INFRAESTRUTURA CRÍTICA E O CONTROLE DE INVESTIMENTO EXTERNO: A REGULAÇÃO DO BRASIL EM CONTRASTE

Michelle Ratton Sanchez Badin[1]
Maria Eugênia do Amaral Kroetz[2]
Ana Maria Morais[3]
Manu Misra[4]

SINOPSE

Consideram-se setores de infraestrutura crítica (IC) aqueles de tal importância que sua destruição ou obstrução pode acarretar prejuízos para a segurança e a economia de uma sociedade. Com efeito, a abrangência do conceito é dinâmica, acomodando as necessidades dos países em seus diferentes momentos históricos e incluindo atenção à resiliência para atividades consideradas essenciais no contexto de suas políticas públicas (por exemplo, abastecimento de água, saúde pública, transportes, energia, telecomunicações, redes de transmissão de dados). Na experiência internacional, a IC tem sido considerada na implementação dos Instrumentos de Avaliação de Investimento Externo (IAIE). Em diálogo com esse contexto, o objetivo desta contribuição é apresentar como o Brasil se insere no debate de IC, em geral, e identificar se o país, quando das operações de investimento externo, conceitua a proteção às ICs, nos mesmos moldes da prática internacional ou de maneira própria.

Palavras-chave: infraestrutura crítica; Brasil; investimento externo; Instrumentos de Avaliação de Investimento Externo.

ABSTRACT

Critical infrastructure (CI) sectors are important apparatus for the economic and social life of a nation, and any harm, obstructing or destroying them, may affect the security, economy or health of States. The scope of the CI definition has accommodated the needs of countries in their historical moment, and it has included the resilience of activities traditionally described as essential. Examples on this sense are water supply, public health, transport, energy, telecommunications, financial services and data networks. More recently, investment screening mechanisms have taken part in this process, checking the impact of foreign direct investment in local CI. This paper aims to describe the Brazilian regulation about CI, track the recent national debates about this topic, and investigate whether the country, when it comes to foreign investment operations, carries out actions to protect CI.

Keywords: critical infrastructure; Brazil; foreign investment; Investment Screening Mechanism.

JEL: F13; K24; K33.

Artigo recebido em 31/3/2023 e aprovado em 28/7/2023.

DOI: http://dx.doi.org/10.38116/bepi36art2

1. Bolsista do Programa de Pesquisa para o Desenvolvimento Nacional (PNPD) na Diretoria de Estudos e Relações Econômicas e Políticas Internacionais do Instituto de Pesquisa Econômica Aplicada (Dinte/Ipea); e professora associada do programa de pós-graduação *stricto sensu* em direito e desenvolvimento da Escola de Direito de São Paulo da Fundação Getulio Vargas (PPGD/FGV-SP). *E-mail*: michelle.sanchez@fgv.br.

2. Advogada; e doutoranda e mestre em direito dos negócios no programa de direito e desenvolvimento da FGV-SP. *E-mail*: mekroetz@gmail.com.

3. Bolsista do PNPD na Dinte/Ipea; e doutoranda no programa de pós-graduação em economia da Universidade Federal de Juiz de Fora (PPGE/UFJF). *E-mail*: anammoraiss@hotmail.com.

4. Pós-doutorando junto ao PPGD/FGV-SP. *E-mail*: manu.misra@bocconialumni.it.

1 INTRODUÇÃO

A infraestrutura crítica (IC) tem sido um dos focos de atuação dos Instrumentos de Avaliação de Investimentos Externos (IAIE) em diversos países (OECD, 2020; Sanchez-Badin *et al.*, 2021; Misra, 2023). Essa relação é recente e está associada a diferentes fatores da conjuntura global contemporânea, entre os quais se encontram preocupações de ordem geoeconômica e geopolítica, com a ascensão da China e sua exportação de capital (Roberts, Moraes e Ferguson, 2019), riscos e vulnerabilidades das redes de prestação de serviços essenciais (OECD, 2019; Dunn, 2005) e efeitos da pandemia de covid-19 (OECD, 2020; UNCTAD, 2016; 2019).

Como apresentado em Sanchez-Badin *et al.* (2021), alguns países, como Austrália, Canadá, Estados Unidos, Índia, Rússia e Alemanha, vêm construindo uma ligação entre a proteção de sua IC e o controle ou avaliação do investimento externo, com destaque para casos no setor de energia. Alguns acordos internacionais alinhados a este movimento também têm incorporado a proteção às ICs como parte das exceções de segurança na proteção ao investimento externo.[5] Recentemente, a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) redigiu uma nota de política pública na qual sugere orientações para países em desenvolvimento para atrair investimento estrangeiro direito (IED) em maior quantidade, melhor qualidade e seguro para ampliação e modernização de sua IC local.[6] A preocupação de segurança da OCDE, alinhada com a intenção declarada do Grupo dos Sete (G7), é de proteção contra potenciais ameaças à segurança econômica dos países em desenvolvimento, as quais teriam origem especialmente em operações de IED realizadas por entidades estrangeiras apoiadas pelo Estado (State-backed FDI), muitas vezes combinadas com financiamento e implementação também confiados a entidades apoiadas pelo Estado (OECD, 2023).

Entretanto, o debate sobre IC é anterior à sua associação com os IAIEs e tem as suas próprias particularidades. No caso do Brasil, o ordenamento jurídico nacional define IC como "instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade" (Brasil, 2018).[7] Contudo, ainda não se observa, no Brasil, uma relação direta entre controle do investimento externo e a regulação de ICs no país.[8]

5. A título de exemplo, ver os acordos de investimento celebrados entre a Associação de Nações do Sudeste Asiático (Association of Southeast Asian Nations – Asean) e Hong Kong (2017, art. 8º, exceções de segurança) e entre a Asean e a Índia (2014, art. 22, exceções de segurança). Disponíveis em: https://investmentpolicy.unctad.org/international-investment-agreements/iia-mapping. Acesso em: 28 mar. 2023.

6. Tradução direta de "Supporting EMDEs [emerging market and developing economies] in attracting more, better and safe FDI [Direct Foreign Investment]" (OECD, 2023).

7. Essa definição, encontrada no art. 1º, inciso I, do anexo do Decreto nº 9.573/18, , disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm, é inspirada na definição dos Estados Unidos, que apresenta seu conceito de IC como "sistemas e ativos, sejam físicos ou virtuais, tão vitais para os Estados Unidos que a incapacidade ou destruição de tais sistemas e ativos teria um impacto debilitante na segurança, na segurança econômica nacional, na saúde ou segurança pública nacional, ou em qualquer combinação dessas questões" (tradução nossa). Disponível em: https://www.cisa.gov/infrastructure-security#:~:text=Critical%20infrastructure%20describes%20the%20physical,or%20public%20health%20or%20safety. Acesso em: 28 mar. 2023. Outros países seguem padrão semelhante, como: o Reino Unido – Infrastructure Act, de 2015, disponível em: https://www.legislation.gov.uk/ukpga/2015/7/contents/enacted; a Austrália – Security of Critical Infrastructure Act, de 2018, disponível em: https://www.legislation.gov.au/Details/C2018A00029; e a África do Sul – Critical Infrastructure Act, de 2019, disponível em: https://www.mondaq.com/southafrica/government-contracts-procurement-ppp/878390/critical-infrastructure-act-2019.

8. Nota-se que apenas o Acordo para Cooperação e Facilitação de Investimentos (ACFI) assinado entre Brasil e Índia, em 2020, contém a indicação de medidas de proteção à infraestrutura pública essencial entre as exceções de segurança, para as regras gerais do acordo (art. 24.1.b.v). Esta redação, contudo, é similar àquela que a Índia tem adotado em outros acordos de investimento – por exemplo, no acordo celebrado com o Quirguistão (2019). Disponível em: https://investmentpolicy.unctad.org/country-navigator/98/india. Acesso em: 24 jun. 2022.

O objetivo deste artigo é localizar o Brasil no debate internacional sobre IC e sua relação com o IED em áreas essenciais para o funcionamento do país. A análise é feita em duas partes: a primeira, com enfoque na construção do conceito e de políticas para ICs, e outra que traça a relação entre as ICs e o controle de investimento externo, como forma de proteção a elas. Em cada uma das partes, encontram-se duas subseções. Na primeira parte, inicialmente é apresentado o debate sobre IC e seus marcos temporais, conforme liderado pela regulação em alguns países e coordenado pela OCDE; em seguida, analisa-se como essa concepção de IC tem influenciado a sua regulação no Brasil. Na segunda parte, detalha-se, a princípio, como tem se dado a associação de setores de IC com a atuação dos IAIEs em alguns países selecionados. Na sequência, apresenta-se um contraponto sobre como as autoridades brasileiras têm atuado na proteção de IC e no controle de operações econômicas envolvendo capital externo, para identificar se existe no país a sobreposição dessas agendas, como se identifica na experiência internacional. Por fim, são apresentadas breves conclusões.

2 A CONSTRUÇÃO DE POLÍTICAS PARA IC

2.1 Histórico recente sobre políticas de proteção para IC

O entendimento da proteção às ICs como um ramo de política pública autônoma é um fenômeno relativamente recente. É consensual dar a devida importância e o devido protagonismo a essa agenda da Comission on Critical Infrastructure Protection (CCIP), criada em 1996 pelo então presidente dos Estados Unidos, Bill Clinton, e ao seu relatório Critical Foundations, de 1997, que consolidou as ICs como assunto de segurança nacional, e seu funcionamento contínuo como premissa central para "prosperidade econômica, força militar e vitalidade política dos Estados Unidos" (Collier e Andrew, 2008, p. 17, tradução nossa).[9]

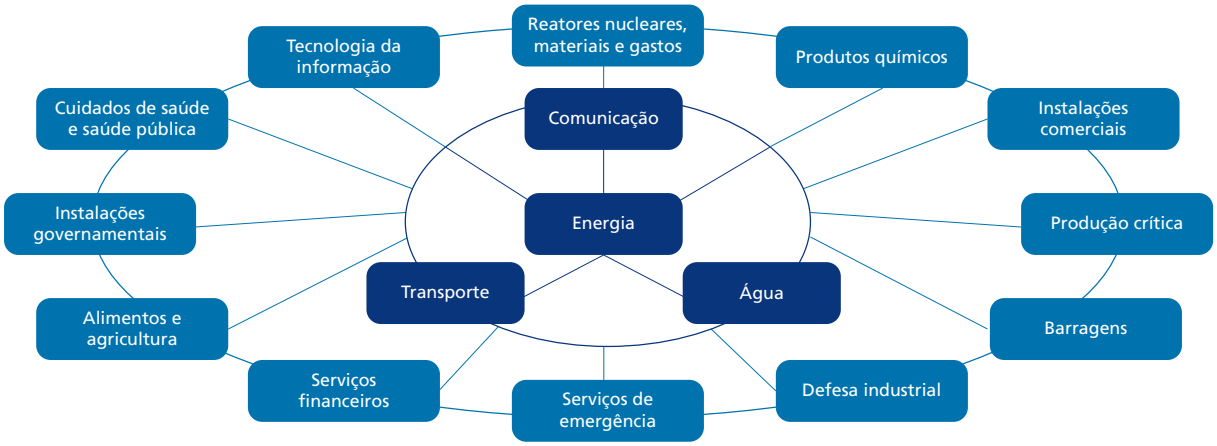
Até meados da década de 1990, a IC tinha como ponto central da sua política pública a adequação das obras às necessidades de segurança nacional. Dois movimentos marcaram uma redefinição dessa política pública. Primeiramente, a resposta aos atentados às Torres Gêmeas no 11 de setembro de 2001, em que os Estados Unidos alteraram suas regras de migração e de controles em aeroportos, articularam um discurso antiterrorismo e implementaram uma política específica governamental de proteção às ICs (Dunn, 2005). Em segundo lugar, a revolução tecnológica, que permitiu maior integração e interdependência entre os sistemas de IC, trouxe a identificação de novas vulnerabilidades. Esses dois fatores promoveram uma expansão expressiva no número de setores e tipos de ativos considerados "críticos" para fins de segurança interna e uma mudança no conteúdo de instrumentos de política pública, leis e regulações nos setores eleitos (Moteff e Parfomak, 2004; Moteff, Copeland e Fischer, 2003). De forma pioneira, os Estados Unidos adotaram, então, diretrizes internas de segurança e trabalharam para a centralização da proteção às ICs pelo governo federal. A coordenação entre agências e autoridades dos diferentes espaços da Federação com o setor privado

9. Apesar do perceptível avanço do arcabouço regulatório e dos estudos técnicos sobre as ICs a partir dos anos 1990, há correlações com estratégias militares da Segunda Guerra Mundial, especificamente, naquele momento sobre o papel das infraestruturas físicas civis para as ofensivas em outros territórios. Collier e Lakoff (2008) qualificaram como *distributed preparedness* a abordagem que considera: i) a preocupação com os sistemas críticos dos quais a sociedade, a economia e a política modernas dependem; ii) a identificação das vulnerabilidades desses sistemas e das ameaças que podem explorar essas vulnerabilidades como questões de segurança nacional; e iii) o esforço para desenvolver técnicas para mitigar as vulnerabilidades do sistema. Nota-se, assim, que um debate mais longínquo que foi liderado pelo setor de defesa passou, mais recentemente, a fazer parte da agenda burocrática civil para a manutenção das condições necessárias para a realização da atividade econômica.

e outras entidades foi também construída como uma faceta importante dos programas de IC dos Estados Unidos (United States, 2009).

A partir desses movimentos, há uma redefinição das ICs como estruturas essenciais para o funcionamento de uma economia e sujeitas a riscos pela interdependência gerada com suas informações, instalações, acessórios e equipamentos compartilhados.[10] Como se trata de sistemas essenciais, não é difícil imaginar um efeito cascata em caso de problemas. Por isso, pode-se dizer que a noção de interdependência é quase constitutiva das ICs contemporâneas. Nesse sentido, Rocha (2019, p. 12) apresenta que "as ICs funcionam em uma complexa rede de conexões que são interdependentes" e que formam "redes de infraestruturas". É ilustrativa a figura 1, que apresenta essa interdependência de algumas ICs e potenciais impactos de suas atividades em diferentes setores relevantes.

