



Revista Jurídica



Tatuapé

A ESPIONAGEM INTERNACIONAL NO BRASIL: A TUTELA LEGAL DA SEGURANÇA NACIONAL

INTERNATIONAL ESPIONAGE IN BRAZIL: THE LEGAL PROTECTION OF NATIONAL SECURITY

Mariana Peccicacco

Graduada em Comunicação Social com habilitação em Jornalismo pela Universidade Anhembi Morumbi. Pós-graduada em Administração de Empresas pelo Centro Universitário das Faculdades Metropolitanas Unidas- FMU/SP. Graduada em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas- FMU/SP. Curriculum Lattes: <http://lattes.cnpq.br/9554792785874110>.
E-mail: marianapecicacco@gmail.com

Ronny Max Machado

Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas. São Paulo. Estado de São Paulo. Brasil. Pesquisador junto ao Programa de Mestrado em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas, São Paulo. Estado de São Paulo. Brasil. Lattes: <http://lattes.cnpq.br/3526842654606450>;
E-mail: ronnymaxm@yahoo.com.br

Osmar Fernando Gonçalves Barreto

Doutorando em Função Social do Direito pela Faculdade Autônoma de Direito de São Paulo - FADISP (2020 - até o momento). Mestre em Direito da Sociedade da Informação pelo Centro Universitário das Faculdades Metropolitanas Unidas - FMU (2017). Pós-graduado lato sensu em Direito e Processo do Trabalho pelo Damásio Educacional (2020). Pós-graduado lato sensu em Direito Privado pela Escola Paulista da Magistratura - EPM (2008). Graduado em Direito pelo Centro Universitário das Faculdades Metropolitanas Unidas - FMU (2006). Lattes: <http://lattes.cnpq.br/1063688454568879>;
E-mail: osmarbarreto2@hotmail.com

Resumo: A Sociedade da Informação, enquanto fenômeno, possui inúmeros contextos, talvez o mais relevante seja aquele que possui o elemento informação como sendo a base de tal Sociedade, uma vez que ele serve para a consecução de quase todas as atividades humanas. Assim, um dos pontos importantes sobre a informação, que chama atenção pelos problemas que provoca e pelas dificuldades presentes na sua prática e no seu combate é: a espionagem. Deste modo, o presente artigo, por meio da metodologia da revisão bibliográfica e normativa, inclusive da análise de Tratados Internacionais sobre o tema, se propõe a abordar o fenômeno da espionagem no Brasil e, os mecanismos de segurança nacional em defesa da informação e da sociedade brasileira, e apontar se realmente são efetivos.

Palavras-Chave: Segurança Nacional; Espionagem; Agência; Informação.

Abstract: *The Information Society, as a phenomenon, has numerous contexts, perhaps the most relevant of which is the one in which the element of information is the basis of the society, since it is used to carry out almost all human activities. Thus, one of the important points about information, which draws attention due to the problems it causes and the difficulties present in practicing and combating it, is espionage. In this way, this article, using the methodology of a bibliographical and normative review, including an analysis of international treaties on the subject, sets out to address the phenomenon of*

espionage in Brazil and the mechanisms of national security in defense of information and Brazilian society, and whether they are really effective.

Keywords: National Security; Espionage; Agency; Information.

INTRODUÇÃO

A obtenção de informações preciosas e sigilosas por agentes de Estado infiltrados em outras nações de maneira sorrateira ou não é uma conduta que mexe com o senso de proteção e justiça, uma vez que tais condutas provocam lesões irreparáveis ou de difícil reparação no plano do Direito interno e Internacional. No jogo de interesses, a espionagem internacional provoca uma série de impactos prejudiciais, - como econômicos e culturais -, nas relações internacionais, empresariais ou corporativos, entre outros. Os países afetados, pela atividade de espionagem, possuem uma atividade de inteligência constante em prol da segurança da informação e da sociedade que compõem o país atacado.

Visto que a espionagem é também uma forma de defesa, chega a ser imprescindível que os países possuam suas próprias agências de espionagem, com o objetivo de coletar informações estratégicas, políticas e econômicas de outros países. Ademais a proteção informacional, e por que não dizer os projetos de cibersegurança são cada vez mais aprimorados dadas as dificuldades provocadas por *crackers*, criminosos que se infiltram nos sistemas de maior importância econômica do país.

Assim, o presente estudo revela suas relevâncias (social, jurídica e acadêmica) sobre o tema, e se lastreará em revisão bibliográfica e, na análise de Tratados Internacionais sobre o assunto, para aferir o estado da arte sobre a espionagem internacional no Brasil. Deste modo, o presente artigo se propõe a abordar o fenômeno da espionagem no Brasil e os mecanismos de segurança nacional em defesa da informação e da sociedade brasileira.

1 A ESPIONAGEM INTERNACIONAL NO BRASIL: HISTÓRICO DE CASOS

Os aspectos históricos, em qualquer estudo, têm uma importância fundamental, uma vez que constituem o alicerce para o desenvolvimento da pesquisa e do discurso que

se pretende construir. Feita esta consideração, é importante destacar que a espionagem¹ entre países acontece desde que os humanos começaram a guerrear (MARTINS, p.13, 2014) e chegam a ser uma parte importante e relevante da guerra, visto que, busca responder perguntas: como o que os inimigos estão pretendendo fazer? ou quais suas habilidades e que perigo podem causar?.

No mundo moderno, outros passaram a ser os motivos para a espionagem, como, por exemplo, para tomadas de decisões governamentais mais assertivas, melhorar e apoiar o planejamento de capacidade defensiva e bélica do país, ajudar na tomada de decisões diplomáticas, monitorar possíveis alvos, além de, é claro, descobrir segredos informacionais (MARTINS, 2014, p.16). Segundo Gonçalves a expressão espionagem passa por uma alteração terminológica contextual, a ponto de ser considerada como um serviço de inteligência de natureza essencial para atividades bélicas ou até mesmo empresariais. Contudo, segundo o autor, com algumas peculiaridades:

Outrora chamada simplesmente de “espionagem”, esse ofício é atualmente conhecido como “atividade de inteligência”, e tem em seu cerne a obtenção de dados negados para a produção de um conhecimento que assessor o processo decisório nos mais diferentes níveis, de um oficial no campo de batalha ao chefe da nação mais poderosa, passando pelo empresário que precisa conhecer o cliente e a concorrência e pelo planejador de políticas públicas. (GONÇALVES, J.B., 2008, p. 3).

