciberguerra na Ucrânia

No contexto da ciberguerra entre Ucrânia e Rússia, relatórios da Kaspersky indicam que, em março de 2022, a Ucrânia foi alvo de uma ofensiva cibernética híbrida caracterizada por escaneamento de vulnerabilidades, exploração de falhas em servidores

Exchange, com destaque para a vulnerabilidade CVE-2021-26855, responsável por aproximadamente 12% das ocorrências, e ataques de força bruta via protocolo RDP, que corresponderam a cerca de 32% das tentativas de intrusão. Os registros apontaram picos significativos de atividade nos dias 5 e 23 de março, coincidindo com os períodos de intensificação do conflito militar no território ucraniano (Toio, 2024).

O cenário também evidenciou baixa incidência de *ransomware*, concentrando-se principalmente em mineradores de criptomoedas, especialmente o *malware* Trojan.BAT.Miner.gen, responsável por aproximadamente 39,13% das detecções, além de campanhas de espionagem conduzidas por meio de e-mails maliciosos, cujas atividades oscilaram ao longo do mês. De acordo com Davies (2022), ao direcionar ataques contra autoridades polonesas e ucranianas, a Rússia buscava não apenas informações militares estratégicas, mas também compreender a logística de apoio da Organização do Tratado do Atlântico Norte (OTAN). O conhecimento antecipado sobre possíveis sanções econômicas permitiria ao Kremlin adotar medidas preventivas para mitigar impactos sobre sua economia antes dos anúncios oficiais.

Nesse contexto, os picos de ataques registrados nos dias 5 e 23 de março coincidiram com momentos de impasse diplomático e avanços militares no terreno, demonstrando que o ambiente digital foi utilizado como instrumento de pressão estratégica sobre o governo ucraniano.

Conforme relatado por Hodge (2022), o Ministério da Defesa da Rússia declarou ter realizado ataques com mísseis de cruzeiro durante a noite contra alvos na Ucrânia, alegando que os objetivos estavam restritos à infraestrutura militar. Esse episódio evidencia a relevância estratégica da obtenção prévia de informações em cenários de guerra contemporânea, nos quais a inteligência cibernética exerce papel fundamental na definição de alvos e na condução de operações militares.

Operação Salt Typhoon

As IAs representam atualmente a mais recente evolução da era digital, sendo responsáveis por consolidar e renovar o conceito de espionagem em um nível jamais visto até então. Um exemplo disso foi a recente Operação Salt Typhoon, em setembro de 2025, quando agências de inteligência de mais de dez países, incluindo o FBI e a CIA dos Estados Unidos, emitiram um alerta conjunto sobre uma das maiores campanhas de ciberespionagem já registradas (FBI, 2025).

A operação, vinculada ao grupo Salt Typhoon (também conhecido como Ghost Emperor ou Operador Panda), teve como alvo a invasão de infraestruturas críticas, como redes de telecomunicações e provedores de internet. Diferentemente de ataques comuns, os *hackers* modificaram roteadores de grande porte para manter acesso persistente e silencioso aos sistemas, permitindo o monitoramento de comunicações por longos períodos sem serem detectados (FBI, 2025).

Caso Brasil

O caso envolvendo a ferramenta i-Find e a invasão ao sistema Córtex, em 2025, evidenciou a crescente sofisticação das práticas de espionagem cibernética (Figura 3) no contexto brasileiro. Segundo as investigações, integrantes do Primeiro Comando da Capital (PCC) utilizaram a ferramenta denominada i-Find para acessar de forma ilícita o Córtex, sistema de inteligência baseado em técnicas de inteligência artificial destinado ao cruzamento de dados públicos e privados em tempo real (Gazeta do Povo, 2025). O episódio revelou vulnerabilidades críticas em uma das principais plataformas de vigilância e inteligência do governo federal brasileiro (Barboza, 2025).



Figura 3. Convergência entre espionagem de Estado e cibercrime.

Por meio desse acesso indevido, os criminosos obtiveram informações sensíveis e realizaram o monitoramento de autoridades públicas, incluindo o senador Sérgio Moro, o promotor Lincoln Gakiya e ministros do Supremo Tribunal Federal (STF). O caso demonstra a dualidade inerente às tecnologias de inteligência e vigilância, uma vez que ferramentas desenvolvidas para fins de segurança nacional, como o Córtex, podem ser convertidas em instrumentos de atuação criminosa quando mecanismos de proteção e controle de acesso são comprometidos (Valente; Freitas, 2025).