FIGURA 1
Interdependência de ICs conforme a US Homeland Security



Fonte: Rocha (2019, p. 13, tradução nossa).

A essa concepção de interdependência passaram a ser associados os conceitos de resiliência e risco.[11] O conceito de resiliência, quando apresentado na política estadunidense, foi questionado quanto à sua precisão.[12] Em resposta, a agência National Infrastructure Advisory Council (Niac) publicou um relatório em que apresentou três critérios para uma IC resiliente: i) a capacidade de manter funções críticas e absorver o impacto em caso de crise ou interrupção; ii) a capacidade de responder e gerenciar uma crise, com habilidade adaptativa e flexibilidade para redirecionar recursos e ativos; e iii) a capacidade de retornar às operações normais da forma mais rápida e eficiente possível.[13]

10. De acordo com um estudo de Giannopoulos, Filippini e Schimmer (2012, p. 4), há quatro tipos de interdependência: i) física, quando depende de um insumo material específico de outra IC; ii) cibernética, quando depende da informação transmitida por outra IC; iii) geográfica, quando é afetada pelas condições ambientais locais de outra IC; e iv) lógica, que seria qualquer outra dependência que não as anteriores.

11. A respeito desta associação, "Devido à multiplicidade de ameaças, à incerteza percebida e à complexidade das interdependências globais, a maioria das estratégias de segurança nacional parece ter adotado uma abordagem baseada no risco de 'todos os perigos' e 'toda a sociedade' como o novo paradigma" (Fjäder, 2014, p. 119, tradução nossa).

12. Walker e Copper (2011) fazem uma genealogia da aplicação da ideia de resiliência nas políticas públicas, apontando para seu uso inicial associado à ecologia e a riscos ao meio ambiente. Contudo, essa percepção da importância da resiliência tem sido estendida para outros fenômenos que aportem riscos, em especial para o funcionamento de ICs. A esse respeito, consultar Fjäder (2014).

13. Disponível em: http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf. p. 12. Acesso em: 28 mar. 2023.

As iniciativas do governo dos Estados Unidos sobre ICs, a partir dos anos 1990, foram recepcionadas por organismos internacionais e reproduzidas por outros países – inclusive pela necessidade de cooperação intergovernamental para o combate às ameaças sistêmicas (Markopoulou e Papakonstantinou, 2021).[14] Seguindo a tendência, a União Europeia implementou em 2006 o Programa Europeu de Proteção das Infraestruturas Críticas (Pepic). O desenho regulatório foi apresentado pela Comissão Europeia em forma de diretiva, sujeitando todos os Estados-membros a seus critérios. O Pepic também serve como base para a estratégia recém-implementada na União Europeia sobre cibersegurança e o aumento da resiliência de estruturas críticas, físicas e digitais do bloco (European Commission, 2020).[15] De maneira similar, África do Sul, Austrália, Canadá, Japão, Reino Unido e Rússia desenvolveram estratégias para a antecipação de incidentes que possam impedir o funcionamento de infraestruturas e serviços com dimensão estratégica (Brunner e Suter, 2009; Fjäder, 2014, p. 124).

A partir de então, uma série de iniciativas para melhor conceituação das ICs resilientes e sobre como avaliar seus riscos tem avançado na literatura especializada.[16] O objetivo neste texto não é explorar detalhadamente o avanço do debate técnico sobre o assunto, que foi assumindo particularidades locais conforme o perfil e o gerenciamento dos setores incluídos nas categorias de IC, incluindo o grau de participação dos setores públicos e privados na prestação desses serviços e também tecnicalidades associadas ao perfil do setor. A proposta é trazer o indício de caminhos deste debate sobre IC em diferentes países, e então, na parte seguinte, compreender como isso tem sido incorporado nos IAIEs.

No tocante a organizações internacionais na área econômica,[17] mais especificamente, destaca-se o papel da OCDE ao analisar políticas associadas a ICs e traçar algumas recomendações a seus membros. Na agenda da organização, o tema de ICs foi associado à agenda de gerenciamento de riscos.[18] A organização, então, legitima sua agenda ao indicar que o não funcionamento das ICs nacionais

14. Como exemplo dessa mobilização internacional, tem-se a publicação da Resolução do Conselho de Segurança da Organização das Nações Unidas (CSONU) nº 1.373/01 e sua disseminação para a estrutura regulatória interna dos Estados. A Resolução CSONU nº 1.373 reconheceu o direito dos países de legítima defesa individual ou coletiva contra atos de terrorismo internacional ao classificá-los como uma "ameaça à paz e segurança internacionais". No Brasil, a Resolução CSONU nº 1.373 foi internalizada pelo Decreto nº 3.976/01. No entanto, a pauta passou a ser de maior relevância para o governo brasileiro a partir de 2006, quando estruturas do estado de São Paulo foram alvo de nove ataques perpetrados por uma organização criminosa, conforme a introdução do anexo ao Decreto nº 10.569/20. Para mais detalhes sobre essa relação entre ataques terroristas e medidas de segurança para ICs, consultar Souza (2008).

15. Vale notar que o programa europeu está alinhado com as alterações regulatórias que ocorreram em diversos países, em que as políticas de segurança da IC passam a se preocupar com o aspecto digital dos serviços e instalações, com regras transversais e setoriais específicas, eminentemente no que se refere à proteção de dados (Roguski, 2021; Dawson *et al*., 2021; Rajavuori e Huhta, 2020).

16. Entre algumas referências relevantes, encontram-se Osei-Kyei *et al*. (2022) e Mottahedi *et al*. (2021).

17. Observa-se que os temas de risco e resiliência integram as agendas de outros organismos mais associados à segurança e também a questões ambientais – estes são espaços que desenvolveram esses conceitos. A respeito, consultar a iniciativa em 2017, no âmbito da Organização das Nações Unidas (ONU) para um comitê de alto nível de diferentes programas no âmbito da organização. Disponível em: https://unsceb.org/analytical-framework-risk-and-resilience. Acesso em: 28 mar. 2023.

18. Entre algumas iniciativas da OCDE a destacar, estão: i) um relatório de 2003 que apresenta cinco grandes eixos – desastres naturais, acidentes tecnológicos, doenças infecciosas, segurança alimentar e terrorismo – para análise de riscos e resiliência (OECD, 2003); ii) uma publicação sobre as ICs enquanto foco de atuação dos IAIEs (OECD, 2008); iii) após a crise financeira de 2008, um relatório com atenção a outros eixos para análise de risco, considerando a crescente interconexão na economia global, tais como crises financeiras, ciberespaço, sistemas biológicos e até mesmo tempestades geomagnéticas (OECD, 2012); iv) a partir de tais diagnósticos a edição, em 2014, das Recommendations of the Council on the Governance of Critical Risks, documento baseado em incertezas geopolíticas, ambientais, sociais e econômicas e que menciona as ICs como foco das políticas de segurança em seus países-membros (OECD, 2014); e, mais recentemente, v) o relatório sobre risco e resiliência com atenção para mudanças climáticas, a pandemia de covid-19 e a crise financeira decorrente (OECD, 2021). Mais relatórios no campo de resiliência e risco disponíveis em: https://www.oecd-ilibrary.org/governance/oecd-reviews-of-risk-management-policies_19934106. Mais informações sobre risco e resiliência em países mais vulneráveis e uma concepção mais associada à governança pública e formas de gerenciamento do risco disponíveis em: https://www.oecd.org/dac/conflict-fragility-resilience/risk-resilience/.

pode enfraquecer do sistema econômico global, levar à disrupção das cadeias de valor interligadas e à vulnerabilidade de capital investido (OECD, 2019, p. 13).

Em relatório de 2019, a OCDE sistematizou a política para ICs em 25 de seus países-membros e definiu o rol de boas práticas para desenvolver a devida resiliência nas ICs (OCDE, 2019).[19] De acordo com o relatório, seis setores são os mais recorrentes nesses países: energia, tecnologias da informação e de comunicação, transporte, saúde, água e finanças. Apesar de a necessidade de proteção das ICs e de resposta resiliente ser uma constante, o que é considerado como risco tem alterações ao longo do tempo (Roberts, 2023; Markopoulou e Papakonstantinou, 2021; Rajavuori e Huhta, 2020). Como consequência prática, tem-se o aumento de setores que são considerados críticos durante o tempo, conforme o avanço das tecnologias e a consequente vulnerabilidade dos sistemas de IC, bem como o interesse dos governos em priorizar determinados setores econômicos.[20]

Também vale observar que, para além das economias da OCDE, em geral os países apresentam significativas diferenças entre as instalações, serviços, bens e sistemas considerados críticos, a depender de seu ponto de vista local e da organização econômica dos setores em nível nacional. A título de exemplo, no apêndice A é apresentado um quadro comparativo (quadro A.1) entre os setores considerados como ICs no Brasil, nos Estados Unidos, na Rússia, no Reino Unido e nos países da União Europeia.

A OCDE, no relatório de 2019, também estabeleceu entre suas orientações para as políticas de IC: i) a criação de uma estrutura de governança multissetorial para resiliência de IC; ii) a avaliação das interdependências e vulnerabilidades nos sistemas de infraestrutura para priorizar os esforços de resiliência; iii) o desenvolvimento de confiança entre o governo e os operadores, em especial para o compartilhamento de informações relacionadas a risco; iv) a promoção de parcerias para definir estratégias comuns e objetivos viáveis de resiliência; v) a combinação de políticas para priorizar medidas de resiliência econômicas em todo o ciclo de vida; vi) a prestação de contas e o monitoramento da implementação de políticas de resiliência de IC; e, ainda, vii) a atenção à dimensão transfronteiriça dos sistemas de infraestrutura. Este último ponto atenta para a necessidade de convergência e cooperação intergovernamental dos países (OECD, 2019).

A garantia da segurança de ICs dos países, portanto, parece estar em um movimento de expansão e escalada, começando por preocupações militares de resguardar as estruturas internas dos países contra ataques terroristas, e passando a incluir crescentemente uma ampla gama de serviços prestados pelos governos. Conclui-se, portanto, a partir das análises dos casos dos Estados Unidos, da União Europeia e de alguns membros da OCDE, que as políticas mobilizadas para proteção das ICs de eventuais riscos estão essencialmente associadas à ideia de segurança nacional. Contudo, tais políticas também mobilizam novas linguagens e conceitos para a implementação das políticas públicas. Destacam-se, neste ponto, a preocupação com a resiliência dos sistemas das ICs, as técnicas para mensurabilidade dos riscos e a atenção à interdependência entre as ICs, para a coordenação das políticas necessárias, nacional e internacionalmente. Por fim, nota-se que tem havido crescente influência da agenda da

19. Os países-membros que responderam à pesquisa da OCDE (2019) foram: Áustria, Bélgica, Canadá, República Tcheca, Estônia, Finlândia, França, Alemanha, Irlanda, Israel, Coreia, Letônia, Luxemburgo, Holanda, Nova Zelândia, Noruega, Polônia, Portugal, República Eslovaca, Espanha, Suécia, Suíça, Turquia, Reino Unido e Estados Unidos.

20. Vale notar como o tema de ICs em geral tem se cruzado cada vez mais com o de infraestruturas críticas em comunicação, que consideram os avanços e a relação com o mundo digital e cibernético. Nesse sentido, consultar Dunn (2005, p. 265) e também, como exemplo, a agenda do tema nos Estados Unidos, disponível em: https://www.cisa.gov/national-risk-management.

pauta cibernética, em especial no dimensionamento da vulnerabilidade e de riscos dos sistemas, com impacto nas políticas de IC. Fica claro que o conceito de IC é dinâmico e procura abranger os desafios que os governos precisam enfrentar em seu cotidiano, conforme as ameaças próprias de seu momento histórico (Roberts, 2023; Markopoulou e Papakonstantinou, 2021; Fjäder, 2014; Dunn, 2005). E esse é o caso da interseção entre as políticas de proteção de ICs, sob a égide do conceito de segurança nacional, e das políticas de avaliação do investimento externo, que têm ganhado mais adeptos desde 2016, como será apresentado na seção 3.

2.2 Brasil e suas políticas de proteção à IC

Na América do Sul, o Brasil foi o primeiro país a apresentar um programa de segurança da IC. Como argumenta Guterres (2016, p. 36), o tema já nasceu "crescido" no Brasil, ao resgatar indistintamente um histórico longo do debate sobre segurança, vulnerabilidades e resiliência, análise e gerenciamento de riscos e sua associação às ICs, tal como desenvolvido em outros países, em especial a partir dos Estados Unidos e dos países da União Europeia.[21]

Pode-se dizer que o tema das ICs conta com dois marcos principais na legislação brasileira: um primeiro momento, entre 2007 e 2008, associado aos grandes eventos internacionais em território nacional, como a Copa do Mundo, a Rio +20 e os Jogos Olímpicos; e um segundo momento, a partir de 2016, de rearticulação da temática, incluindo a questão digital. Em ambos os momentos, observa-se uma influência forte do movimento regulatório iniciado em outras partes do mundo, tal como apresentado anteriormente. Esses movimentos foram feitos diretamente a partir da Presidência da República e de seus órgãos de assessoramento, entre os quais destacam-se a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (Creden)[22] e o Gabinete de Segurança Institucional da Presidência da República (GSI/PR).[23]

Em 2007, a maior exposição global do Brasil, face aos grandes eventos internacionais, bem como as exigências de quantidade e qualidade na prestação e continuidade dos serviços (Santos, Carvalho e Cavalcante, 2011), favoreceram a proposição pela Creden ao presidente da República para a inclusão dos assuntos relacionados à segurança de ICs e da informação nas suas competências (Resolução Creden nº 2/2007) e para a criação de um Grupo Técnico de Segurança de Infraestruturas Críticas (GT/Siec). Esse GT seria responsável por propor medidas e ações de segurança para as ICs nos setores de energia, transporte, água e telecomunicações. Essa foi a primeira vez em que apareceram na regulação nacional a concepção de ICs e a exemplificação de setores em políticas associadas a ICs. Em 8 de fevereiro de 2008, o GSI lançou a portaria que criava o GT, definindo o conceito de

21. A Estratégia Nacional de Segurança de Infraestruturas Críticas, publicada em 2020, em anexo ao Decreto nº 10.569/2020 (introdução), reconhece explicitamente a influência dos parâmetros estabelecidos no exterior para o desenho da política nacional.