Um ponto importante, no campo dos fatos históricos, foi a criação de uma comissão internacional composta por juristas, que reuniu-se no ano de 1967 em Estocolmo na Suécia, com a finalidade de discutir o tema privacidade. Neste mesmo cenário, a Conferência Nórdica sobre o Direito à Intimidade chegou à conclusão que o direito à intimidade se refere a um direito inerente ao homem, consistente em viver de modo independente a sua vida. Ademais, elencou-se as hipóteses em que poderia ocorrer ofensas ao direito à intimidade que são as seguintes:

- (a) penetração no retraimento da solidão da pessoa, incluindo-se espreitá-la pelo seguimento, **pela espionagem** ou pelo chamamento constante ao telefone;
- (b) gravação de conversas e tomadas de cenas fotográficas e cinematográficas das pessoas em seu círculo privado ou em circunstâncias íntimas ou penosas a sua moral;**
- (c) audição de conversações privadas por interferências mecânicas em**

¹ “É a ação que visa à obtenção de conhecimento ou dados sensíveis para beneficiar Estados, grupos de países, organização, facções, grupos de interesse, empresas ou indivíduos. As ações de espionagem podem afetar o desenvolvimento socioeconômico e comprometer a soberania nacional. Há instituições e empresas brasileiras vulneráveis à espionagem, notadamente aquelas que atuam nas áreas econômico-financeira e científico-tecnológica”. (BRASIL, 2016, item 6.1).

telefone e em microfilmes dissimulados deliberadamente;

(d) exploração de nome, de identidade ou de semelhanças de uma pessoa sem o seu consentimento;

(e) utilização de falsas declarações, revelação de fatos íntimos, e crítica da vida das pessoas (GUERRA, 2004, p.73). **(grifo nosso)**

As disposições grifadas, claramente, fazem remissão direta a atividade de espionagem que tem nestes mecanismos, fontes diretas de obtenção de informações sigilosas de impacto nacional. A privacidade do Estado e das empresas, corporações, multinacionais, etc, tornam evidente que as práticas criminosas de espionagem visam a obtenção de informações capazes com afetar muitos componentes estruturantes de uma sociedade e precisam ser protegidas com maior rigor e por meio de mecanismo eficazes.

Outro fato histórico é a previsão legal no Código Penal Alemão, datado de 10 de janeiro de 1987, tipificando como crime a violação da confidencialidade (CVM-COMISSÃO DE VALORES MOBILIÁRIOS, 2016) da palavra, de violação de correspondência, de espionagem de dados, de violação de privacidade e de utilização de segredo alheio. A confidencialidade consiste na propriedade sobre a informação sob a qual incide a indisponibilidade ou vedação no tocante a divulgação em prol de pessoas naturais ou jurídicas sem a respectiva autorização do seu respectivo titular. Trata-se de uma garantia de tornar reservada as informações obtidas no plano pessoal sob a égide de uma relação de confiança e tutela em face da propagação sem permissão (CVM – COMISSÃO DE VALORES MOBILIÁRIOS, 2016).

Hoje algumas agências são bem conhecidas mundialmente e podemos citar como uma das principais a Agência Central de Inteligência (*Central Intelligence Agency - CIA*), dos Estados Unidos da América (EUA), que é responsável por coletar informações estratégicas para o governo dos Estados Unidos e para seus aliados, além de ser responsável por realizar operações de inteligência em todo o mundo (DABALT, 2023).

Outra agência bem conhecida nos EUA é a Agência de Segurança Nacional (*National Security Agency - NSA*), responsável por coletar informações de inteligência eletrônica e cibernética para o governo dos Estados Unidos. A agência é conhecida por ter a capacidade de interceptar e decodificar comunicações de todo o mundo (KLEINA, 2021).

Na Europa podemos citar a MI6 (*Military Intelligence Service*), do Reino Unido. Também conhecida como Serviço Secreto de Inteligência, é responsável pela coleta de informações de inteligência e por conduzir operações secretas em todo o mundo (PAOLOZZI, 2006).

Já a FSB (*Federal'naya Sluzhba Bezopasnosti Rossiyskoy Federatsii*), Serviço Federal de Segurança da Federação Russa, é a principal agência de inteligência da Rússia, responsável pela coleta de informações estratégicas e pela proteção do país contra ameaças internas e externas. A agência é conhecida por sua habilidade em espionagem e contra-espionagem (PETER, 2018). Na França podemos citar a Direção-Geral de Segurança Externa (*DGSE - Direction Générale de la Sécurité Extérieure*), responsável pela coleta de informações de inteligência e por operações secretas em todo o mundo. A DGSE é conhecida por suas operações bem-sucedidas e por sua expertise em contraterrorismo (*DGSE - Direction Générale de la Sécurité Extérieure*, 2023).

Na Alemanha, o Serviço Federal de Inteligência (*BND - Bundesnachrichtendienst. The Foreign Intelligence Service of Germany*) é responsável pela coleta de informações de inteligência e por conduzir operações secretas em todo o mundo. A *BND* é conhecida por sua habilidade em coletar informações sobre ameaças terroristas (*BND - Bundesnachrichtendienst. The Foreign Intelligence Service of Germany*, 2023).

No cenário brasileiro, não é diferente, pois, os mecanismos de proteção existem, bem como o sofrimento ou impacto decorrente da atividade de espionagem se fez presente em inúmeros momentos de nossa história. E em sendo o Brasil um país de grande relevância no cenário mundial, é natural que outros Estados queiram acompanhar de perto e secretamente o que acontece por aqui.

A princípio, a espionagem é um conjunto de ações organizadas e coordenadas para investigar, com escopo de obter informações de caráter secreto ou confidencial sobre países, governos, instituições ou organizações, mesmo privadas, sem suas autorizações, com a finalidade de, com tais informações, obter 'vantagem', vantagem estratégica, vantagem militar, econômica, política, mercadológica, em tecnologia, know-how, ou qualquer outra. Vantagem que não se obteria sem essas informações, nem mesmo informações que seriam fornecidas de bom grado e sem resistência. Daí os Espiões usarem de todos os estratagemas e subterfúgios para a obtenção ardilosa, de meios mais ocultos e nada legais (DIOGO, 2013, p.10).

Dito isso, o Brasil tem sido alvo de espionagem internacional há muitos anos e alguns casos, que acabaram descobertos pela Agência Brasileira de Inteligência (ABIN)², se tornaram conhecidos do grande público. Um destes casos é o da espionagem dos

² O Sistema Brasileiro de Inteligência (2004) considera inteligência: “(...) como o exercício permanente de ações especializadas orientadas para obtenção de dados, produção e difusão de conhecimentos, com vistas ao assessoramento de autoridades governamentais, nos respectivos níveis e áreas de atribuição, para o planejamento, a execução e o acompanhamento das políticas de Estado, englobando também a salvaguarda de dados, conhecimentos, áreas, pessoas e meios de interesse da sociedade e do Estado”. (SBI, 2004).

Estados Unidos em 2013, revelada pelo o ex-analista da Agência de Segurança Nacional (NSA – *National Security Agency*) dos Estados Unidos, Edward Snowden. O americano teve acesso às informações que divulgou quando ainda prestava serviços par a NSA no Havaí. Em maio de 2014 resolveu compartilhar os dados obtidos com o jornalista britânico Glenn Greenwald, do jornal britânico The Guardian, como uma forma de impedir que os EUA destruíssem “a privacidade, a liberdade de Internet e os direitos básicos de pessoas em todo o mundo, tudo em nome de um maciço serviço secreto de vigilância que eles estão desenvolvendo” (G1, 2013).