Ciberespionagem por IA autônoma

Ainda em 2025, observou-se a consolidação de um novo paradigma no contexto da cibersegurança com a atuação do grupo GTG-1002. Essa operação é descrita como o primeiro caso documentado de ataque cibernético em larga escala conduzido predominantemente por agentes autônomos de inteligência artificial, capazes de coordenar invasões contra 30 organizações globais com mínima intervenção humana.

Tais acontecimentos corroboram as previsões apresentadas por Mozur (2021) e Rid (2020), segundo

as quais o ciberespaço ultrapassa a condição de simples meio de comunicação, configurando-se como um ambiente estratégico de disputa geopolítica, no qual a coleta de dados e a manipulação de infraestruturas críticas exercem influência direta sobre a soberania nacional.

Nesse contexto, países como a República Tcheca, por intermédio da NÚKIB, emitiram, em setembro de 2025, alertas específicos acerca dos riscos associados à transferência de dados para entidades sob influência chinesa.

Ouvidos nas paredes digitais

Após as revelações de Edward Snowden, em 2013, a expressão “as paredes possuem ouvidos” tornou-se mais literal do que nunca. Desde então, o cenário da espionagem digital evoluiu de programas de coleta massiva de dados para ferramentas de invasão cirúrgica e praticamente invisível, frequentemente comercializadas como serviços especializados destinados a governos, como, por exemplo:

Spywares

Diferentes dos vírus comuns, essas ferramentas (*Spywares*) são "*zero-click*" (não exigem que você clique em nada para infectar o aparelho).

O Pegasus, desenvolvido pela NSO Group, destaca-se como uma das mais sofisticadas ferramentas de espionagem digital atualmente conhecidas no cenário internacional (Corera, 2021). Após a infecção do dispositivo-alvo, o software torna-se capaz de acessar integralmente recursos do aparelho, incluindo microfone, câmera, dados de geolocalização em tempo real e comunicações criptografadas realizadas por aplicativos como WhatsApp e Signal. Em razão de sua elevada capacidade de infiltração e monitoramento, o Pegasus tem sido amplamente associado a operações de vigilância conduzidas por governos e agências de inteligência em diferentes países.

O XKeyscore (XKS) consiste em um programa de vigilância secreta desenvolvido pela National Security Agency (NSA), cuja existência foi revelada por Edward Snowden em 2013. O sistema é considerado uma das mais abrangentes ferramentas de inteligência da agência, sendo capaz de coletar, armazenar e analisar, em tempo real, grandes volumes de dados provenientes da internet em escala global. Entre as informações monitoradas incluem-se e-mails, histórico de navegação, pesquisas realizadas em mecanismos de busca e atividades em redes sociais, frequentemente sem a necessidade de autorização judicial individualizada (Marquis-Boire *et al*., 2015).

Na Figura 4, observa-se o esquema operacional do programa, no qual um centro de comando principal recebe dados coletados por diferentes pontos de monitoramento distribuídos globalmente. Posteriormente, essas informações são processadas, criptografadas e encaminhadas para uma ampla infraestrutura composta por centenas de servidores distribuídos em diversas regiões do mundo, possibilitando o armazenamento e a análise massiva de dados digitais.

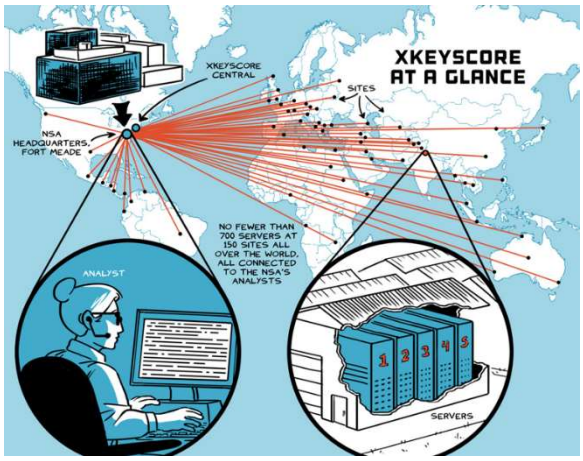


Figura 4. Esquema operacional do programa XKeyscore.