22. O Conselho de Governo foi estruturado pela Lei nº 8.028/1990 e posteriormente alterado até a sua atual estruturação conforme Lei nº 13.844/2019 (art. 13). Ao conselho compete assessorar o presidente da República, a partir de sua convocação, na formulação de diretrizes de ação governamental. A Creden é uma das câmaras na estrutura do Conselho de Governo e foi criada pelo Decreto nº 4.801/2003, com modificações em sua competência até sua atual regulamentação pelo Decreto nº 9.819/2019. Seu objetivo é abrangente, na medida em que lhe compete: i) formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do governo federal; ii) aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos, no âmbito de ações cujo escopo ultrapasse a competência de um único ministério; e iii) acompanhar questões e fatos relevantes, que apresentem potencial risco à estabilidade institucional. Desde 2019, com o Decreto nº 9.819, o chefe de gabinete do GSI/PR preside a Creden.

23. O GSI/PR é o órgão responsável por questões associadas a risco, segurança e inteligência do Estado, no assessoramento do presidente da República. Foi criado em 1999, pela Medida Provisória nº 1.911-10, passou por algumas reformulações institucionais e foi "recriado" como estrutura autônoma em 2018, com o Decreto nº 9.637/2018. Atualmente, encontra-se regulado pelos arts. 10 e 11 da Lei nº 13.844/2019.

ICs como "as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional" (art. 2º).[24] No contexto da crise financeira global de 2008, o GSI ainda incluiu o setor de finanças no rol de setores de ICs (Portaria GSI nº 2/2008).

Desde 2008, o GSI/PR exerce papel de relevância na pauta de segurança das ICs, a partir de sua posição de coordenador do debate de ICs junto à Creden.[25] Suas atividades incluem a articulação, em todos os níveis e esferas de poder e com o envolvimento dos setores público e privado, de processos de segurança preventiva dos recursos humanos, equipamentos, instalações, serviços, sistemas, informações e outros ativos que, de alguma forma, assegurem o funcionamento dos serviços indispensáveis ao Estado e à sociedade. Para concretizar tais ações, os GTs/Siec coordenados pelo GSI/PR conduzem reuniões mensais, com propostas de estudos específicos para os setores e de avaliação de riscos. Os GTs são compostos por representantes dos ministérios correspondentes às áreas prioritárias.

Em 2016, sob a gestão Temer, a política de segurança da infraestrutura nacional foi redesenhada, tanto em termos de conteúdo quanto em relação à sua organização institucional, passando a estar acoplada às políticas de inteligência e de segurança cibernética e concentrando-se no GSI/PR. Assim, o primeiro passo foi dado com a associação da proteção de ICs à Política Nacional de Inteligência, aprovada pelo Decreto nº 8.793/2016.[26] Em 2018, foram aprovadas a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) (Decreto nº 9.573/2018) e a Política Nacional de Segurança da Informação (Decreto nº 9.637/2018). Essa última indica, entre os seus objetivos, a segurança da informação das ICs (art. 4º, inciso VI, b do Decreto nº 9.637/2018). As políticas traçam os objetivos e diretrizes gerais que são detalhados e implementados a partir de estratégias nacionais e planos nacionais específicos,[27] conforme discriminado na figura 2. Também se observa na figura a inter-relação entre as políticas e suas estratégias e planos.

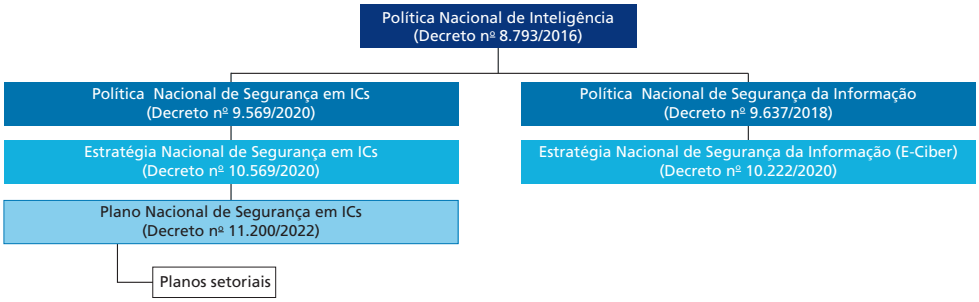
24. Disponível em: https://www.diariodasleis.com.br/legislacao/federal/198823-infra-estruturas-cruticas-gtsic-institui-grupos-tucnicos-de-seguranua-de-infra-estruturas-cruticas-gtsic-e-du-outras-providuncias.html.

25. Essa predefinição levou à incorporação das competências requeridas pela Creden no Decreto nº 6.371/08. O decreto de 2008 foi posteriormente consolidado no Decreto nº 9.819/2019, que dispõe sobre a Creden.

26. Neste decreto, as ameaças às ICs são indicadas como centrais para a Política Nacional de Inteligência. O item 8.9 da política indica que a "inteligência deve participar do processo de avaliação de riscos e vulnerabilidades relativos a alvos potenciais daquelas ameaças, visando a concorrer para a proteção das infraestruturas críticas nacionais".

27. A Política Nacional de Inteligência é a única que conta, até o momento, com uma estratégia aprovada (Decreto sem número, de 15 de dezembro de 2017) e um plano assinado em 3 de maio de 2018 e aprovado pela Portaria GSI/PR nº 40/2018. Disponíveis em: https://www.defesanet.com.br/inteligencia/noticia/29224/Plano-Nacional-de-Inteligencia-e-assinado/ e https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/Col3v5.pdf. Acesso em: 30 jun. 2022. O plano, contudo, é de acesso restrito dada a sua classificação como sigiloso por conter informações consideradas imprescindíveis à segurança da sociedade ou do Estado nos termos dos incisos I, II e IX do art. 25 do Decreto nº 7.724/2012.

FIGURA 2
Brasil: a regulamentação das ICs no contexto da Política Nacional de Inteligência



Elaboração dos autores.

A seguir, são apresentados alguns detalhes de cada uma dessas regulamentações, com destaque para como estão coordenadas e também para como ampliam o rol de ICs e das estratégias para sua proteção.

A PNSIC, mais especificamente, atualizou e alinhou a política nacional com o debate externo, apontando para conceitos como interdependência entre ICs e resiliência entre o tempo de interrupção e recuperação das atividades. Ela foi estruturada a partir de uma lógica de prevenção e precaução, com base em análise de riscos e na integração entre as diferentes esferas do poder público, do setor empresarial e dos demais segmentos da sociedade, conforme as orientações da OCDE (2019). O Decreto nº 9.573/18 também indicou como importante instrumento para a PNSIC a criação de um Sistema Integrado de Dados de Segurança de ICs.

Em 2020, na gestão Bolsonaro, foram articulados os passos para a definição das estratégias para a PNSIC e da Política Nacional de Segurança da Informação. A Estratégia Nacional de Segurança de Infraestruturas Críticas (Ensic) (Decreto nº 10.569/2020) reitera a ênfase em ações de prevenção e resiliência e na prestação dos serviços essenciais, com o intuito de continuidade da atividade, privilegiando a segurança física e operacional, por meio da análise de risco. A Ensic, a fim de promover a implementação das políticas em ICs e proporcionar elementos para a criação do plano nacional, estabelece quatro eixos estruturantes para sua implementação: i) a articulação institucional entre governo e diferentes agentes envolvidos; ii) a conscientização com a divulgação de informações e formação de uma cultura sobre a segurança das ICs, bem como a capacitação dos órgãos envolvidos; iii) a promoção e o apoio, inclusive financeiro, para ações coordenadas; e iv) a gestão de dados e informações, de forma acessível aos responsáveis pelas decisões estratégicas. Esses eixos definem iniciativas estratégicas que devem ser detalhadas no plano nacional, com a definição da execução das ações e do atingimento de metas. Além disso, a Ensic consolida a coordenação da PNSIC pelo GSI/PR e indica como setores prioritários para atuação comunicações, energia, transportes, finanças e águas.

Já a E-Ciber foi construída em módulos chamados de eixos temáticos transversais, para contemplar a segurança e a defesa cibernéticas, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados. Centralizada no GSI/PR, ao lado do Ministério da Defesa, a iniciativa foca a proteção da administração pública federal contra ataques e sabotagens no meio digital. No momento, a maior preocupação da estratégia nacional parece ser a segurança dos dados produzidos e compartilhados pelo governo federal, prevendo, inclusive, diretrizes para a utilização de aparelhos de informação, como celulares, por servidores públicos.

Não obstante, vale mencionar que a E-Ciber se mostra mais abrangente que a Ensic, inclusive na regulamentação da proteção de IC. Oficialmente, ela abrange os setores de telecomunicação, transportes, energia, água e financeiro, mas considera em "âmbito análogo" o setor de saúde e "a importância estratégica da indústria farmacêutica" (seção 1.3 do Decreto nº 10.222/20). Ademais, ela já passa a prever disposições mais concretas de proteção cibernética aos prestadores de serviço desses setores, a exemplo da atividade realizada pelo Banco Central do Brasil (BCB) para com as atividades bancárias (Brasil, 2020).

Seguindo a chave da necessidade de resiliência das ICs, a fim de possibilitar a contínua prestação de serviços essenciais, a E-Ciber aborda as atividades de informação como um ponto vulnerável para a segurança de ICs, na medida em que interligação das redes de informação e comunicação globais "tornam-se alvo de *malwares*, *hackers*, hacktivistas e de operações estatais adversas" e, pela interconectividade global, como "um risco para outras nações" (parte I, diagnóstico).[28] A E-Ciber eleva a proteção cibernética das ICs a uma condição central para segurança nacional e elenca como principais tipos de ameaças dessa classificação: ataques de *phishing*, negação de serviço em larga escala, vazamentos de informações privadas ou institucionais, espionagem cibernética e interrupção de serviços.

É importante mencionar que, em 2008, a Portaria GSI/PR nº 2/08 já havia criado GTs para a concretização das políticas de proteção às ICs, elegendo como áreas prioritárias energia, transporte, água, telecomunicações e finanças. Em nova edição da portaria pelo GSI, em 2018 (Portaria GSI/PR nº 53/18), os temas biossegurança e bioproteção foram incluídos. As atividades dos GTs seriam manter em contínuo acompanhamento a classificação de ICs, identificando possíveis ameaças e vulnerabilidades e propondo medidas de controle para a redução dos riscos. Apesar de, em 2019, os GTs referentes a ICs terem sido destituídos (Portaria GSI/PR nº 73/19), em fevereiro de 2022 eles foram reestabelecidos (Resolução GSI/PR nº 14/22). Os novos GTs foram criados para os setores de abastecimento urbano de águas, barragens, telecomunicações, radiodifusão, serviços postais, energia elétrica, petróleo, gás natural e biocombustíveis, finanças, transportes aéreos, transportes aquaviários, transportes terrestres (especificamente no modal ferroviário), biossegurança e bioproteção.

Em setembro de 2022, foi aprovado o Plano Nacional de Segurança de Infraestruturas Críticas (Plansic) (Decreto nº 11.200/2022), para os setores já definidos anteriormente no decreto de 2020 da Ensic e pela Resolução GSI/PR nº 14/2022. O Plansic tem como objetivo principal a implementação, no prazo de quatro anos, de um sistema com metodologias de identificação das ICs, de compartilhamento de informações e fornecimento de dados sobre alertas de riscos em estrutura de cooperação entre os setores público e privado. O Plansic referencia a lógica de análise de risco e de interdependência das ICs,[29] absorvendo a experiência externa de outros países e reiterada pela OCDE.[30] Basicamente, estão responsáveis pela implementação do Plansic: i) o GSI/PR, para coordenar seus principais elementos e a interação com outros agentes; ii) os ministérios responsáveis pelas áreas prioritárias, conforme detalhado no quadro 1; ii) a Agência Brasileira de Inteligência (Abin), para monitorar ações contra ICs; e, complementarmente, iv) demais órgãos e entidades do setor público federal.

28. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

29. A Resolução GSI/PR nº 14/2022 define a interdependência de ICs como "a relação de dependência ou interferência de uma IC em outra ou de uma área prioritária de infraestruturas críticas em outra" (art. 2º, § 2º).

30. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2022/setembro/decreto-aprova-o-plano-nacional-de-seguranca-de-infraestruturas-criticas. Acesso em: 28 mar. 2023.

QUADRO 1
Distribuição das responsabilidades para a elaboração dos planos setoriais de segurança de ICs

Área prioritária	Setor	Ministério responsável
Águas	Barragens	Ministério do Desenvolvimento Regional
	Abastecimento urbano de águas	
Energia	Energia elétrica	Ministério de Minas e Energia
	Petróleo, gás natural e biocombustíveis	
Transporte	Terrestre	Ministério da Infraestrutura
	Aéreo	
	Aquaviário	
Comunicações	Telecomunicações	Ministério das Comunicações
	Radiodifusão	
	Serviços postais	
Finanças	Finanças	Ministério da Economia
Biossegurança e bioproteção	Biossegurança e bioproteção	Ministério da Saúde
Defesa	Defesa	Ministério da Defesa

Fonte: Decreto nº 11.200, de 15 de setembro de 2022. Disponível em: https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2022/Decreto/D11200.htm#:~:text=DECRETO%20N%C2%BA%2011.200%2C%20DE%2015,de%20Seguran%C3%A7a%20de%20Infraestruturas%20Cr%C3%ADticas.

A organização institucional prevista pelo Plansic é a de que os ministérios envolvidos comuniquem o GSI/PR, via ofício, quais serão as secretarias ou departamentos responsáveis pela elaboração de planos setoriais-específicos a serem entregues no prazo de seis meses (item 9 do Plansic). As autoridades comporão um Comitê Gestor de Segurança de Infraestruturas Críticas a ser liderado pelo GSI/PR.

Como se pode observar, a concentração das estratégias de proteção às ICs em um órgão, a promoção de intercâmbio de informações entre as autoridades técnicas responsáveis pelo controle dos setores considerados críticos e a adoção da técnica de regulação de riscos endossados pela legislação brasileira são condizentes com aquelas boas práticas de risco e resiliência das ICs anunciadas pela OCDE (OECD, 2019). O quadro A.2, no apêndice A, apresenta um resumo das agências envolvidas nas legislações brasileiras relacionadas com IC.