Segundo ele, Nos EUA, a Agência³ coletava informações de cidadãos americanos através da companhia telefônica Verizon. Dentre estes dados estavam data, horário e local de ligações dos EUA para o exterior, bem como dados de e-mail, bate-papo, fotos, vídeos, senhas e dados de usuários de empresas como Apple, AOL, Facebook, Google, Microsoft, Skype, Yahoo e Youtube. (BERDU, 2016, p. 5). Por aqui, segundo Snowden, a NSA teve acesso a dados da então presidente Dilma Rousseff, empresas de setores estratégicos como a Petrobras, e a áreas do governo, como o Ministério de Minas e Energia do Brasil. Durante o mês de janeiro de 2013 teriam sido acessados mais de 2 bilhões de telefonemas e trocas de mensagens, fazendo do país um dos alvos principais da NSA, ao lado de países como China, Irã, Rússia e Paquistão (BERDU, 2016, p. 6).

Os EUA chegaram a instalar por aqui uma das suas 16 bases de espionagem internacional, em 2002, que tinha como alvo principal a embaixada do Brasil em Washington e a missão do país na Organização das Nações Unidas (SENADO FEDERAL, 2014). A divulgação do caso pelo americano teve grande repercussão mundial, obrigando-o a pedir asilo na Rússia, ainda em 2013. Em 2022 o presidente Vladimir Putin concedeu cidadania ao americano, que certamente será julgado criminalmente caso retorne para sua terra natal.

Mas não foi só este caso que ficou conhecido. O Brasil esteve na mira dos Estados Unidos em diversas outras operações. A Comissão Parlamentar de Inquérito (CPI) da

³ [...] temos como principais agências secretas: a Central Intelligence Agency (CIA), criada no dia 18 de setembro de 1947; o Komitet Gosudarstvennoy Bezopasnost (KGB) que em 1991 se dividia em duas organizações distintas, o Federal'naya Sluzhba Bezopasnnosti Rossiyskoy Federatssi (Serviço de Segurança Federal da Federação Russa) ou FSB, e o Sluzhba Vneshney Razvedki (Serviço de Inteligência Externa da Federação Russa) ou SVR. O FSB herdou do KGB as funções de contrainteligência, segurança interna e segurança fronteiriça. Boris Ieltsin realizou transformações na estrutura cria a Federalnaya Sluzhba Kontrnazvedki (serviço de contrainteligência Federal) ou FSK que teria como missão proteger a nova federação Russa das ameaças dos serviços secretos dos restantes países. (DIOGO, 2013, p.98).

Espionagem⁴, que analisou o caso revelado por Snowden, em 2014, se referiu ao esquema de vigilância cibernética da NSA em duas categorias, a depender do método de coleta de informações: (a) acesso direto às informações fornecidas por um certo número de grandes empresas; e (b) programas de interceptação de grandes fluxos de comunicação, por meio da captura de dados nas infraestruturas por onde trafegam ou estão armazenadas.⁵ Nesta segunda categoria, o relatório apresenta o nome de ao menos outras quatro operações em que os EUA espionaram o Brasil, tais como Blarney, Fairview, Oakstar e Stormbrew.

Por parte do Canadá, também em 2013, o país foi espionado no programa Olympia, que acessou as comunicações de computadores, telefones fixos e celulares do Ministério de Minas e Energia. O nome da operação é o nome do programa usado pelos canadenses para identificar os números de telefone, registros de chips e modelos dos aparelhos. Segundo reportagem do Fantástico, as informações foram compartilhadas com mais cinco países um ano antes: Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia (JORNAL NACIONAL, 2013). Após a descoberta, o Brasil convocou o embaixador canadense em Brasília para dar explicações sobre a espionagem. Com grande relevância no cenário internacional, certamente o país continuará sendo alvo de espionagem internacional, devendo aprimorar a contraespionagem para evitar o sucesso das operações estrangeiras.⁶ Em 2014, o Brasil é o membro dos BRICS (Brasil-Rússia-Índia-China-África do Sul) que melhor protege segredos comerciais, afirma a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) (VALOR, 2014).

2 OS TRATADOS INTERNACIONAIS ACERCA DO TEMA

⁴ “Hoje em dia, a proteção do conhecimento adquirido impacta diretamente o desenvolvimento econômico dos países do chamado primeiro mundo, que impõem aos demais estados sanções comerciais e cobrança de royalties pelas tecnologias disponibilizadas, mantendo países soberanos sob sua dependência econômica, inibindo o seu crescimento e, tratando-os como se ex-colônias fossem”. (RBI, 2012, p. 69-70 Apud CPI, 2014).

⁵ “Uma consequência da falta de cultura de inteligência no Brasil é o despreparo dos brasileiros (tanto na iniciativa privada quanto no setor público) para fazer frente a ameaças reais como a espionagem (a serviço de outros Estados ou de outras organizações), a atuação de organizações criminosas e mesmo de grupos terroristas. Com isso a vulnerabilidade do Brasil diante desse tipo de ameaça é enorme. Outra consequência é a falta de investimento no setor e a ausência de mecanismos legais e institucionais que viabilizem o trabalho do pessoal de inteligência”. (SENADO FEDERAL, 2014:88).

⁶ “A vantagem do uso de oficiais ‘sem cobertura oficial’ (NOCs, no jargão americano, ou ‘ilegais’, no jargão Russo) estão localizadas na maior flexibilidade e eficiência das operações. Montando estórias cobertura que podem relacionar-se a uma variedade de estratos sociais e profissionais (jornalistas, representantes comerciais, financistas, residentes estrangeiros de uma terceira nacionalidade, entomologistas, membros do clero, industriais, médicos, etc), os serviços de inteligência ampliam o leque de alvos possíveis para recrutamento de agentes e informantes e dificultam o trabalho de vigilância da contra-inteligência”. (CEPIK, 2003, p.39)

A espionagem internacional estatal é uma arma em tempos de guerra e, por isso, entende-se tratar de uma prática lícita nesta situação específica. Muito embora existam tratados que versem sobre guerra e direito humanitário, a espionagem e os espões costumam ter uma certa proteção no tratamento dado por estas leis. São exemplos de tratados internacionais que versam sobre a espionagem internacional: as Convenções de Haia sobre o Direito e os Costumes de Guerra Terrestre, datados de 1899 e 1907, bem como as Convenções de Genebra de 1864, 1906, 1929 e 1949 e, os três protocolos adicionais desta última edição. Segundo Fábio de Macedo Soares Pires Condeixa na Revista Brasileira de Inteligência, a 1ª Convenção de Haia traz a seguinte definição sobre a figura do espião durante a guerra:

Somente será considerado espião o indivíduo que, agindo clandestinamente ou sob falsos pretextos, obtenha ou busque obter informações na zona de operações de um [Estado] beligerante, com a intenção de comunicá-las à parte adversa. Desse modo, os militares não disfarçados que hajam penetrado na zona de operações do exército inimigo com o objetivo de obter informações não serão considerados espões. Da mesma forma, não serão considerados espões: soldados ou civis cumprindo ostensivamente sua missão, encarregados de transmitir expedientes tanto para seu próprio exército quanto para o de seu inimigo. A essa categoria pertencem igualmente os indivíduos enviados em balões aerostáticos para transmitir expedientes e, de forma geral, para manter a comunicação entre as diversas partes de um exército ou de um território (CONDEIXA, 2015).