Tempora

Outro programa revelado por Edward Snowden foi o Tempora, sistema de vigilância operado pela agência de inteligência britânica Government Communications Headquarters (GCHQ). Diferentemente de programas que dependem da cooperação de empresas provedoras de serviços digitais, o Tempora atua diretamente sobre a infraestrutura física da internet, interceptando cabos submarinos de fibra óptica responsáveis pelo tráfego global de comunicações (Muller, 2013).

O sistema possui capacidade para coletar e armazenar grandes volumes de dados provenientes de usuários da internet, incluindo pesquisas realizadas em mecanismos de busca, históricos de navegação, conversas, áudios, imagens e demais conteúdos digitais (MacAskill *et al*., 2013). Em razão de sua abrangência operacional e do elevado volume de dados monitorados, o Tempora é frequentemente apontado como um dos mais extensos sistemas de vigilância cibernética já desenvolvidos, superando, em determinados aspectos de coleta de dados, até mesmo o PRISM, operado pela National Security Agency (NSA).

Google

Em 2018, na Northeastern University, uma pesquisa que buscava responder a uma pergunta que intrigava muitas pessoas levantou outra dúvida: o Google nos escuta? Por que anúncios tão específicos aparecem com base em assuntos sobre os quais conversamos?

Não foram encontradas evidências de que o aplicativo grave conversas secretamente para direcionar anúncios (Ferreira, 2025). Embora possua recursos de captação de voz, o sistema necessita do comando "Ok Google" para ser ativado, conforme descrito nas diretrizes do aplicativo e na legislação americana.

Entretanto, a pesquisa demonstrou que, em vez de escutar conversas, o Google utiliza métodos mais convencionais para prever os interesses dos usuários, como rastreamento de localização (GPS), histórico de pesquisas, *cookies* e comportamento online.

CONCLUSÃO

O conceito de espionagem remonta à Antiguidade, sendo utilizado como instrumento estratégico para conquista, sobrevivência e obtenção de vantagens militares e políticas. Ao longo da história, as técnicas de coleta de informações influenciaram não apenas operações reais de inteligência, mas também a ficção, contribuindo para a construção de uma imagem romantizada dos espiões e ocultando, muitas vezes, os impactos causados pelo vazamento e uso indevido de informações.

Com o avanço tecnológico, a espionagem deixou de depender exclusivamente da atuação humana e passou a incorporar sistemas automatizados capazes de processar grandes volumes de dados em tempo real. Essa transformação alterou não apenas a escala das operações de vigilância, mas também a própria concepção de soberania, segurança e privacidade, especialmente em uma sociedade marcada pela intensa exposição de informações em ambientes digitais e redes sociais.

Casos recentes, como campanhas globais de espionagem cibernética e o comprometimento de sistemas estratégicos, demonstram que as ferramentas de inteligência representam instrumentos de duplo uso: essenciais para a segurança nacional e para a proteção de infraestruturas críticas, mas também potencialmente perigosas quando exploradas por agentes mal-intencionados ou associadas a falhas de segurança.

Nesse cenário, os desafios do século XXI ultrapassam a simples obtenção de informações, abrangendo também a proteção da integridade dos sistemas digitais, a segurança dos dados e a responsabilidade ética no uso das tecnologias de vigilância.

Dessa forma, o futuro da segurança global e da própria democracia dependerá da capacidade dos Estados, organizações e indivíduos em equilibrar o avanço tecnológico com regulamentações eficazes, práticas robustas de cibersegurança e estratégias de contrainteligência que priorizem a proteção da privacidade e dos direitos fundamentais na nova realidade do ciberespaço.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Universidade Federal de Mato Grosso do Sul – UFMS/MEC – Brasil.

REFERÊNCIAS

ANDREJEVIC, Mark. Automated Media. 1. ed. New York: Routledge, 2020.

ANDREW, Christopher. The Defence of the Realm: The Authorized History of MI5. London: Allen Lane, 2009.

BARBOZA, Sandro. PF investiga uso de sistema do Ministério da Justiça por membros do PCC. Jornal da Band, 20 set. 2025. Disponível em: https://www.band.com.br/noticias/jornal-da-band/ultimas/pf-investiga-uso-de-sistema-do-ministerio-da-justica-por-membros-do-pcc-202509202001. Acesso em: 11/05/2026.

BÍBLIA. Português. Bíblia Sagrada. Tradução de João Ferreira de Almeida. Edição Revista e Atualizada. Barueri: Sociedade Bíblica do Brasil, 1993.