Após a descrição desses marcos temporais e alguns dos principais elementos das políticas voltadas para ICs no Brasil, pode-se observar que o país tem procurado sistematizar e organizar não apenas conceitualmente, mas sobretudo organizacionalmente, essas políticas. Também é notável como a temática tem sido influenciada pela prática internacional, incluindo a sua inter-relação com as políticas cibernéticas, ainda que com adaptações à realidade brasileira. Isso fica mais claro na definição do Plansic das preocupações com barragens, serviços postais e biopirataria e bioproteção, que são ICs com destaque especial no contexto brasileiro – quando se contrastam com os setores eleitos por outros países, conforme o quadro A.1 do apêndice A. Passa-se, então, a entender como as políticas de proteção a ICs têm se entrelaçado com as políticas de avaliação de investimentos externos, considerando as particularidades do Brasil nesta outra forma de regulação pública.

3 A RELAÇÃO ENTRE IC E INVESTIMENTO EXTERNO

3.1 A IC sob o foco dos IAIEs em diferentes países

O debate sobre ICs despontou como uma questão sobre segurança nacional, mas, em um primeiro momento, dissociado da lógica do inimigo externo. Os riscos eram relacionados ao perfil da atividade e ao tipo de dependência econômica, tecnológica e até mesmo psicológica dessas infraestruturas. Sua associação com as relações econômicas transfronteiriças e agentes externos passou a ser estabelecida nas últimas décadas, ampliando a ligação de segurança de ICs com a agenda externa dos Estados. Nesta seção, são apresentadas as aplicações e as associações do conceito de ICs ao da avaliação dos investimentos externos– por meio dos IAIEs – em alguns países.

Em um trabalho anterior, Sanchez-Badin *et al*. (2022) analisaram o funcionamento de quinze IAIEs, selecionados a partir de alguns critérios que propiciaram a manutenção de certa diversidade de países,[31] inclusive quanto ao grau de restrição ao capital externo. Das quinze jurisdições analisadas,[32] nem todas estabeleceram uma relação específica das suas políticas de ICs com seus IAIEs. Vale notar que, ainda que os países possam definir setores prioritários, nem sempre essa relação passa pela linguagem de IC. O apêndice A apresenta um quadro resumindo a definição de IC utilizada em alguns países, com os respectivos setores incluídos em tal definição (quadro A.3). A seguir, são apresentadas as classificações aplicadas quanto à forma como as legislações tratam os setores eleitos para algum tipo de controle em relação ao investimento externo.

A situação mais extrema de controle é a proibição do investimento externo no setor. Essa forma de discriminação direta e absoluta dos investimentos externos pode ser apresentada de diferentes formas nas legislações nacionais e internacionais. Pode-se ter a excepcionalização do setor por uma restrição constitucional ou em lei infraconstitucional e isso ser informado como parte da legislação interna. O caso mais notório atualmente é o da China, que publica uma lista negativa de setores em que investimentos externos não são admitidos.[33] Os países-membros da OCDE, juntamente com outros voluntários, ao assinarem a Declaration on International Investment and Multinational Enterprises, a fim de evitar o tratamento discriminatório entre investidores nacionais e estrangeiros, também se comprometeram com a transparência de declarar os setores em que mantêm limitações ao investidor externo.[34]

31. Os critérios utilizados em Sanchez-Badin *et al*. (2022) são: i) países com sistemas muito estruturados e utilizados (por exemplo, Estados Unidos e Austrália); ii) países emergentes (por exemplo, México e África do Sul); iii) países com cultura jurídica próxima à do Brasil (por exemplo, Portugal); e iv) particularidade regional (por exemplo, União Europeia).

32. O último levantamento da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (United Nations Conference on Trade and Development – UNCTAD) identificou 28 jurisdições que possuem IAIEs. São elas: África do Sul, Alemanha, Austrália, Áustria, Bélgica, Canadá, China, Coreia do Sul, Dinamarca, Espanha, Estados Unidos, Finlândia, França, Hungria, Índia, Islândia, Itália, Japão, Letônia, Lituânia, México, Nova Zelândia, Noruega, Polônia, Portugal, Reino Unido, Romênia e Rússia. Além desses 28 países, também foi estabelecido pela União Europeia um mecanismo de cooperação para a triagem do investimento estrangeiro (UNCTAD, 2019, p. 3). Em Sanchez-Badin *et al*. (2022), quinze desses mecanismos foram analisados em mais detalhes quanto a suas estruturas institucionais e procedimentos: África do Sul, Alemanha, Austrália, Canadá, China, Coreia do Sul, Espanha, Estados Unidos, Índia, Japão, México, Portugal, Reino Unido, Rússia e União Europeia.

33. A lista mais atual data de 2022 e é nomeada Negative List for Market Access (2022 Edition). Disponível em: https://fdi.mofcom.gov.cn/EN/come-newzonghe.html?parentId=125&name=The%20Legal%20System%20for%20Foreign%20Investment&comeID=3. Acesso em: 28 mar. 2023.

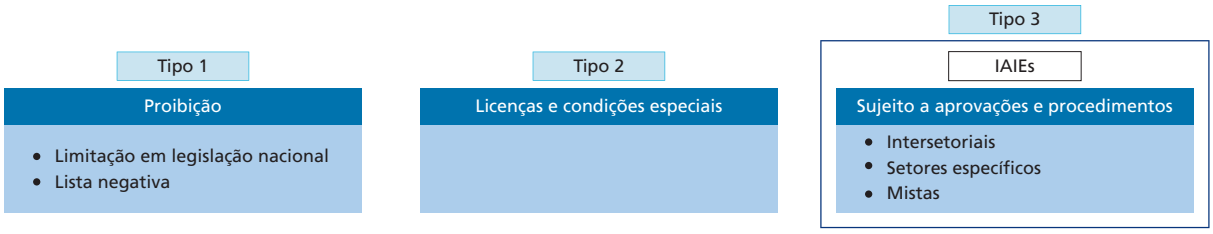
34. São signatários da declaração os 38 atuais membros da OCDE e outros doze países não membros, incluindo o Brasil, que é signatário desde 1997. Disponível em: https://www.oecd.org/daf/inv/investment-policy/nationaltreatmentinstrument.htm. Acesso em: 28 mar. 2023.

Também são consideradas formas de discriminação aquelas que exigem licenças especiais para estrangeiros ou mesmo procedimentos específicos em caso de investimento em determinados setores. Essas formas de discriminação são discutidas em maiores detalhes, no caso do Brasil, na subseção 3.2.

Por fim, tem-se mais recentemente o desenvolvimento dos IAIEs que fazem uma avaliação sobre o impacto do investimento externo. Como a implementação desses mecanismos é relativamente recente e a forma de seu funcionamento tem sido ampliada nos últimos anos, não há ainda uma avaliação ampla sobre o impacto dos mecanismos na discriminação de investimentos em termos globais (Sanchez-Badin *et al.*, 2022).

A figura 3 pontua essas diferentes formas de controle e discriminação dos investimentos externos, com o objetivo de localizar com mais clareza o espaço de atuação dos IAIEs em relação a práticas que foram mais disseminadas no controle do investimento externo no passado.

FIGURA 3
Formas de controle e discriminação do investimento externo



Fonte: OECD (2008, p. 7) e Danzman e Meunier (2022, p. 7-8).
Elaboração dos autores.

Para fins de análise, esta subseção foca no tipo 3, que recai exclusivamente sobre os casos em que há a atuação do IAIE. Observam-se, pelo menos, três interseções entre as políticas de implementação dos IAIEs e as de IC descritas na seção 2: i) o recurso ao fundamento de proteção da segurança nacional; ii) a identificação de setores relevantes para acompanhamento mais próximo pelas autoridades públicas; e iii) a aplicação dos conceitos de risco e resiliência. Contudo, não há necessariamente uma identificação completa entre essas duas políticas, até mesmo porque o conceito e os critérios de avaliação de IC recaem da mesma forma sobre o investimento nacional. Também não há uma relação direta, pois nem sempre que há uma referência para atuação de um IAIE se trata de setores considerados como IC. A seguir, demonstra-se como diferentes jurisdições têm invocado a competência de seus IAIEs para análises setoriais, com ou sem o recurso ao conceito de IC. Esse exercício é relevante para se pensar sobre a criação de um IAIE no Brasil (Sanchez-Badin, Morais e Bonini, 2021) e sobre como a relação entre políticas setoriais e de IC devem ser desenhadas.

Ainda entre as considerações preliminares, vale apresentar uma forma de categorização da atuação dos IAIEs quanto ao desenho de suas competências. Danzman e Meunier (2022, p. 7-8), que elaboraram a base mais extensiva de mapeamento de IAIEs – a Politics and Regulation of Investment Screening Mechanisms (Prism), com foco nos países da OCDE –, propõem qualificar as competências em três modalidades: intersetoriais, setoriais e mistas (conforme pontuado no tipo 3 da figura 3). Como as próprias autoras observam, além de a criação e a intensificação da atuação desses IAIEs serem recentes, tem havido reformas constantes no âmbito de sua atuação face o aumento da competição e das tensões geoeconômicas internacionais (Danzman e Meunier, 2022).

Considerando a classificação de Danzman e Meunier (2022), entre as quinze jurisdições estudadas em Sanchez-Badin *et al.* (2022), apenas Portugal tem um IAIE com competência exclusivamente intersetorial, ou seja, os critérios para definir a avaliação de um investimento externo não estão atrelados a setores específicos.[35] Austrália e Estados Unidos também definiam a atuação de seus IAIEs com enfoque intersetorial até recentemente (2017 e 2020, respectivamente), mas, nos últimos anos, passaram a listar setores de alta tecnologia,[36] tendo então uma competência mista.

Em movimento diferente, também se tem o caso de países como Alemanha e Reino Unido, que definiam a competência de seus IAIEs com base em uma lista de setores previamente indicada e que incluíram a competência intersetorial mais recentemente, ampliando suas bases de atuação. África do Sul, Coreia do Sul, Japão e México, em contrapartida, mantêm a competência de seus IAIEs como exclusivamente setorial.[37] Não é possível identificar uma tendência no perfil da competência dos IAIEs – o que é mais nítido é que os países adaptam essas competências conforme suas necessidades e opções geoeconômicas. O que se observa da base Prism[38] é que, nos países que têm competência setorial ou mista, mais de uma autoridade é envolvida no processo de avaliação, ainda que uma delas lidere o processo.[39]

A seguir, descreve-se como algumas jurisdições coordenam a eleição dos setores envolvidos nas listagens com a concepção de IC, para a atuação de seus IAIEs. São, ainda, apresentados alguns casos exemplificativos dessa fundamentação de ICs para a avaliação dos investimentos externos.

Observa-se que África do Sul, China, Coreia do Sul e Japão qualificam a atuação de seus IAIEs para alguns setores, sem associá-los ao conceito de IC. Esses países até fazem referências genéricas a setores associados à definição de IC, mas sem uma relação ou experiência concreta que evidencie que essa relação possa ser estabelecida.[40]

35. Nota-se que Portugal, enquanto membro da União Europeia, está sujeito à Diretiva do Conselho nº 2008/114/EC sobre a política regional de ICs e ao Regulamento (EU) nº 2019/452 do Parlamento e do Conselho Europeu que regula o IAIE regional. Este último define que os Estados-membros da União Europeia e a comissão devem considerar os efeitos dos investimentos externos à região em ICs, tecnologias e suprimentos essenciais para a segurança e a manutenção da ordem regional, fazendo referência específica aos termos e políticas da regulamentação regional sobre ICs (art. 4.1 do Regulamento – EU – nº 2019/452). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452. Acesso em: 28 mar. 2023.

36. A este respeito, consultar a Executive Order do presidente Biden, nos Estados Unidos, para elencar setores específicos, de 15 de setembro de 2022. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/. Acesso em: 28 mar. 2023. Danzman e Meunier (2022) também qualificam esses novos setores listados como Critical Technologies and Dual Use, Next Gen Critical Infrastructure, em contraponto com o que nomeiam de Physical/Conventional Critical Infrastructure. Uma perspectiva temporal da inclusão desses diferentes setores está disponível em: https://investmentscreening.princeton.edu/data-visualizations/sectors-covered-over-time-country. Acessos em: 28 mar. 2023.

37. Os dados estilizados da base Prism pontuam essas características. Disponível em: https://investmentscreening.princeton.edu/data-visualizations/types-investment-screening-measures. Acesso em: 28 mar. 2023.

38. Neste caso, acessamos a base completa que alimenta os dados estilizados do *site*. Disponível em: https://investmentscreening.princeton.edu/. Acesso em: 31 jan. 2023. Agradecemos a Sarah Danzman, Sophie Meunier e à equipe por compartilharem a base completa, em janeiro de 2023.

39. Por exemplo, de acordo com a base Prism, nas reformas recentes na Austrália que levam a análises setoriais, de duas a três autoridades podem ser envolvidas. No caso do Canadá, são cinco autoridades em geral. E as recentes reformas nos Estados Unidos levaram ao envolvimento de até duas autoridades.

40. Esclarece-se que, por haver uma identificação dos setores comumente associados a IC, ainda que não haja uma associação direta à sua política de IC, na base Prism, por exemplo, há a inclusão de ICs como setores dentro do escopo das autoridades de IAIE. Disponível em: https://investmentscreening.princeton.edu/data-visualizations/sectors-covered-over-time-country. Acesso em 28 mar. 2023. Essas relações automáticas acabam promovendo ruídos sobre a relação entre as políticas de IC e dos IAIEs.