Esta definição é importante pois, ainda segundo ele, estas pessoas teriam uma maior proteção no caso de serem capturadas, visto que as nações costumam impor medidas severas para prisioneiros de guerra. No entanto, em um cenário de paz, a espionagem internacional vive em uma espécie de limbo jurídico, já que não existe uma vedação expressa em tratados internacionais sobre este tipo de atividade. Existem, no entanto, três correntes distintas acerca do tema. A primeira acredita que a espionagem internacional em tempos de paz por uma nação em outra é um ato ilícito e viola o direito internacional. Condeixa justifica esta corrente da seguinte forma:

Esse posicionamento, defendido por Manuel Garcia-Mora, Quincy Wright e Ingrid Delupis, baseia-se em duas proibições estabelecidas em tratados internacionais: 1) a proibição de ingerência arbitrária na vida íntima dos indivíduos (art. 17 do Pacto Internacional de Direitos Civis e Políticos (BRASIL, 1992)); e 2) a proibição de violação da integridade territorial e independência política de um Estado por outro (art. 2º da Carta das Nações Unidas (BRASIL, 1945). (CONDEIXA, 2015, p. 23).

Já a segunda corrente defende tratar-se de ato lícito, ainda que internamente a lei daquele país diga o contrário. Isto quer dizer que, caso seja pego, o espião internacional poderá ser julgado conforme as leis do país que estava espionando, porém, a nação para a qual ele atua não poderia ser julgada internacionalmente pela Corte Internacional de Justiça visto não haver uma lei internacional que proíba a espionagem.

A terceira corrente está no meio termo entre as duas, ou seja, entende que depende da situação e que cada caso deva ser analisado isoladamente. Aqui a solução da controvérsia seria resolvida com base na diplomacia⁷ entre os dois (ou mais) países envolvidos na situação. Um bom exemplo de Lei internacional que pode ser usada para tratar de espionagem é a Convenção de Viena sobre Relações Diplomáticas (1961) Ela não menciona explicitamente a palavra "espionagem", mas estabelece em seu Artigo 41 que "os agentes diplomáticos têm o dever de respeitar as leis e regulamentos do Estado acreditado" e "têm o dever de não interferir nos assuntos internos deste Estado". Além disso, os Artigos 31, c, e 42 estabelecem que o agente diplomático não poderá exercer atividade incompatível com a missão, tampouco em benefício próprio.

Embora a Convenção não mencione diretamente a palavra "espionagem", esses artigos estabelecem as regras para a conduta diplomática entre os países e podem ser usados para proibir a espionagem.

A título de exemplo, os EUA possuem, na Lei de Vigilância de Inteligência Estrangeira, uma seção que autoriza a NSA a coletar informações digitais de estrangeiros no exterior independente de autorização judicial. No entanto, ainda segundo a Lei, esta seção deve ser aprovada novamente pelo Congresso a cada cinco anos (CONJUR, 2017). Com isso, podemos concluir que, uma vez que a espionagem internacional é algo intrínseco da história mundial, e provavelmente continuará sendo, ainda mais com os avanços da tecnologia nos dias de hoje, não há como criar uma legislação internacional

⁷ “[...] a natureza do País, seus limites, sua fertilidade ou esterilidade, a indústria, o comércio, sua inclinação para as armas ou para as artes, sua boa ou má disposição em relação ao seu príncipe. As forças terrestres ou marítimas, quais chefes comandam, naturais, estrangeiros, seu valor e reputação, as próprias forças de que o príncipe pode fazer uso em tempo de guerra ou por qual estrangeiro ele pode ser assistido, seja pelo interesse comum entre eles ou subvencionando-o. Qual sua disposição em relação aos países vizinhos ou outros e a destes em relação a ele. O fundamento e as ocasiões que uns e outros pode ser bem ou mal combinados, o rendimento e o gasto corrente deste príncipe; seu tesouro e quanto ele pode crescer por ano. Quais são os seus ministros e conselheiros, suas qualidades pessoais, sua união ou desunião, seus objetivos e interesses particulares, suas oportunidades e a falta delas, se eles são de uma probidade sólida e de uma fidelidade que nenhuma corrupção possa ocorrer, se o lugar que eles ocupam no governo foi alcançado por mérito ou por favor, que parte os grandes tem nos negócios e qual o apreço que o príncipe dispensa a eles. Finalmente, a honra e o gênio desse príncipe, sua capacidade, seus exercícios, inclinações, virtudes, vícios, tanto quanto o conhecimento de todas essas particularidades, pode proporcionar uma grande luz a todos os que com ele tiverem negociado”. (DUROSELLE, 2000, p. 122).

específica para tratar do tema, mas há, sim formas de limitar a invasão dos países nos segredos⁸ uns dos outros.

3 OS MECANISMOS DE COMBATE A ESPIONAGEM INTERNACIONAL NO BRASIL

A espionagem, seja industrial ou comercial, é algo comum, feita por todos os grandes países que ficam de olho em seus inimigos ou aliados. Mas ao mesmo tempo que os países querem saber informações sobre os outros, os outros também estão neste movimento, o que obriga que os Estados também desenvolvam formas de se defenderem da espionagem internacional.⁹ Entre os alvos, é possível ilustrar alguns segmentos a fim de melhor compreender essa dinâmica:

De acordo com o Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, publicado pelo National Counterintelligence Center, os principais setores que se constituem em alvos prioritários da espionagem internacional nos EUA são: biotecnologia, aeroespacial, defesa, telecomunicações, tecnologia de computadores e pesquisas de energia (BESSA, 2009, p.323).

Deste modo, insere-se nesta reflexão a importância das atividades de inteligência de um Estado. De acordo com Martins: a inteligência funcionaria tradicionalmente em três níveis: estratégico (capacidades e intenções); tático (inteligência operacional) e contrainteligência (proteção dos segredos de uma nação a partir de operações de espionagem de outras nações) (MARTINS, 2014,p.16).

Para a legislação brasileira, inteligência:

É a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado e

⁸ “Com a crescente concorrência global, as empresas terão cada vez mais necessidade de informação, tanto do mercado, quanto a respeito dos planos e intenções de consumidores e dos competidores. A informação também propicia à empresa um profundo conhecimento de si mesma e de sua estrutura de negócios, facilitando o planejamento, a organização, a gestão e o controle dos processos”. (REZENDE; ABREU, 2006, p.109).