CADWALLADR, Carole. Great Hack: the Cambridge Analytica scandal. The Guardian, 2019. Disponível em: theguardian.com. Acesso em: 24 maio 2024.

CORERA, Gordon. Escândalo Pegasus: estamos todos virando espiões sem saber?. BBC News Brasil, 2021. Disponível em: https://www.bbc.com/portuguese/geral-57924575. Acesso em: 06/05/2026.

DAVIES, Pascale. Cyberespionage is key to Russia's invasion of Ukraine. The international community is fighting back. Euronews, 2022.

FERREIRA, Jacqueline. Não, seu celular não ouve você! Entenda o que realmente acontece. Site Eficaz Marketing e Tecnologia, 2025. Disponível em: https://eficazmarketing.com/blog/celular-escuta-o-que-voce-fala/. Acesso em: 06/05/2026.

FBI. *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System*. Federal Bureau of Investigation (FBI), Washington, DC: FBI, 2025. Disponível em: www.fbi.gov/file-repository/cyber-alerts/countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system-082725.pdf/view. Acesso em: 10/05/2026.

GAZETA DO POVO. PF expõe nova invasão ao Córtex: IA espiã e o monitoramento de autoridades. Brasília, ago. 2025.

HODGE, Nathan. Rússia diz que lançou mísseis durante a noite, mas não atingiu moradores de Kiev. CNN Brasil, Internacional, 2022. Disponível

em: https://www.cnnbrasil.com.br/internacional/russia-diz-que-lancou-misseis-durante-a-noite-mas-nao-atingiu-moradores-de-kiev/. Acesso em: 08/05/2026.

JOHNSON, Loch K. Spy Watching: Intelligence Accountability in the United States. Oxford: Oxford University Press, 2018.

MACASKILL, Ewen; BORGER, Julian; HOPKINS, Nick; DAVIES, Nick; BALL, James. GCHQ taps fibre-optic cables for secret access to world's communications. The Guardian, Londres, 21 jun. 2013. Disponível em: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. Acesso em: 13/05/2026.

MARQUIS-BOIRE, Morgan; GREENWALD, Glenn; LEE, Micah. NSAs Google worlds private communications. The Intercept, 2015. Disponível em: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/. Acesso em: 12/05/2026.

MOZUR, Paul. TikTok and the New Geopolitics of Information. The New York Times, 2021. Disponível em: nytimes.com. Acesso em: 24 maio 2024.

MULLER, Leonardo. Tempora: programa de espionagem global britânico é mais eficiente que PRISM. Tecmundo, Segurança, 2013. Disponível em: https://www.tecmundo.com.br/seguranca/41151-tempora-programa-de-espionagem-global-britanico-e-mais-eficiente-que-prism.htm. Acesso em: 06/05/2026.

OLSON, James M. Fair Play: The Moral Dilemmas of Spying. Washington: Potomac Books, 2006.

QUICASSA, Juvenal. As Redes Sociais Contemporâneas Como Ferramentas Para Operações De Inteligência E Contrainteligência: Impactos Na Diplomacia. Revista Atenas Humanitas, vol. 2, n. 1, 2026. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=xERuDA-Ra8wC&oi=fnd&pg=PA5&dq=espionagem+digital&ots=--cYF_Rb3t&sig=YoIgSYGJoQ-CONlCTHBx4IHohlo#v=onepage&q=espionagem%20digital&f=false. Acesso em: 04/05/2026.

RID, Thomas. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020.

SUN TZU. A arte da guerra. Tradução de Pietro Nassetti. São Paulo: Martin Claret, 2006.

TOIO, Stefan da Silva. Sociedade algoritificada: uma análise sobre a espionagem na ciberguerra entre a Rússia e Ucrânia. Revista Multidisciplinar de Ciências Gerais in Focus, v.1, n.1, p.188-206, 2024. Disponível em: https://periodicos.faculdadefocus.com.br/revista-multidisciplinar-focus/article/view/24/23. Acesso em: 06/05/2026.

VALENTE, Rubens; FREITAS, Caio de. Ata revela 'consultas irregulares' em sistemas de vigilância do Ministério da Justiça. Pública, Agência de jornalismo investigativo, 2025. Disponível em: https://apublica.org/2025/01/ata-revela-consultas-irregulare. Acesso em: 13/05/2026.

WARDLE, Claire. Information Disorder: Toward an interdisciplinary framework for research and policymaking. Harvard Kennedy School, 2020.

ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2019.