Na África do Sul, o Competition Amendment Act 18, ao introduzir a triagem de investimento externo no país, previu uma lista de interesses de segurança nacional que inclui investimentos com o uso ou transferência de tecnologia sensível, segurança de infraestrutura e fornecimento de bens ou serviços essenciais (Korsten *et al*., 2021, p. 218).[41]

De forma similar, na Coreia do Sul, a Lei de Promoção de Investimento Externo (Foreign Investment Promotion Act),[42] apesar de não fazer menção direta à IC, prevê o processo de avaliação do investimento externo, especificamente, para os setores militares, produtos agrícolas essenciais, energia, infraestrutura, transportes, tecnologias-chave e fabricação de equipamentos que envolvam a segurança nacional. Além disso, o controle societário de empresas de informação e mídia e de tecnologia da informação é limitado ao investimento externo. Tais disposições evidenciam a preocupação não só com setores críticos para o funcionamento do país, como também com a segurança de dados. Embora não se tenha informação pública sobre a aplicação dessas restrições a transações específicas, o levantamento da base de dados Prism indica setores coincidentes com os de ICs entre 2007 e 2022.[43]

Na China, por sua vez, há um conjunto regulatório fragmentado que especifica setores relevantes para o escrutínio do seu IAIE e, ainda, tratativas internacionais que podem ser associadas ao conceito específico de ICs. Partindo da regulação básica, sabe-se que o IAIE chinês prioriza a análise de setores considerados importantes para a soberania nacional e para a independência estratégica, tais como certos produtos agrícolas, energia e recursos naturais, equipamentos críticos, infraestrutura importante, transporte, serviços culturais, tecnologia e internet e serviços financeiros (Blacklock, 2022). Quanto aos setores cibernéticos, em setembro de 2021, entrou em vigor a Lei de Segurança de Dados,[44] que estabeleceu que, se operações de investimento externo implicarem a transferência de "dados importantes" para o exterior, estarão sujeitas à avaliação da Administração do Ciberespaço da China – que é uma autoridade distinta da responsável pelo IAIE na China e também da responsável por IC (quadro A.4, no apêndice A). No caso da China, também é interessante notar que o Comprehensive Agreement on Investment (CAI), assinado entre China e União Europeia, em dezembro de 2020, já designa como exceções de segurança para liberalização do investimento setores que envolvam o acesso a informações cuja divulgação possa ser contrária aos interesses de segurança e para proteger infraestruturas públicas críticas, como comunicações, energia e água.[45]

Finalmente, no Japão, a Lei de Câmbio e Comércio Exterior (Foreign Exchange and Foreign Trade Act) exige notificação prévia para investimentos relacionados à segurança nacional (armas, aviões, energia nuclear, desenvolvimento espacial); à infraestrutura pública (eletricidade, gás, água, telecomunicações, ferrovias); à segurança pública (vacinas, segurança privada); e à proteção da

41. A parte da legislação sul-africana relativa ao IAIE (art. 14) ainda não havia entrado em vigor até dezembro de 2022, mas logo que entre em operação é esperada a publicação de uma lista dos setores que estão associados às questões de segurança nacional (Korsten *et al*., 2021, p. 220). Atualizações sobre o processo de vigência da legislação estão disponíveis em: https://www.gov.za/documents/competition-amendment-act-18-2018-englishafrikaans-14-feb-2019-0000. Acesso em: 15 dez. 2022.

42. Disponível em: https://legal.un.org/avl/pdf/ls/Shin_RelDocs.pdf. Acesso em 10 jan. 2022. Mais informações a respeito em Jeon e Jung (2016) e Jang e Kim (2021).

43. Consultar, a respeito, Prism Dataset, na seleção sobre os setores cobertos por país, em seus IAIEs. Disponível em: https://investmentscreening.princeton.edu/data-visualizations/sectors-covered-over-time-country. Acesso em: 15 dez. 2022.

44. Disponível em: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml. Acesso em 28 mar. 2023.

45. V. Seção VI, art. 10 – Security exceptions. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2541. Acesso em: 8 dez. 2023.

indústria doméstica (agricultura).[46] Um caso observado envolvendo o controle de investimento externo em um setor que pode ser interpretado como de IC no Japão ocorreu em 2008, quando o fundo inglês The Children's Investment Master Fund (TCI Fund) tentou aumentar sua participação de 9,9% para 20% nas ações da J-Power, uma fornecedora de eletricidade do Japão. O Ministério das Finanças não permitiu que o TCI Fund adquirisse mais de 10% das ações da J-Power, alegando que a aquisição ameaçava a ordem pública. Na recomendação, o governo forneceu algumas razões para essa ameaça: a J-Power desempenha um papel importante no fornecimento de eletricidade e na política nuclear do país. Logo, se o TCI Fund adquirisse 20% das ações, isso teria efeito sobre a gestão da J-Power, o que poderia ameaçar o fornecimento de eletricidade acessível, bem como a implementação da política nuclear do Japão pela J-Power (Takahashi e Kawamura, 2020).

Além desses exemplos de regulamentação setorial pontual, há um grupo de países que iniciaram discussões sobre preocupações quanto à IC há mais tempo e associam suas políticas específicas para a IC a seus IAIEs. São destacados aqui os casos da Alemanha, da Austrália, do Canadá e dos Estados Unidos.

Na Alemanha, a avaliação de todo investimento externo à União Europeia ocorre em três áreas diferentes: i) setor A: setor militar e de informações classificadas de Estado; ii) setor B: setor de IC;[47] e iii) setor C: outras entidades potencialmente críticas.[48] O destaque ao setor de IC está associado ao número crescente de aquisições estrangeiras de empresas alemãs que operam essas ICs (Cotta, Li e Wistinghausen, 2021). As transações em IC e indústrias críticas são, então, condicionadas à liberação pelo Ministério Federal da Economia e Energia (BMWi). Se não forem previamente autorizadas, podem ser processadas como atos criminosos.

Há dois casos interessantes que passaram pelo IAIE alemão evidenciando a importância do conceito de IC para o país. O primeiro foi em 2018, quando o grupo Yantai Taihai Corporation, da China, notificou a intenção de adquirir a alemã Leifeld Metal Spinning, que fabrica materiais usados nas indústrias automotiva, aeroespacial e nuclear. O governo alemão anunciou, à época, que exerceria seu direito de bloquear o negócio devido a preocupações para proteger a IC do país (Hilf, Röhling e Braun 2018).[49] No mesmo ano, a empresa estatal chinesa State Grid fez uma oferta para adquirir uma participação equivalente a 20% da empresa alemã 50Hertz, uma *joint venture* que detém parte relevante da rede elétrica alemã. Apesar de a lei de investimento externo na época estabelecer

46. Os ministérios devem analisar os relatórios no prazo de trinta dias, inclusive ouvindo opiniões do Conselho de Alfândega, Tarifas, Câmbio e outras transações.

47. Consideram-se os seguintes setores: energia, água, alimentação, telecomunicações, saúde, setor financeiro e de seguros, transporte e trânsito, *softwares* para operação de infraestruturas críticas, encarregados de medidas de vigilância, serviços de computação em nuvem e empresas de mídia que participam da formação de opinião pública. Seguindo a tendência internacional, no final de 2018, o governo alemão expandiu o escopo de seu IAIE, e a definição de IC foi ampliada para abranger as empresas de notícias e mídia para a "formação da opinião pública" Disponível em: https://www.bafa.de/SharedDocs/Kurzmeldungen/EN/Foreign_Trade/Newsletter_Export_Control/2018_02_newsletter_export_control.html. Em 2020 e 2021, novas revisões ampliaram as ICs, incluindo comunicação estatal, farmacêutica e equipamentos de proteção individual. Ainda em 2021, foi adotada uma segunda alteração para incluir *software* e serviços de tecnologia da informação. Essa emenda fornece a classificação de IC em todos os sete setores (energia, tecnologia da informação e telecomunicações, água, alimentos, transporte, saúde e finanças e seguros) e esclarece os limites a se atingirem para que a infraestrutura seja considerada crítica. Disponível em: https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s4163.pdf%27%5D__1637167988789. Acesso em: 28 mar. 2023.

48. Foreign Trade and Payments Act (AWG) e Foreign Trade and Payments Ordinance (AWV). Disponíveis em: https://www.gesetze-im-internet.de/englisch_awg/englisch_awg.html e https://www.gesetze-im-internet.de/englisch_awv/. Acesso em mar. 2023.

49. Em agosto de 2018, a Yantai Taihai retirou sua notificação de investimento. Mais detalhes sobre o caso são apresentados em Sanchez-Badin *et al*. (2021).

a base para aquisições acima de 25% do capital, os reguladores alemães alegaram a necessidade de intervenção por questões de segurança, associadas a riscos relacionados à IC do país.[50]

A Austrália, por sua vez, conta com a Lei de Segurança de IC (Security of Critical Infrastructure Act – Lei Soci), de 2018, que criou uma estrutura para o gerenciamento de IC, estabelecendo um registro de ativos de IC e coletando informações sobre a operação, por meio de obrigações de relatórios pelos detentores de tais ativos.[51] O Conselho de Revisão de Investimento Estrangeiro (Foreign Investment Review Board – Firb), responsável pelo IAIE australiano, deve sempre consultar o Centro de IC como parte de seus procedimentos (Korsten *et al*., 2021). Em dezembro de 2021, a Lei de Emenda à Legislação de Segurança de IC (Security Legislation Amendment (Critical Infrastructure Act) – Lei Slaci) entrou em vigor, expandindo os tipos de ativos de IC contidos na Lei Soci e ampliando o significado do termo negócios de segurança nacional. Foram adicionados à lista de ativos de IC: telecomunicações, transmissões, armazenamento de dados, setor bancário, previdência, seguro, infraestrutura do mercado financeiro, operador de energia, combustível, hospitais, educação, comida, carga, frete, transporte público, aviação e defesa.[52] Em 2022, entrou em vigor a segunda parte das alterações à Lei Soci, introduzidas pela Lei Slaci, agora introduzindo obrigações aprimoradas no setor de segurança cibernética para ativos críticos.[53]

Apesar de essa relação de questões cibernéticas ser recente na legislação do IAIE na Austrália, houve um caso em 2012 em que foi realizado o bloqueio de investimentos da Huawei devido a preocupações com a segurança cibernética. Essas preocupações surgiram pelo fato de a Huawei ter sido fundada por um ex-oficial do Exército de Libertação do Povo da China, o que alimentou a alegação de que teria uma relação com o governo chinês.[54]

O Canadá é outro país que faz referência nominal a ICs nos processos de seu sistema de IAIE. Em sua Guidelines on the National Security Review of Investments, publicada em 2021, faz referência à atuação de seu IAIE, que considera, entre outros, os efeitos do investimento nos interesses de defesa e atividades de inteligência, na transferência de tecnologia sensível, na segurança da IC e no fornecimento de serviços essenciais (Korsten *et al*., 2021, p. 32).[55] Todavia, não foram localizadas informações sobre casos nesses setores em que tenha sido acionado o IAIE canadense.[56]

Finalmente, nos Estados Unidos, tem-se que o Comitê de Investimentos Externos nos Estados Unidos (Committee on Foreign Investment in the United States – CFIUS), criado nos anos 1970, é responsável por avaliar se os investimentos estrangeiros apresentam riscos para a segurança

50. Essa preocupação apareceu mais fortemente após o aumento repentino e recorde, em 2017, de aquisições de empresas alemãs por empresas chinesas. Ilustrativamente, tem-se o dado de que empresas chinesas investiram em torno de US$ 16,8 bilhões na compra de participações ou da totalidade das ações de 54 empresas alemãs. Disponível em: https://www.dw.com/en/chinas-sgcc-to-buy-stake-in-german-grid-operator-50hertz/a-42522944. Acesso em 28 mar. 2023. No caso da 50Hertz, o governo alemão se propôs a investir, a partir do banco estatal KfW, na empresa para impedir que o investimento fosse feito pela empresa chinesa State Grid (DW, 2018b). Essa mobilização do governo alemão foi inédita (Marray, 2018; Pohl e Rosselot, 2020) e serviu para impedir o investimento sem a necessidade de vetar explicitamente a transação pelo procedimento do IAIE (Sanchez-Badin *et al*., 2021).

51. Disponível em: https://www.legislation.gov.au/Details/C2018A00029. Acesso em: 28 mar. 2023.

52. Disponível em: https://www.legislation.gov.au/Details/C2021A00124. Acesso em: 28 mar. 2023.

53. Disponível em: https://www.legislation.gov.au/Details/C2022A00033. Acesso em: 28 mar. 2023.

54. Disponível em: https://www.reuters.com/article/us-australia-huawei-nbn-idUSBRE82P0GA20120326/. Acesso em: 8 dez. 2023.

55. Disponível em: https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html. Acesso em: 28 mar. 2023.

56. A base de pesquisa foi a página oficial do Canadá e os relatórios anuais publicados. Disponível em: https://ised-isde.canada.ca/site/investment-canada-act/en. Acesso em: 28 mar. 2023.

nacional. Em 2018, em resposta à crescente preocupação com o investimento chinês, em particular em tecnologias consideradas críticas, entrou em vigor a Lei de Modernização de Revisão de Risco de Investimento Estrangeiro (The Foreign Investment Risk Review Modernization Act of 2018 – Firrma), que expandiu a autoridade do CFIUS para a revisão de investimentos externos e *joint ventures* em IC, tecnologia crítica ou dados pessoais confidenciais de cidadãos norte-americanos e transações envolvendo propriedades nas proximidades de certos aeroportos, portos marítimos e instalações militares (Lichtenbaum e Ribner, 2021, p. 8-9).[57] Além da regulamentação específica para investimentos externos, os Estados Unidos contam também com o Plano Nacional de Proteção de Infraestrutura: Parceria para Segurança e Resiliência de Infraestrutura Crítica, de 2013, que regulamenta e esclarece o conteúdo das infraestruturas críticas, incluindo sistemas e ativos, físicos ou virtuais, tão essenciais que a incapacidade ou destruição de tais sistemas teria um impacto desestruturante na segurança nacional, na estabilidade econômica nacional, na saúde pública ou na combinação desses assuntos, no território dos Estados Unidos (OECD, 2019, p. 65).

O escopo das questões que se enquadram na categoria de segurança nacional nos Estados Unidos se ampliou nos últimos anos, passando a incluir elementos de IC. Setores específicos que são foco principal do CFIUS incluem telecomunicações, serviços financeiros, água, transporte, alimentação e agricultura, saúde e serviços de infraestrutura cibernética e física essenciais para manter a defesa, a continuidade do governo, a prosperidade econômica e a qualidade de vida nos Estados Unidos (West, Luther e Wilcox, 2020). Ainda em fevereiro de 2022, o CFIUS atualizou sua lista de tecnologias críticas que podem se tornar relevantes para a segurança nacional dos Estados Unidos em um futuro próximo.[58]

Um caso envolvendo estrutura crítica nos Estados Unidos se deu 2017, quando a Dragon Gem Limited e a Absolute Frontier Limited, ambas investidoras de Hong Kong, tentaram realizar um investimento na PEDEVCO Corp., uma empresa de energia de capital aberto responsável pelo desenvolvimento de projetos estratégicos de energia de alto desempenho nos Estados Unidos (Sanchez-Badin *et al*., 2021).[59] As partes notificaram a operação ao CFIUS, mas o órgão não respondeu no prazo regular de trinta dias, e a transação foi cancelada.