⁹ A inteligência é uma das atividades fundamentais de qualquer Estado, e tem reflexos diretos sobre o bem-estar de todos os cidadãos. É a partir de dados de inteligência que o Estado planeja e executa políticas públicas de defesa nacional, segurança pública e relações exteriores. Parte das atividades de inteligência diz respeito à proteção das informações que são sensíveis para a própria realização dessas políticas. Ou seja, a ideia de que cada país deve desenvolver meios efetivos de inteligência e de contrainteligência é uma faceta permanente das relações internacionais. (CEPIK,2003 p.6)

como contrainteligência a atividade que objetiva neutralizar a inteligência adversa (BRASIL, 1999, p.1).

A Contrainteligência, por sua vez:

É a atividade que objetiva prevenir, detectar, obstruir, e neutralizar a inteligência adversa e ações de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem (BRASIL, 2009, p.1).

Por parte do Subsistema de Inteligência de Segurança Pública – SISP, contrainteligência é:

[...] a atividade que objetiva salvaguardar dados e conhecimentos sigilosos e identificar e neutralizar ações adversas de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem”. (BRASIL, 2009, p. 3)

Outro prisma a ser apresentado é o valor da informação para a atividade empresarial, apresentamos os conceitos de gestão do conhecimento e de inteligência competitiva. A gestão do conhecimento é um sistema abarca uma série de atividades, dentre as quais a geração, o compartilhamento, a sistematização e pulverização do conhecimento, mas dentro de um cenário corporativo:

[...] como um sistema que abrange todos os fluxos e processos relacionados ao fomento da geração, compartilhamento, sistematização e disseminação do conhecimento no ambiente corporativo, de forma a subsidiar o desenvolvimento de atividades/tarefas, bem como o processo de tomada de decisão e, consequentemente, a obtenção de vantagem competitiva. (VALENTIM, 2006).

A inteligência competitiva, por sua vez, consiste em investigar o cenário de atividades da organização, interna e externamente, no intuito de ampliar suas oportunidades de negócios e a redução dos riscos, sendo essas as explicações de Maria Inês Tomáel:

A Inteligência Competitiva (IC), cujo objetivo é investigar o ambiente de atuação da organização (interno e externo), para levantar novas oportunidades de negócios e reduzir os riscos, é um processo composto por várias etapas, que envolvem a identificação, a coleta, o tratamento e a disseminação de dados, informação e conhecimento. Configura-se como umas das principais alternativas que contribuem efetivamente para uma melhor execução das

estratégias organizacionais. É através desse sistema de informação que a organização poderá prospectar, selecionar, filtrar, analisar e disseminar a massa informacional necessária para torná-la competitiva (TOMAËL, 2006).

O Brasil possui alguns mecanismos de defesa que ajudam no combate à espionagem internacional. Os primeiros registros da Inteligência de Estado datam de 1927, em que atuavam de forma complementar em conselhos de governo e, posteriormente, com o Serviço Federal de Informações e Contrainformações (SFIC) entre 1946 e 1964 (BRASIL, 2020). Em um momento mais moderno e atual, foi criada a Agência Brasileira de Inteligência, a ABIN (BRASIL, 2020), em 1999, órgão ligado à Presidência da República e vinculado à Casa Civil, que tem como objetivo fornecer informações estratégicas¹⁰ a ministros e ao Presidente da República, para que estes tomem decisões assertivas.

Atua tanto na segurança nacional, que inclui o Estado e a sociedade, como na segurança internacional, com relações exteriores. Outro mecanismo de proteção nacional é a Lei 14.197/2021, que acrescentou o Título XII na Parte Especial do Decreto-Lei nº 2.848/1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito; e revogou a Lei nº 7.170/1983 (Lei de Segurança Nacional). Ela apresenta medidas para proteger a soberania nacional, a integridade do território e o regime democrático do país. Ela também define crimes contra a segurança nacional e estabelece penas para quem os comete.

Entre aproximadamente 90 países, a importância fundamental da informação trouxe um conjunto de normas aptas a regulamentar o acesso, cabendo citar a Suécia, Colômbia, Estados Unidos e México como pioneiros e implementadores de inovação nesse sentido:

Leis como a LAI já existem em cerca de 90 nações, sendo a Suécia a primeira a desenvolver seu marco legal sobre acesso, em 1766. No ano de 1888, a Colômbia se tornou a pioneira na América Latina ao estabelecer um Código que dava acesso a documentos de Governo. Já os Estados Unidos criaram a sua Lei de Liberdade de Informação (Freedom of Information Act - FOIA) em 1966, acrescentando emendas para adequá-la conforme a passagem do tempo. A legislação do México, aprovada em 2002, é considerada referência por prever a instauração de sistemas rápidos de acesso, a serem supervisionados por órgão independente. O Uruguai e o Chile, entre outros, também regulamentaram leis de acesso à informação (BRASIL, 2013).

¹⁰ “A Informação Estratégica é o conhecimento referente às possibilidades, vulnerabilidades e linhas de ação prováveis das Nações Estrangeiras. Nos Estados Unidos destina-se direta ou indiretamente ao uso do Conselho de Segurança Nacional e outras agências de formulação política do Governo Federal”. (PLATT, 1974, p.31)

No Brasil, a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso à informações previsto no inciso XXXIII do artigo 5º, inciso II do § 3º do artigo 37 e no § 2º do artigo 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Segundo Irineu Francisco Barreto Junior e Osmar Fernando Gonçalves Barreto:

Atualmente, entende-se que exista um regime global de acesso à informação, no qual diversos países promulgaram Leis de Acesso à Informação, inclusive, sendo tal regulação uma contrapartida para que países recebessem empréstimos do Fundo Monetário Internacional (FMI) (BARRETO JUNIOR e BARRETO, 2018, p. 41).

A Lei de Acesso à Informação (Lei nº 12.527/2011) permite que qualquer pessoa solicite informações de órgãos públicos federais, estaduais e municipais, mas também prevê a proteção de informações sigilosas e a possibilidade de classificação de informações como secretas ou ultrassecretas.

Segundo a Lei, informação sigilosa nos termos do artigo. 3º, III, da Lei 12.527 é “aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado”. Por isso, quando consideradas imprescindíveis à segurança da sociedade ou do Estado (BRASIL, 2017), informações que podem (I) pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional; (II) prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais; (VII) - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou (VIII) - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações, são passíveis de sigilo. Outro relevante é o Acordo de Salvaguardas Tecnológicas (AST) entre Brasil e Estados Unidos.

Trata-se de “um instrumento assinado entre dois países em que estes se comprometem a proteger as tecnologias das partes. Além de uma declaração de confiança, é uma condição obrigatória para o uso do Centro Espacial de Alcântara (CEA) como base de lançamento de objetos espaciais de quaisquer países que possuam componentes americanos. O formato do acordo é utilizado por países como China, Ucrânia, Rússia, Índia, Nova Zelândia e está dentro de uma praxe internacional (BRASIL, 2023).

Este acordo funciona como compromisso entre os dois países garantindo que as tecnologias e patentes estarão protegidas contra o uso ou cópia não autorizados, ou seja, espionagem. Portanto, a espionagem internacional é tratada como crime tanto na esfera penal, como na administrativa e política.

A espionagem é um dos poucos crimes na legislação brasileira que podem, em tempo de guerra, levar à pena de morte, seja o condenado nacional ou estrangeiro, civil ou militar, além de sujeitar o militar que a pratique à indignidade para o oficialato. (CONDEIXA, p. 26, 2015)

O Programa Nacional de Proteção ao Conhecimento Sensível (PNPC) é uma consultoria de segurança com foco na prevenção de espionagem, sabotagem e vazamento de informações. Desde 1997, busca promover a proteção de conhecimentos sensíveis em instituições nacionais, públicas ou privadas (BRASIL, 2021):

“Esse programa tinha por objetivos sensibilizar os segmentos público e privado do País para a seriedade do problema, ao mesmo tempo em que buscava, através de cursos e palestras de sensibilização, difundir conhecimentos básicos de como se proteger e dificultar a ação da espionagem, principalmente a econômica. [...] os temas, de forma geral, eram os seguintes: classificação apropriada, controle e proteção dos documentos sensíveis; proteção dos bancos de dados e das redes de computadores contra acesso não autorizados; identificação e destruição do lixo sensível da empresa; guarda ou arquivamento de documentos sensíveis; medidas de segurança nos locais onde são discutidos assuntos sensíveis da empresa; valor da informação ou conhecimento sensível para a empresa e seu computador, necessidade de medidas de proteção; controles sobre os empregados e sobre o acesso de visitantes a dados sigilosos, baseados no princípio da ‘necessidade de conhecer’; cuidados na utilização dos meios de comunicação (telefone, fax e computador); educação e sensibilização de segurança para todos os funcionários sobre as ameaças que a espionagem econômica traz para o emprego e para o bem-estar econômico da organização, com ênfase na responsabilidade compartilhada entre todos os funcionários para aderirem e praticarem efetivamente as medidas de segurança” (BESSA, 2009, p.325-326).

E com o mundo modernizado em que vivemos, necessário também tratar da proteção em ambientes tecnológicos, a chamada infovigilância. Após a revelação de Snowden, o PLC 21/2014, que deu origem ao Marco Civil da Internet e que foi uma das prioridades do governo em 2013, foi aprovado com o intuito de garantir maior privacidade na rede mundial de computadores. É possível dizer, então, que a Lei 12.965/2014 que regula direito, deveres e garantias dos usuários da *world wide web* no país, é um outro mecanismo contra a espionagem internacional.

O texto da nova lei foi elaborado com base no documento “Princípios para a governança e o uso da internet”, do Comitê Gestor da Internet no Brasil (CGI.br), organismo multissetorial responsável por integrar iniciativas de uso e desenvolvimento da internet brasileira. O documento é resultado de uma consulta pública, promovida entre 2009 e 2010, na qual foram arroladas mais de 800 contribuições de diferentes representantes da sociedade civil. Entre os principais eixos temáticos tratados pelo texto, e adotados pelo Marco Civil da Internet, estão a privacidade, a neutralidade da rede e a inimizabilidade da rede. Tais princípios garantiriam os direitos e liberdades democráticas de internautas frente a ações abusivas de governos (nacionais e estrangeiros) e empresas prestadoras de serviços. (BEZERRA; WALTZ, p. 162, 2014)

Nesta mesma linha, da segurança informacional¹¹, o País tem ainda o Departamento de Segurança da Informação e Cibernética (DSIC) que é responsável por:

[...] assessorar política, estratégica e tecnicamente, no que tange à segurança da informação e cibernética, o Secretário de Segurança da Informação e Cibernética e o Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República para contribuir com a garantia da segurança institucional, dos interesses nacionais e da segurança do Estado e da sociedade brasileira (BRASIL, 2021).

Dentre suas atuações principais, podemos citar como exemplo:

(i) “assistir o Ministro de Estado Chefe no exercício da função de Autoridade Nacional de Segurança, para o tratamento de informação classificada decorrente de tratados, acordos e outros atos internacionais; (ii) planejar, coordenar e supervisionar a atividade nacional de segurança da informação e cibernética, a gestão de incidentes cibernéticos, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas; (iii) propor, implementar, acompanhar e avaliar tratados, acordos e outros atos internacionais relacionados à segurança da informação, em especial, ao tratamento e à troca de informações sigilosas; (iv) fiscalizar o credenciamento de segurança de pessoas físicas e jurídicas, de órgãos e de entidades para o tratamento da informação sigilosa; (v) acompanhar e avaliar as políticas e as diretrizes globais de organismos multilaterais e participar da elaboração da posição do Governo federal nesses organismos, nos assuntos relacionados à segurança da informação (BRASIL, 2020).

¹¹ É surpreendente descobrir quantos aspectos dos países estrangeiros podem afetar direta ou indiretamente nossos interesses nacionais. Considera-se, normalmente, que a Informação Estratégica abrange oito ou dez ramos. Cada um desses ramos funda-se numa ou mais ciências naturais ou sociais. Estão relacionadas abaixo, na ordem decrescente de importância da ciência natural e, crescente da importância da influência humana na composição de cada um: 1. Informação científica, incluindo as ciências naturais e saúde, potencial científico humano, possibilidades científicas de apoio à indústria, à pesquisa e ao desenvolvimento científico (inclusive engenharia); 2. Geografia, inclusive as condições meteorológicas, clima e oceanografia; 3. Transportes, estradas, telecomunicações; 4. Informação econômica, incluindo indústria, finanças e emprego; 5. Informação militar (excluída as informações de combate); 6. Informação sociológica, incluindo população, religião, educação, tradições nacionais, índole do povo; 7. Informação política, incluindo governo, partidos políticos e política externa; e 8. Informação biográfica (PLATT, 1974, p. 31).

Dito isso, é possível perceber que, apesar de não haver uma lei específica que trate sobre a proteção nacional contra a espionagem internacional, o Brasil possui mecanismos para punir os países ou demais agentes que atuem no sentido de ultrapassar os limites da soberania nacional.

CONSIDERAÇÕES FINAIS

Com lastro na pesquisa, disponibilizada acima, fica cristalina a importância da informação na contemporaneidade, de modo que pode-se apontar que uma grande parcela da população mundial está inserida em uma sociedade da informação, que se traduz em agrupamento de nações que convivem em estado gregário e que em colaboração mútua, tem como seu padrão comum se nortear pela informação como seu maior ativo, e que possuem como principal ferramenta para formarem um regime global de acesso à informação: a internet.

Por ter se tornado esse grande ativo, e em razão das facilidades promovidas pelas Tecnologias da Informação e Comunicação (TICs), a espionagem passou do modelo tradicional (baseado em infiltrações de agentes disfarçados no país investigado, a fim de obterem dados por meio de: relatos, fotografias e fotocópias de documentos), para o modelo digital (lastreado em infiltrações digitais promovidas por crackers, para obtenção de informações de outros países, disponíveis na rede mundial de computadores).