Também em 2017, a PatientsLikeMe Inc., uma *startup* de saúde digital de Massachusetts, recebeu um investimento de aproximadamente US$ 100 milhões da iCarbonX, uma *startup* de saúde digital supostamente apoiada pela gigante chinesa Tencent (West, Luther e Wilcox, 2020). O PatientsLikeMe não apresentou uma revisão voluntária porque, na época, o CFIUS não havia demonstrado interesse público em transações desse porte ou no setor de saúde. Mas o negócio chamou a atenção do comitê, que tem reprimido agressivamente os investimentos chineses em empresas norte-americanas, especialmente quando a segurança nacional e os segredos comerciais estão em risco (Farr e Levy, 2019). O governo Trump forçou uma alienação após uma revisão do CFIUS, um sinal de que o CFIUS começou a expandir sua atuação além de grandes negócios que envolvem IC, movendo-se para áreas de dados do consumidor, na chave da IC cibernética.

57. De acordo com Korsten *et al*. (2021, p. 249-256), a Firrma foi impulsionada por preocupações sobre os investimentos chineses em tecnologia dos Estados Unidos e por preocupações sobre o acesso de estrangeiros a informações de identificação pessoal de seus cidadãos. A legislação, contudo, não indica o tratamento discriminatório pela origem do investimento.

58. The White House, Critical and Emerging Technologies List Update, 2022. Disponível em https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf. Acesso: 15 dez. 2022.

59. O contrato teria resultado em um investimento de US$ 12 milhões, em troca de aproximadamente 53,86% do capital da PEDEVCO. Disponível em: https://www.tradepractitioner.com/2017/10/cfius-filing-withdrawn-and-abandoned-dragon-gem-limitedabsolute-frontier-limited-and-pedevco-corp/. Acesso em: 8 dez. 2023.

Outro caso envolvendo segurança cibernética nos Estados Unidos ocorreu em 2018, em que a Pamplona Capital Management comprou uma participação minoritária na Cofense Inc., uma empresa de segurança cibernética norte-americana que atende grandes corporações. As empresas não buscaram a aprovação do CFIUS porque o sistema de revisão era voluntário. Porém, em 2019, o CFIUS exigiu que a Pamplona Capital Management vendesse sua participação minoritária (47%) na Cofense Inc., por questões de segurança nacional (West, Luther e Wilcox, 2020). A pressão para desinvestir ocorreu no momento em que Washington aumentava o escrutínio sobre a participação de investidores estrangeiros em empresas de tecnologia dos Estados Unidos.

A apresentação, nesta seção, de informações sobre a crescente regulação de IAIEs e o aumento de suas competências indica que a relação de IAIEs com a política oficial de ICs varia. Há, contudo, uma simplificação na literatura que traz essa associação mesmo quando os países apenas listam setores relevantes na sua economia para análise. E, há, também, situações como as da Alemanha, da Austrália, do Canadá e dos Estados Unidos, em que tal relação entre as políticas é articulada, promovendo a apropriação na avaliação de investimentos externos dos setores englobados em IC, incluindo a parte cibernética, a linguagem operacional para o controle de ICs e até mesmo, em alguns casos, a mobilização de autoridades específicas envolvidas com a política de IC. Porém, também é verdade que, mesmo nos países em que é feita essa associação, ela não é completa. Há uma autonomia resguardada para as políticas de ICs em relação àquelas para avaliação dos investimentos externos.

3.2 O Brasil e o investimento externo em setores de IC

A partir da delimitação de IC na legislação brasileira, a proposta desta subseção é analisar algumas particularidades da regulação dos setores considerados como tal no Brasil e identificar alguns órgãos ou agências responsáveis pela supervisão das políticas públicas implementadas nesses setores, conforme o arcabouço regulatório desenhado para a atividade.

Muitos setores indicados como parte das ICs brasileiras são considerados "serviços públicos", com a consequência de estarem sujeitos ao regime especial dessas atividades, conforme texto constitucional. De acordo com a legislação nacional, particulares que prestam serviços públicos, independentemente de sua nacionalidade, estão sujeitos a certo controle pelo Estado. Essa é uma particularidade do Brasil em comparação aos demais países estudados, em especial os membros da OCDE, que funcionam com outra forma de organização dos bens e serviços de uso público mais ancorados no mercado e na atuação direta de empresas privadas.

Desde a edição do Decreto nº 6.703/08, a legislação brasileira define como setores de IC os de energia, transporte, águas e comunicações. Posteriormente, adicionou-se o setor financeiro como parte das atividades de sensibilidade do país. Esses setores estão regulados pela Constituição Federal (CF/88) em regime restritivo.[60]

60. O art. 21, incisos XI e XII, alíneas a-f da CF/88, fruto de emendas constitucionais (ECs), indica que é de competência da União a exploração dos serviços de telecomunicações; radiodifusão sonora e de sons e imagens; instalações de energia elétrica e o aproveitamento energético dos cursos de água; navegação aérea, aeroespacial e a infraestrutura aeroportuária; de transporte ferroviário e aquaviário; de transporte rodoviário; de portos marítimos, fluviais e lacustres. Como parte do Programa Nacional de Desestatização (Lei nº 8.031/90, reformulado pela Lei nº 9.491/97), o presidente Fernando Henrique Cardoso encampou a promulgação de ECs para ampliar a participação de agentes privados nos setores públicos, permitir o investimento estrangeiro e fomentar a competição nessas atividades. Em termos de ECs, duas transformações da ordem econômica brasileira são importantes: a extinção de determinadas restrições ao capital estrangeiro (EC nº 6/95, EC nº 7/95 e EC nº 36/02) e a flexibilização dos monopólios estatais (EC nº 5/95, EC nº 8/95 e EC nº 9/95).

A atuação de agentes privados em tais atividades é permitida apenas a partir da outorga de autorizações, permissões ou concessões. Esses títulos jurídicos, previstos pelo art. 175 da CF/88 e regulamentados em leis específicas, transferem a gestão de atividades estatais ao particular, por tempo determinado e precedido de licitação. O modelo de delegação da atividade mantém a propriedade da infraestrutura na pessoa jurídica da União, sendo possível, portanto, a retomada das atividades pelo Estado a qualquer tempo em que o delegatário não cumpra os parâmetros por ele estipulados à sua conveniência e comodidade (Mello, 2016; Aragão, 2013b; Monteiro, 2010).

As atividades de emissão de moeda, administração das reservas cambiais do país e fiscalização das operações de natureza financeira, especialmente as de crédito, câmbio e capitalização, de seguros e de previdência privada, estão sujeitas a regime ainda mais restritivo, sendo de monopólio da União, conforme o art. 21, incisos VII e VIII da CF/88. Também nesse sentido está a exploração dos serviços e das instalações nucleares de qualquer natureza, nas atividades de pesquisa, lavra, enriquecimento e reprocessamento; a industrialização e o comércio de minérios nucleares e seus derivados (art. 21, inciso XXIII da CF/88); e, recentemente, a organização, a fiscalização e o tratamento de dados pessoais (art. 21, inciso XXVI da CF/88).

Para além do regime constitucional, o funcionamento das ICs é passível de controle pelo Estado, em especial, visando à concretização de objetivos de interesse público. Princípios orientadores para o funcionamento são a garantia da eficiência na realização da atividade, a continuidade e a universalidade (Pietro, 2013).[61]

Para além do regramento legal, vale notar que as atividades de IC também são reguladas por normas setoriais específicas e monitoradas por autoridades ministeriais e agências reguladoras. Criadas como consequência da desestatização da prestação de certos serviços no Brasil, essas figuras têm a função de suprir a necessidade de fortalecimento de sua função reguladora e fiscalizadora.[62] A atividade das agências reguladoras é guiada pela busca por escolhas técnicas, preservadas das disputas partidárias e das complexidades dos debates congressuais, mais apropriados às escolhas político-administrativas (Moreira Neto, 2002).

Até 2002, haviam sido criadas no país as seguintes agências reguladoras: a Agência Nacional de Telecomunicações (Anatel), prevista na Lei nº 9.472/97; a Agência Nacional de Energia Elétrica (Aneel), instituída pela Lei nº 9.427/96; a Agência Nacional do Petróleo (ANP), instituída pela Lei nº 9.478/97; a Agência Nacional de Vigilância Sanitária (Anvisa), estabelecida pela Lei nº 9.782/99; a Agência Nacional de Saúde Suplementar (ANS), prevista na Lei nº 9.961/00; a Agência Nacional de Águas (ANA), instituída pela Lei nº 9.984/00; e a Agência Nacional de Transportes Terrestres (ANTT) e Agência Nacional de Transportes Aquaviários (Antaq), ambas criadas pela Lei nº 10.233/12 (quadro A.2 do apêndice A). Cada uma dessas agências conta com autonomia administrativa, orçamentária e financeira, sendo elevadas ao *status* de independentes. Isso também implica que atuam dentro das suas possibilidades e limitações, havendo diferentes graus de sofisticação entre os trabalhos por elas realizados (Aragão, 2013b).

61. Os prestadores de serviços em setores regulados também tendem a estar sujeitos a obrigações que não são tipicamente exigidas de agentes particulares, como o dever de prestar informações, de limitar a cobrança dos serviços prestados ao valor de tarifas ou de seguir regras de proteção aos usuários dos serviços (Guimarães, 2011).

62. A literatura de direito administrativo relaciona as funções das agências reguladoras em: i) controle de tarifas, de modo a assegurar o equilíbrio econômico e financeiro do contrato; ii) universalização do serviço, estendendo-os a parcelas da população que deles não se beneficiam por força da escassez de recursos; iii) fomento da competitividade nas áreas nas quais não haja monopólio natural; iv) fiscalização do cumprimento do contrato de concessão; e v) arbitramento dos conflitos entre as diversas partes envolvidas: consumidores do serviço, poder concedente, concessionários, a comunidade como um todo, os investidores potenciais etc. (Mannheimer, 1998).

No que se refere ao setor financeiro, as operações são controladas pelo BCB, criado pela Lei nº 4.595/64, que estabelece normativas específicas para as operações desse setor.

Para além das agências reguladoras, as empresas prestadoras de serviços estão sujeitas ao monitoramento constante de outras autoridades públicas especializadas. Citam-se, nesse sentido, os exemplos do setor elétrico e do papel de monitoramento diário das redes de transmissão pelo Operador Nacional do Sistema (ONS). Além do controle setorial específico, em geral, as operações de caráter societário em setores de IC no Brasil também estão sujeitas aos escrutínios de outras autoridades que têm como função regular o bom funcionamento do mercado brasileiro em geral, como o Conselho Administrativo de Defesa Econômica (Cade) e a Comissão de Valores Mobiliários (CVM). A atuação do Tribunal de Contas da União (TCU) também é relevante para atividades relacionadas à IC, no limite em que envolvam a utilização de recursos públicos. Com base em norma interna, a Instrução Normativa nº 81/2018, o TCU vem analisando aspectos de contratos de concessão e até de editais previamente à sua publicação, a fim de prevenir modelagens contratuais equivocadas e aperfeiçoar trabalhos técnicos considerados insuficientes.

No entanto, não foram encontrados, na legislação ou regulamentos, conceitos que diferenciam a nacionalidade de origem do capital que adentra o mercado brasileiro.[63] Empresas estrangeiras podem ser sócias de sociedades brasileiras, aportando capital do exterior (art. 1.134 do Código Civil brasileiro). No âmbito das contratações públicas, a Lei das Licitações (Lei nº 8.666/93, alterada pela Lei nº 14.133/21) estabelece diversos dispositivos que permitem a participação de empresas estrangeiras em procedimentos licitatórios, impedindo tratamentos discriminatórios frente aos nacionais (incisos I e II do § 1º do art. 3º), embora utilize alguns requisitos para sua atuação, como a exigência de representante legal no Brasil (§ 4º do art. 32). Ainda, as autoridades competentes tendem a construir os editais dos leilões de forma a aprovar a participação estrangeira nos processos licitatórios, desde que alguns padrões mínimos de controle da estrutura societária do agente – internacional ou não – sejam cumpridos. Por exemplo, tem-se a obrigação de que a estrutura societária seja construída em conformidade com as leis brasileiras, a partir da constituição de figuras como as Sociedades de Propósito Específico (SPEs).[64] Outro fator previsto pelos reguladores é que, na participação de consórcios no leilão, a pessoa jurídica formada por empresas brasileiras e estrangeiras deve ser liderada por empresa brasileira, como observado nos leilões Aneel nºs 6/2014 e 15/2015.[65] Sendo assim, a entrada de capital estrangeiro parece ser facilmente operacionalizada por meio da constituição de subsidiárias das empresas estrangeiras no país.

De maneira geral, pode-se dizer que não são observadas grandes particularidades na atuação dos órgãos de fiscalização dos serviços públicos pertencentes à IC do Brasil, que modulem a entrada

63. Em virtude da EC nº 6/95, não é vedado às pessoas jurídicas de controle estrangeiro constituídas por leis brasileiras com sede em território nacional a prestação de serviços públicos pela CF/88. Há que se dizer também que as sociedades estrangeiras podem funcionar no país, desde que autorizadas pelo poder Executivo.

64. Em geral, a estrutura das SPEs é escolhida porque os editais de leilões do setor público permitem que consórcios participem deles. Consórcios tendem a ser licitantes mais competitivos porque podem reunir em uma única estrutura sócios operacionais, fornecedores de equipamentos, construtoras especializadas e fundos de investimento (Cazzuro, 2017).