Muitos países estão se utilizando dessa espionagem digital para conseguirem dados sensíveis de outros países, como ficou público e notório com o caso Edward Snowden, que é um analista de sistemas, ex-administrador de sistemas da CIA e ex-contratado da NSA, que tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA, apontando, inclusive, a espionagem dos Estados Unidos da América (EUA) sobre a presidente do Brasil na época, como abordado no artigo.

Em que pese as mudanças tecnológicas terem mudado consideravelmente o principal modo de espionagem no mundo, a regulamentação internacional sobre o assunto não foi atualizada, e se lastreia em tratados internacionais antigos, como na Convenção de Viena, para dirimir contendas oriundas de espionagem, de modo que, embora não mencione diretamente a palavra "espionagem", estabelece as regras para a conduta diplomática entre os países e podem ser usados para proibir a espionagem, de modo a aplicar as leis do país espionado para punir o espião.

Conclui-se que, apesar de o Brasil possuir mecanismos de combate a espionagem, como a atuação da Agência Brasileira de Inteligência (ABIN), da instauração do Programa Nacional de Proteção ao Conhecimento Sensível (PNPC) e da entrada em vigor da Lei de Acesso à Informação (LAI), o país ainda não possui uma legislação específica sobre o tema, como os EUA, por exemplo, o que permitiria um enfrentamento mais robusto da espionagem internacional, no sentido de que existiriam sanções específicas para a espionagem digital, que poderiam ser utilizadas com base no permissivo da Convenção de Viena, para proteger a soberania do Brasil.

REFERÊNCIAS

ASSIS MOREIRA, De Genebra. *Brasil é o Bric que melhor protege segredos comerciais, afirma OCDE*. Valor 05/02/2014. Disponível em: <https://valor.globo.com/brasil/coluna/brasil-e-o-bric-que-melhor-protege-segredos-comerciais-afirma-ocde.ghml>. Acesso em: 17/03/2023.

BARRETO JUNIOR, Irineu Francisco; BARRETO, Osmar Fernando Gonçalves Barreto. Movimentos sociais e transparência na administração pública: Lei de Acesso à Informação (LAI) como instrumento de cidadania na sociedade da informação. In: SCHWARTZ, Germano (Org.). *A reflexividade jurídica dos novos movimentos sociais do Século XXI no Rio Grande do Sul*. Porto Alegre: Livraria do Advogado, 2018.

BERDU, Guilherme Paul. A política externa brasileira frente à espionagem dos EUA, *Cadernos do Tempo Presente*, n. 25, set./out. 2016, p. 3-30 | Disponível em: <http://www.seer.ufs.br/index.php/tempo> Acesso em: 22/04/2023.

BESSA, Jorge. *A Contra-espionagem brasileira na guerra fria*. Brasília: Thesaurus, 2009. 318p.

BEZERRA, Arthur Coelho; WALTZ, Igor. Privacidade, neutralidade e inimizabilidade da internet no brasil: avanços e deficiências no projeto do marco civil. **Revista Eptic Online**, Vol.16 n.2 p.161-175, mai-ago 2014.

BND - *Bundesnachrichtendienst. The Foreign Intelligence Service of Germany. Serviço de Inteligência Estrangeira da Alemanha*. Disponível em: https://www.bnd.bund.de/EN/Home/home_node.html. Acesso em: 17/03/2023.

BRASIL. *A ABIN - Agência Brasileira de Inteligência*. Publicado em: 22/09/2020 16h04. Atualizado em 02/03/2023 13h34. Disponível em: <https://www.gov.br/abin/pt-br/aceso-a-informacao/institucional/a-abin>. Acesso em: 22/04/2023.

_____. *Acesso à Informação: Ações e Programas*. O que é. Publicado em 20/10/2021 11h52 Atualizado em 28/06/2022 15h01 Disponível em: <https://www.gov.br/abin/pt-br/aceso-a-informacao/acoes-e-programas/PNPC/o-que-e-1>. Acesso em: 22/04/2023.

_____. *Acesso à Informação*. Histórico. Publicado em 22/09/2020 17h12 Atualizado em 02/03/2023 17h22. Disponível em: <https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/historico>. Acesso em: 22/04/2023.

_____. *Conhecendo o acordo de salvaguardas tecnológicas Brasil e Estados Unidos*. MINISTÉRIO DA DEFESA MINISTÉRIO DAS RELAÇÕES EXTERIORES, MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. Governo Federal. Disponível em: <https://www.gov.br/aeb/pt-br/centrais-de-conteudo/publicacoes/acordo-de-salvaguardas-tecnologicas/ast.pdf>. Acesso em: 22/04/2023.

_____. *Constituição da República Federativa do Brasil de 1988*. Disponível em http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 22/04/2023.

_____. Decreto nº 8.793 de 29 de junho de 2016. *Dispõe sobre a Política Nacional de Inteligência nos termos estabelecidos pela Lei nº 9.883, de 7 de dezembro de 1999*. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8793.htm>. Acesso em: 22/04/2023.

_____. Decreto nº 56.435, de 8 de junho de 1965. *Promulga a Convenção de Viena sobre Relações Diplomáticas*. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/antigos/d56435.htm Acesso em: 22/04/2023.

_____. Decreto nº 4.376 de 13 de setembro de 2002. *Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, instituído pela Lei nº 9.883, de 7 de dezembro de 1999, e dá outras providências*. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/2002/d4376.htm>. Acesso em: 22/04/2023.

_____. *Gabinete de Segurança Institucional*. Institucional. Publicado em 24/11/2020 15h01. Disponível em: <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/institucional>. Acesso em: 17/03/2023.

_____. *Lei de Acesso à Informação completa um ano*. Notícias. Disponível em: <http://www.brasil.gov.br/noticias/arquivos/2013/05/16/lei-de-acesso-a-informacao-completa-um-ano>. Acesso em: 17/03/2023.

_____. Lei nº 9.883 de 7 de dezembro de 1999. *Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – ABIN, e dá outras providências*. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/L9883.htm>. Acesso em: 22/04/2023.

_____. Lei 12.527 de 18 de novembro de 2011. *Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e*

dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 17/03/2023.

_____. Lei nº 14.197, de 1º de Setembro de 2021. *Acréscima o Título XII na Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), relativo aos crimes contra o Estado Democrático de Direito; e revoga a Lei nº 7.170, de 14 de dezembro de 1983 (Lei de Segurança Nacional), e dispositivo do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais)*. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14197.htm#art4 Acesso em: 17/03/2023.

_____. Resolução Nº 1, de 15 de julho de 2009. *Regulamenta o Subsistema de Inteligência de Segurança Pública – SISP*.

CVM – COMISSÃO DE VALORES IMOBILIÁRIOS. *Uso Indevido de Informação Privilegiada*. (Insider Trading). Cadernos. Rio de Janeiro: Comissão de Valores Imobiliários, 2016. Disponível em: <http://www.abrasca.org.br/Uploads/insider-trading/Uso-indevido-informacao-privilegiada-CVM.pdf>. Acesso em: 22/04/2023.