65. É interessante salientar que, no Edital Aneel nº 2015/2015, que se referia à construção de linhas de transmissão de energia elétrica, a agência reguladora permitiu que empresas estrangeiras concorram individualmente sem a constituição de SPEs, caso demonstrem, por meio da documentação necessária, capacidade legal para tanto e nomeiem representantes autorizados da empresa no Brasil.

de investimento estrangeiro no país, nos moldes observados na experiência comparada. O que se percebe é a mera reafirmação da estrutura dos investimentos já prevista na legislação para o setor.[66]

Um caso que pode ser considerado exceção a tal tendência é a revisão do TCU do edital de leilão redigido pela Anatel referente à exploração de serviços utilizando a tecnologia de conectividade móvel 5G. As discussões sobre esse edital foram feitas previamente à sua publicação, em um contexto de sabida concorrência tecnológica entre empresas dos Estados Unidos e da China. Havia, portanto, forte especulação a respeito dos interesses geopolíticos envolvidos.

Após uma discussão política entre diferentes ministérios, a redação final do edital não teve efeitos discriminatórios entre empresas estrangeiras, inclusive no que se refere à chinesa Huawei. Havia certa comoção a respeito de temas de segurança nacional e desconfiança a respeito de uma possível espionagem ser realizada através das redes 5G, tendo inclusive o Ministério da Defesa sido ouvido sobre o assunto.[67] No entanto, em nenhum dos documentos oficiais do processo o argumento da segurança nacional foi decisivo. Nesse sentido, os votos do TCU que aprovaram o edital e recomendaram a alteração de alguns termos do leilão, sob relatoria do ministro Raimundo Carreiro, fundamentaram-se em aspectos financeiros da operação e de resguardo do erário público. Mesmo o voto divergente, do ministro Aroldo Cedraz, apontou problemas de cálculo do preço da aquisição dos direitos de exploração das faixas de frequência, e não qualquer argumento de bloqueio do investidor estrangeiro sob o argumento de ameaça à segurança nacional.

Por fim, a redação do Decreto nº 11.200/22, que aprovou o Plansic, estabelece a obrigação do GSI/PR de apresentar, no prazo de dois anos, uma minuta de projeto de lei sobre a política nacional de segurança de infraestruturas críticas à Câmara de Relações Exteriores e de Defesa Nacional do Conselho de Governo. Assim, o ordenamento jurídico pátrio mostra, de certa forma, estar preocupado com ameaças externas contra as ICs nacionais, sem, contudo, fazer qualquer tipo de referência explícita ao investimento externo.

4 CONSIDERAÇÕES FINAIS

Historicamente, o debate sobre as ICs tem como ponto central questões de segurança nacional. Com a revolução tecnológica presenciada no mundo nos últimos anos, que elevou a interdependência e a interação entre os sistemas de ICs, esse debate tem sido foco dos IAIEs em diversos países. Assim, este artigo procurou investigar as iniciativas brasileiras de proteção à IC e sua relação com o tratamento ao investimento externo em áreas essenciais para o funcionamento do país.

O termo infraestrutura crítica descreve ativos que são essenciais para os países e suas políticas públicas, geralmente envolvendo atividades como produção e distribuição de alimentos, suprimento de água, saúde pública, transportes (incluindo portos, aeroportos e rodovias), serviços de geração,

66. A realização de estudo, que foge ao escopo desta contribuição, dos editais e decisões de outras entidades administrativas, como o Cade e o TCU, seria interessante para o fortalecimento do argumento aqui desenvolvido. Nesse sentido, também a investigação da jurisprudência dos tribunais brasileiros, já que o Judiciário também exerce uma camada de controle à prestação de serviços de IC. Não obstante, inexiste, em nosso conhecimento, ação das autoridades administrativas brasileiras que bloqueiem a entrada de capital estrangeiro sob o argumento de salvaguarda da segurança nacional ou de proteção das infraestruturas críticas.

67. Disponível em: https://www.camara.leg.br/noticias/727377-grupo-que-discute-leilao-do-5g-vai-ouvir-ministerio-da-defesa-sobre-seguranca-nacional/. Acesso em: 28 mar. 2023.

transmissão e distribuição de energia, telecomunicações e serviços financeiros e, mais recentemente, cibersegurança e proteção de dados a partir de tecnologias de infraestrutura de redes, como o 5G.

No cenário internacional, observa-se um grupo de países que, embora não mencionem diretamente o termo infraestrutura crítica em seus IAIEs (como é o caso da Índia, da África do Sul, da Coreia do Sul e do Japão), apresenta preocupações relacionadas aos setores que se encaixam nessa definição ou, ainda, se utilizam de outros termos, como infraestruturas importantes e infraestruturas sensíveis, para tratar do mesmo tipo de preocupação. Em contrapartida, há um segundo grupo de países que apresenta a nomenclatura da IC de forma direta em seus IAIEs (é o caso de Portugal, Alemanha, Estados Unidos e Austrália) e como um dos principais focos de seus mecanismos.

No Brasil, o debate sobre IC se iniciou, mais diretamente, com o Decreto nº 6.703/2008, que definiu oficialmente quais os setores a serem considerados críticos para o país e que se tornaram alvo de regulamentação específica. Nesse sentido, foram articuladas estratégias nacionais de proteção dos setores selecionados como ICs no Brasil (Ensic e E-Ciber), que alertam para a necessidade de estabelecimento de "parcerias estratégicas no ambiente cibernético", principalmente devido ao fato de que grande parte da gestão dessas infraestruturas está sob o comando do setor privado.[68]

A Ensic promove ações de análise e prevenção de riscos associados à prestação dos serviços essenciais, com o intuito de manter a continuidade da atividade, privilegiando a segurança física e operacional. Já a E-Ciber foi construída em módulos chamados de eixos temáticos transversais para contemplar a segurança cibernética, a defesa cibernética, a segurança das infraestruturas críticas, a segurança da informação sigilosa e a proteção contra vazamento de dados. A E-Ciber aborda as atividades de informação e o acesso a dados como pontos vulneráveis para a segurança de ICs.

Apesar da preocupação com a resiliência das estruturas críticas do país e com a higidez no meio digital das atividades da administração pública, nenhuma das iniciativas supracitadas institui qualquer tipo de controle de agentes estrangeiros, tampouco procedimento de avaliação de entrada de capital externo. Pelo contrário, nas poucas vezes em que agentes estrangeiros são mencionados nas políticas de IC brasileiras, a referência é feita no sentido de promoção à participação e à cooperação internacionais.

Referente à regulação da entrada de investimento externo, nota-se, no Brasil, um movimento oposto ao enrijecimento regulatório dos IEAEs ocorrido em países como Estados Unidos, Canadá, Austrália, Alemanha e Japão. As regras brasileiras de acesso a investimentos em setores de infraestrutura consideradas críticas vêm passando por um processo de liberalização, flexibilização e facilitação de acesso da iniciativa privada, seja ela de origem nacional ou estrangeira. Nesse sentido, citam-se as iniciativas de modernização do setor elétrico (PLS 232/16), a reforma da lei de saneamento básico (Lei nº 14.026/20), de cabotagem (Lei nº 14.301/22, chamada BR do Mar), dos portos (Lei nº 14.047/20), do setor financeiro (Lei nº 14.286/21, dos câmbios e o Decreto nº 1.029/19, que autorizou a participação de capital estrangeiro em instituições financeiras brasileiras) e até a proposta de facilitação da lei de concessões (Projeto de Lei nº 7.843/14).

Esse movimento pode ser ligado à constante necessidade de um país em desenvolvimento de receber investimentos para ampliação e modernização de sua infraestrutura, o que o leva a adotar

68. Nos termos do Decreto nº 10.222/20: "A necessidade de estabelecer e consolidar parcerias estratégicas no ambiente cibernético torna-se ainda mais evidente ao se constatar que grande parte das infraestruturas críticas estão sob responsabilidade do setor privado, o que reforça a necessidade de propósitos comuns, em segurança cibernética, entre governo, empresas privadas, academia e a sociedade em geral."

medidas alinhadas às boas práticas internacionais de abertura de mercados. Também pode ser ligado à experiência exitosa brasileira de recepção do capital externo nos últimos anos, a qual conta com um monitoramento constante e técnico dos serviços públicos, nos quais as infraestruturas críticas se incluem.

Essa ausência de aproximação entre a instituição de um IAIE e a proteção às ICs não é exclusiva dos instrumentos jurídicos que estabelecem as políticas de segurança à IC no Brasil (Sanchez-Badin *et al*., 2021). Em levantamento preliminar de bibliografia, os trabalhos acadêmicos tampouco parecem sobrepor os debates, mantendo seu foco em investigações técnicas e métodos de promoção da segurança das ICs (Andrade, 2021; Diniz, 2017; Silva, 2015), com poucos exemplos de investigações sobre a política brasileira de proteção das ICs (Souza Júnior, 2013) e sua relação com a geopolítica global ou com o tema da defesa nacional (Sá, 2017). Fóruns militares, como a Escola Superior de Guerra, se mostram como espaços mais interessantes para a identificação de estudos científicos com uma abordagem mais integrada sobre segurança de infraestruturas críticas – consultar, por exemplo, Rocha (2019) e Sá (2017). Contudo, mesmo entre esses trabalhos, as abordagens setoriais específicas e, em especial, de defesa contra ataques cibernéticos, são as mais recorrentes (Nonato e Pinho, 2021; Araujo, 2020).

A análise feita neste artigo demonstra que o Brasil não parece estar alinhado às práticas identificadas internacionalmente, quando se trata da preservação de infraestruturas críticas por mecanismos de avaliação do investimento estrangeiro. Dessa forma, vislumbramos no debate da avaliação de entrada do capital externo um convite para reflexão sobre a adoção de estruturas mais centralizadas e políticas para lidar com a proteção das infraestruturas críticas.

REFERÊNCIAS

ANDRADE, Edson Ramos de. **Metodologia para avaliação da resiliência e suporte à decisão em ambiente radioativo urbano simulado**. 2021. Tese (Doutorado) – Centro de Tecnologia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2021.

ARAGÃO, Alexandre Santos de. **Direito dos serviços públicos**. 3. ed. Rio de Janeiro: Forense, 2013a.

_____. **Agências reguladoras e a evolução do direito administrativo econômico**. 3. ed. Rio de Janeiro: Forense, 2013b.

ARAUJO, José Euclides Oliveira de. **A atuação da defesa cibernética na proteção de infraestruturas críticas do Brasil**. 2020. Monografia (Especialização) – Escola Superior de Guerra, Brasília, 2020.

BARROSO, Luís Roberto. Agências Reguladoras. **Migalhas**, 22 jan. 2003. Disponível em: https://www.migalhas.com.br/depeso/1007/agencias-reguladoras. Acesso em: 24 jun. 2022.

BATH, Vivienne. Foreign investment, the national interest and national security: foreign direct investment in Australia and China. **Sydney Law Review**, v. 34, n. 1, p. 5-34, 2012.

BLACKLOCK, Jacob. China: foreign direct investment regimes 2023. **ICLG.com**, 30 nov. 2022. Disponível em: https://iclg.com/practice-areas/foreign-direct-investment-regimes-laws-and-regulations/china.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. **Diário Oficial**, Brasília, 22 nov. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm.

_____. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial**, Brasília, 5 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm.

BRUNNER, Elgin M.; SUTER, Manuel. **International CIIP Handbook 2008/2009**: an inventory of 25 national and 7 international critical information infrastructure protection policies. Zürich: Swiss Federal Institute of Technology, 2009.

CANADA. **Annual Report**: Investment Canada Act 2021-2022. Ottawa: Innovation, Science and Economic Development Canada, 2022. Disponível em: https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/annual-report-2021-2022. Acesso em: 29 mar. 2023.

COLLIER, Stephen; ANDREW, Lackoff. The vulnerability of vital systems: how "critical infrastructure" became a security problem ByCollier. *In*: DUNN, Myriam; KRISTENSEN, Kristian. **Securing "the Homeland"**: critical infrastructure, risk and (in)security. Londres, 2008.

COTTA, Philipp; LI, Lelu; WISTINGHAUSEN, Christian von. **Foreign direct investment regimes 2021**: Germany. Disponível em: https://iclg.com/practice-areas/foreign-direct-investment-regimes-laws-and-regulations/germany. (Acesso restrito a membros). Acesso em 8 dez. 2021.

DANZMAN, Sarah Bauerle; MEUNIER, Sophie. **The big screen**: global crises and the diffusion of foreign investment review. 2022. Disponível em: https://ostromworkshop.indiana.edu/pdf/seriespapers/2021spr-colloq/bauerle-danzman.pdf. Acesso em: 8 dez. 2023.

DAWSON, Maurice. *et al*. Understanding the challenge of cybersecurity in critical infrastructure sectors. **Land Forces Academy Review,** v. 26, n. 1, p. 69-75, 2021. Disponível em: https://doi.org/10.2478/raft-2021-0011.

DINIZ, Helder Henrique Lima. **Resilience in the design of critical infrastructure**: applications in power grid and logistic systems. Tese (Doutorado) – Centro de Tecnologia e Geociências, Universidade Federal de Pernambuco, Recife, 2017.

DUNN, Myriam. The socio-political dimensions of critical information infrastructure protection (CIIP). **International Journal of Critical Infrastructures**, v. 1, n. 2-3, p. 258-268, 2005.

ESPLUGUES, Carlos. Towards a common screening system of foreign direct investment on national interest grounds in the European Union. **Cultural Media Entertainment Law Institute Journal**, vol. 15-2, n. 2018, p. 1-56, 2018.

EUROPEAN COMMISSION. **Proposal for a Directive on the resilience of critical entities**. Brussels: EU Comission, 2020.

FARR, Christina, LEVY, Ari. The Trump administration is forcing this health startup that took Chinese money into a fire sale. **CNBC**, 4 Apr. 2019. Disponível em: https://www.cnbc.com/2019/04/04/cfius-forces-patientslikeme-into-fire-sale-booting-chinese-investor.html. Acesso em: 8 dez. 2023.

FJÄDER, Christian. The nation-state, national security and resilience in the age of globalisation. **Resilience**, v. 2, n. 2, p. 114-129, 2014.

GIANNOPOULOS, Georgios; FILIPPINI, Roberto; SCHIMMER, Muriel. Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art. **JRC Technical Notes**, v. 1, n. 1, p. 1-53, 2012.

GUIMARÃES, Bernardo Strobel. **O exercício da função administrativa e o direito privado**. 2011. Tese (Doutorado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2134/tde-26032012-111633/pt-br.php. Acesso em: 24 jun. 2022.