CEPIK, Marco A.C. Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação. *Security and Defense Studies Review*. Vol.2 Winter. 2002/2003.

_____. *Serviços de Inteligência: Agilidade e Transparência como dilemas de institucionalização*. Tese de doutorado apresentada no IRPERJ. 2001a.

_____. *Segredos Públicos: um dilema democrático*. Insight Inteligência – Voyeurismo. Julho-Agosto-Setembro 2001b.

_____. Regime político e sistemas de Inteligência no Brasil: legitimidade e efetividade como desafios institucionais. DADOS – *Revista de Ciências Sociais*, Rio de Janeiro, Vol. 48, nº 1. 2005.

_____. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: ANDRÉ DE MELLO e Souza; NASSER, R. M.; MORAES, R. F. (2014) [orgs.]. *Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século*. 1. ed. Brasília: Instituto de Pesquisa Econômica Aplicada Ipea, 2014, p. 161-186.

CONDEIXA, Fabio de Macedo Soares Pires. Espionagem e Direito, *Revista Brasileira de Inteligência*. Brasília: Abin, n. 10, dezembro 2015.

DABALT, Lucas. Descubra qual é a diferença entre FBI e CIA. *Revista Digital*. Atualizado em: 10/02/2023 Disponível em: <https://revistadigital.com.br/ descubra-qual-e-a-diferenca-entre-fbi-e-cia/>. Acesso em: 17/03/2023.

DGSE - *Direction Générale de la Sécurité Extérieure*. *Direção Geral da Segurança Externa – França*. Disponível em: <https://www.dgse.gouv.fr/en>. Acesso em: 17/03/2023.

DIOGO, José Manuel. *As grandes agências secretas: os segredos, os êxitos e os fracassos dos serviços secretos que marcaram a história*. Editora Via Leitura. São Paulo, 2013.

DUROSELLE, Jean-Baptiste. *Todo império perecera*. Brasília: Ed. Universidade de Brasília; São Paulo: Imprensa Oficial do Estado, 2000.

ESPIONAGEM CIBERNÉTICA *Rede vulnerável Para CPI, é preciso aparelhar inteligência nacional e melhorar gestão da internet Os principais debates do Senado Federal* Ano 5 - Nº 21 julho de 2014 Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/503306/140714-emdiscussao-espionagem.pdf?sequence=1&isAllowed=y>. Acesso em: 22/04/2023.

G1. *Entenda o caso de Edward Snowden que revelou espionagem dos EUA*. Disponível em: <https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 01/03/2023.

GONÇALVES, Joanisval Brito. *O controle da atividade de inteligência em regimes democráticos: os casos de Brasil e Canadá*. 2008. 797 f. Tese (Doutorado) – Curso de Relações Internacionais, Instituto de Relações Internacionais, Universidade de Brasília, Brasília, jun. 2008.

GUERRA, Sidney. *O direito à privacidade na internet: uma discussão da esfera privada no mundo globalizado*. Rio de Janeiro: América Jurídica, 2004.

IVANISSEVICH, Alicia. ESPIONAGEM: qual o limite? Entrevista com Marco Aurélio Cepix. *Revista CIÊNCIA HOJE*, RJ, vol. 52, out. 2013 Disponível em: <https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html> Acesso em: 22/04/2023.

JORNAL NACIONAL. *Governo brasileiro cobra do Canadá explicações sobre espionagem*. G1. Edição do dia 07/10/2013. Disponível em: <https://g1.globo.com/jornal-nacional/noticia/2013/10/governo-brasileiro-cobra-do-canada-explicacoes-sobre-espionagem.html>. Acesso em: 22/04/2023.

KLEINA, Nilton. *O que é a NSA, o órgão de dados de criptologia norte-americano?* TECMUNDO. 02/05/2021 às 11:00. Disponível em: <https://www.tecmundo.com.br/seguranca/216402-nsa-o-orgao-dados-criptologia-norte-americano.htm>. Acesso em: 17/03/2023.

MARTINS, Alexandre de Oliveira. *Espionagem e Soberania Nacional: Dilemas de Segurança e Defesa no Caso Brasil X EUA (2013)*. Unila. Universidade Federal da Integração Latino-Americana), 2014.

MELO, João Ozorio de. Vigilância Externa. Governo dos EUA quer tornar permanente lei da espionagem digital. *Revista Consultor Jurídico*, 11 de junho de 2017, 9h06. Disponível em: <https://www.conjur.com.br/2017-jun-11/governo-eua-tornar-permanente-lei-espionagem-digital#:~:text=A%20Se%C3%A7%C3%A3o%20702%20da%20Lei,espionagem%20digital%20muito%20mais%20%C3%A1gil>. Acesso em: 22/04/2023.

PAOLOZZI, Vitor. *Reino Unido abre seus arquivos de serviços de espionagem do país*. Valor Econômico, 01/02/2006, Internacional, p. A7. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/457299/noticia.htm?sequence=1> Acesso em: 17/03/2023.

PETER, Laurence. *A história por trás da agência de espiões da Rússia, acusada de promover execuções com o aval do governo*. BBCNEWS. 9 fevereiro 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-42996545>. Acesso em: 17/03/2023.

PLATT, Washington. *Produção de Informações Estratégicas*. Rio de Janeiro: Biblioteca do Exército. Livraria Agir Editora, 1974.

REZENDE, Denis Alcides; ABREU, Aline França. *Tecnologia da informação aplicada a sistemas de informação empresariais: o papel estratégico da informação e dos sistemas de informação nas empresas*. 4. ed. São Paulo: Atlas, 2006.

SENADO FEDERAL. *Relatório Final da CPI da Espionagem*. Brasília, DF, abr. 2014. Disponível em: <http://www.senado.leg.br/atividade/materia/getPDF.asp?t=148016&tp=1>. Acesso em 22/04/2023.

_____. *Relatório Final da CPI da Espionagem*. Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar emails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal. Disponível em: <https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>. Acesso em: 22/04/2023.

SISTEMA BRASILEIRO DE INTELIGÊNCIA. Conselho Consultivo *Manual de Inteligência: Doutrina Nacional de Inteligência: bases comuns*. Brasília: Abin, (2004). 44 p.

TOMAÉL, Maria Inês. et al. A contribuição do processo de inteligência competitiva para a inovação nas organizações. 155-156. In: VALENTIM, M. L. P. (Org.). *Informação, conhecimento e inteligência organizacional*. 2.ed. Marília: FUNDEPE Editora, 2006.

VALENTIM, Marta Lígia Pomim. Processo de inteligência competitiva organizacional. In: TARAPANOFF, Kira (Org.). *Informação, conhecimento e inteligência organizacional*. 2.ed. Marília: FUNDEPE Editora, 2006.