GUTERRES, Egon. Regulação de riscos e proteção de infraestruturas críticas: os novos ventos do fenômeno regulatório. **Revista de Direito Setorial e Regulatório**, Brasília, v. 2, n. 1, p. 107-160, maio 2016.

HILF, Juliane; RÖHLING, Frank; BRAUN, Heiner. German foreign investment authority takes off the gloves. **Lexology**, 1 Aug. 2018. Disponível em: https://www.lexology.com/library/detail.aspx?g=9d1dc1c6-3bd9-4ef7-bb45-8f2c5687bb43. Acesso em: 7 dez. 2023.

JANG, Joo Hyoung; KIM, Rieu. **Foreign direct investment regimes 2021**: Korea. Disponível em: https://www.celis.institute/. (Acesso restrito a membros). Acesso em: 28 dez. 2022.

JEON, Jaemin; JUNG, Haneul. Korea. *In*: FACEY, Brian A. **The Foreign Investment Regulation Review**. Law Business Research, 2016. p. 173-183.

JUSTEN FILHO, Marçal. **Teoria geral das concessões de serviços públicos**. São Paulo: Dialética, 2003.

KORSTEN, Léon. *et al*. Multi-jurisdiction guide for screening foreign investments. **DLA PIPER**, 25 maio 2021. Disponível em: https://www.dlapiper.com/en/insights/publications/2021/05/multi-jurisdiction-guide-for-screening-foreign-investments. Acesso em: 29 mar. 2023.

LICHTENBAUM, Greta; RIBNER, David J. Foreign investment screening in the USA. *In*: **YSEC Yearbook of Socio-Economic Constitutions 2020**: a common European law on investment screening (CELIS), p. 363-378, 2021.

MANNHEIMER, Sérgio. Agências estaduais reguladoras de serviços públicos. **Revista Forense**, v. 343, p. 221-236, 1998.

MELLO, Celso Antônio Bandeira de. **Curso de direito administrativo**. 33. ed. rev. atual. São Paulo: Malheiros, 2016.

MISRA, Manu. Foreign investment in critical national infrastructure by SCEs and screening mechanisms. *In*: DELIMATSIS, Panagiotis; DIMITROPOULOS, Georgios; GOURGOURINIS, Anastasios. (Ed.). **State Capitalism and International Investment Law**: studies in international trade and investment law. London: Hart Publishing, 2023.

MARKOPOULOU, Dimitra; PAPAKONSTANTINOU, Vagelis. The regulatory framework for the protection of critical infrastructures against cyberthreats: identifying shortcomings and addressing future challenges – the case of the health sector in particular. **Computer Law and Security Review**, n. 41, 2021.

MARRAY, Michael. Germany blocks investment by China's state grid in 50Hertz. **The Asset**, 1 Aug. 2018. Disponível em: https://www.theasset.com/europe/34804/germany-blocks-investment-by-chinas-state-grid-in-50hertz. Acesso em 7 dez. 2023.

MOTEFF, John D.; COPELAND, Claudia; FISCHER, John. **Critical Infrastructures**: what makes an infrastructure critical? Washington: Congressional Research Service, 2003. Disponível em: https://digital.library.unt.edu/ark:/67531/metacrs5039/. Acesso em: 29 mar. 2023.

MOTEFF, John, D.; PARFOMAK, Paul. **Critical infrastructure and key assets**: definition and identification. 2004. Washington: Congressional Research Service, 2004. Disponível em: https://www.semanticscholar.org/paper/Critical-Infrastructure-and-Key-Assets%3A-Definition-Moteff-Parfomak/3792a62a097ff59a1a5ba5f3326ae65511c26b74. Acesso em: 29 mar. 2023.

MONTEIRO, Vera. **Concessão**. São Paulo: Malheiros Editores, 2010.

MOTTAHEDI, Adel. *et al*. The resilience of critical infrastructure systems: a systematic literature review. **Energies**, v. 14, n. 6, p. 1571, 2021.

MOREIRA, Egon Bockmann. **Direito das concessões de serviço público**. São Paulo: Malheiros Editores, 2010.

MOREIRA NETO, Diogo de Figueiredo. **Direito da regulação**. [s.l.]: [s.n.], 2002.

MOTEFF, John; PARFOMAK, Paul. **Critical infrastructure and key assets**: definition and identification. Washington: Congressional Research Service, Library of Congress, 2004.

NONATO, Marcos Paulo Cardoso; PINHO, Harley de. **A integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das infraestruturas críticas de interesse para Defesa Nacional**. 2021. Monografia (Especialização) – Escola Superior de Guerra, Brasília, 2021.

OECD – ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Emerging risks in the 21st century**: an agenda for action. Paris: OECD Publishing, 2003. Disponível em: https://www.oecd.org/gov/risk/37944611.pdf. Acesso em: 29 mar. 2023.

_____. **Protection of "critical infrastructure" and the role of investment policies relating to national security**. Paris: OECD Publishing, 2008. Disponível em: https://www.oecd.org/investment/investment-policy/40700392.pdf. Acesso em: 29 mar. 2023.

_____. **Future global shock**: improving risk governance. Paris: OECD Publishing, 2012. Disponível em: https://www.oecd.org/governance/48256382.pdf. Acesso em: 29 mar. 2023.

_____. **What does "resilience" means for donors?** Paris: OECD, 2013. (OECD Factsheet). Disponível em: https://www.oecd.org/dac/conflict-fragility-resilience/docs/May%2010%202013%20FINAL%20resilience%20PDF.pdf. Acesso em: 4 abr. 2022.

_____. **Recommendations of the Council on the Governance of Critical Risks**. Paris: OECD, 2014. Disponível em: https://www.oecd.org/gov/risk/Critical-Risks-Recommendation.pdf. Acesso em: 29 mar. 2023.

_____. **Good governance for critical infrastructure resilience**. Paris: OECD Publishing, 2019. (OECD Reviews of Risk Management Policies). Disponível em: https://www.sdg16hub.org/system/files/2020-08/Good%20Governance%20for%20Critical.pdf. Acesso em: 29 mar. 2023.

_____. **Investment screening was already enjoying a heyday before the covid-19 crisis**: the pandemic is accelerating, rather than triggering this trend. [s.l.]: OECD, 2020. Disponível em: https://www.oecd.org/coronavirus/policy-responses/investment-screening-in-times-of-covid-19-and-beyond-aa60af47/. Acesso em: 24 jun. 2022.

_____. **Fostering economic resilience in a world of open and integrated markets**: risks, vulnerabilities and areas for policy action. Paris: OECD Publishing, 2021. Disponível em: https://www.oecd.org/newsroom/OECD-G7-Report-Fostering-Economic-Resilience-in-a-World-of-Open-and-Integrated-Markets.pdf. Acesso em: 29 mar. 2023.

_____. **FDI in critical infrastructure**: supporting EMDEs in attracting more, better and safe FDI. Paris: OECD Publishing, 2023. Disponível em: https://www.oecd.org/investment/FDI-critical-infrastructure.pdf. Acesso em: 19 jul. 2023.

OSEI-KYEI, Robert. *et al*. Systematic review of critical infrastructure resilience indicators. **Construction Innovation**, 2022.

PIETRO, Maria Sylvia Zanella di. Serviços públicos. *In*: DALLARI, Adilson Abreu; NASCIMENTO, Carlos Valder; MARTINS, Ives Gandra da Silva (Coord.). **Tratado de direito administrativo**. São Paulo: Saraiva, 2013. v. 2.

POHL, JOACHIM; ROSSELOT, Nicolás. Acquisition – and ownership-related policies to safeguard essential security nterests – current and emerging trends, observed designs, and policy practice in 62 economies. **SSRN Electronic Journal**, 16 Jun. 2020. Disponível em: https://doi.org/10.2139/ssrn.3607919.

RAJAVUORI, Mikko; HUHTA, Kaisa. Investment screening: implications for the energy sector and energy security. **Energy Policy**, v. 144, p. 111646, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S0301421520303797. Acesso em: 24 jun. 2022.

RIBEIRO, Sérgio Luiz. *et al*. Aplicação da metodologia para identificação da infraestrutura crítica (MI2C) no Pan 2007. **CPqD Tecnologia**, Campinas, v. 3, n. 2, p. 7-16, 2007.

ROBERTS, Anthea. Risk, reward, and resilience framework: integrative policy making in a complex world. **Journal of International Economic Law**, v. 26, n. 2, p. 233-265, 2023.

ROBERTS, Anthea; MORAES, Henrique; FERGUSON, Victor. Toward a geoeconomic order in international trade and investment. **Journal of International Economic Law**, v. 22, n. 4, p. 655-676, 2019.

ROCHA, Paulo Cesar Cardoso. **A relação entre a gestão de riscos integrada em uma organização com infraestrutura crítica e as questões de defesa nacional**. Brasília: ESG, 2019. (Curso de Altos Estudos em Defesa – Caed – da Escola Superior de Guerra).

ROGUSKI, Przemysław. An inspection regime for cyber weapons: a challenge too far? **AJIL Unbound**, n. 115, p. 111-115, 2021.

SANCHEZ-BADIN, Michelle Ratton. *et al*. Avaliação de investimentos externos em infraestrutura crítica: exemplos no setor de energia da Alemanha, da Austrália, dos Estados Unidos e da Rússia. **Boletim de Economia e Política Internacional**, n. 30, p. 95-113, 2021.

_____. **Mapeamento de quinze instrumentos de avaliação dos investimentos externos**. Brasília: Ipea, 2022. (Texto para Discussão, n. 2736).

SANCHEZ-BADIN, Michelle Ratton; MORAIS, Ana Maria; BONINI, Carolina Bianchini. Instrumentos de avaliação de investimento externo e o debate legislativo no Brasil. **Boletim de Economia e Política Internacional**, n. 31, 2021. Disponível em: http://repositorio.ipea.gov.br/bitstream/11058/11142/1/bepi_31_instrumentos_avaliacao.pdf.

SANTOS, Daiene Bittencourt Mendes; CARVALHO, Bruno Eustáquio Ferreira Castro de; CAVALCANTE, Sarita de Paula. Segurança das Infraestruturas Críticas no Brasil. *In*: SIMPÓSIO BRASILEIRO DE RECURSOS HÍDRICOS, 19., 2011, Maceió. **Anais**... Maceió: ABRHidro, 2011.

SILVA, Victor Raul Neumann. **Parametrização do framework Ipsec para a segurança na interoperabilidade em smart grid**. 2015. Dissertação (Mestrado) – Departamento de Engenharia Elétrica, Universidade Federal do Paraná, Curitiba, 2015.

SOUZA, Ielbo Marcus Lobo de. Desafios à ordem internacional: ataques armados por atores não estatais e o direito de legítima defesa. **Revista de Informação Legislativa**, Brasília, ano 45, n. 177, 2008.

SOUZA JÚNIOR, Alcyon Ferreira de. **Segurança cibernética**: política brasileira e a experiência internacional. 2013. Dissertação (Mestrado profissional) – Universidade Católica de Brasília, Brasília, 2013.

TAKAHASHI, Hiroaki; KAWAMURA, Koji. **Foreign direct investment regimes 2021**: Japan. Disponível em: https://iclg.com/practice-areas/foreign-direct-investment-regimes-laws-and-regulations/japan. (Acesso restrito a membros). Acesso em: 11 ago. 2021.

UNCTAD – UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **World investment report**: investor nationality – policy challenges. Geneva: UNCTAD, 2016.

_____. **National security-related screening mechanisms for foreign investment**: an analysis of recent policy developments. Geneva: UNCTAD, 2019.

UNITED STATES. Department of Homeland Security. **National Infrastructure Protection Plan**. Washington: DHS, 2009.

_____. Department of Homeland Security. **Energy sector**: specific plan 2015. Washington: DHS, 2015.

WEST, M.; LUTHER, P.; WILCOX, J. **Foreign direct investment regimes 2021**: USA. Disponível em: https://iclg.com/practice-areas/foreign-direct-investment-regimes-laws-and-regulations/usa. (Acesso restrito a membros). Acesso em: 7 dez. 2023.

APÊNDICE A

QUADRO A.1

Setores eleitos como infraestrutura crítica (IC) no Brasil, Estados Unidos, Rússia, Reino Unido e União Europeia

Setor analisado	Brasil	Estados Unidos	Rússia	Reino Unido	União Europeia
Definição de IC	Instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança nacional do Estado e da sociedade.	Ativos e sistemas (físicos ou virtuais) vitais para os Estados Unidos cuja incapacidade ou destruição teria um impacto debilitante na segurança, na segurança econômica nacional, na saúde pública nacional ou qualquer combinação dessas questões.	Não há definição particular. Contudo, cinco áreas de atenção: sociedade, política, economia, meio ambiente, defesa, segurança e aplicação da lei.	Ativos de infraestrutura (físicos ou virtuais) vitais para a prestação contínua e integridade dos serviços essenciais dos quais o Reino Unido depende, cuja perda ou comprometimento levaria a graves consequências econômicas ou sociais ou à perda de vidas.	Ativos e sistemas localizados em Estados-membros que sejam essenciais para a manutenção de funções vitais da sociedade, saúde, segurança, bem-estar econômico ou social das pessoas, e cuja interrupção ou destruição teria um impacto significativo em um Estado-membro como resultado da não manutenção dessas funções.
Agricultura e nutrição		X		X	X
Águas e esgoto	X	X		X	X
Área de fronteira e região de reserva	X				
Barragens	X	X			X
Biossegurança e bioproteção	X				
Energia	X	X	X	X	X
Indústria de defesa		X	X		
Indústrias de mineração e metalurgia	X		X		
Indústria química		X	X		
Instalações comerciais		X			
Instalações governamentais		X		X	X
Manufatura crítica		X			
Mídia, radiodifusão e ativos culturais	X			X	X
Portos					X
Reatores, materiais e resíduos nucleares	X	X	X	X	
Saúde pública		X	X	X	X
Serviços emergenciais		X		X	
Serviços postais	X				
Sistema financeiro	X	X	X	X	X
Sistemas de transporte	X	X	X	X	X
Tecnologia da informação		X			X
Telecomunicações	X	X	X	X	X

Fonte: Brasil – Resolução GSI/PR nº 14 (24/2/2022), Decreto nº 10.569 (9/12/2020) e Decreto nº 9.573, (22/11/2018); Estados Unidos – Executive Order nº 13.636 (10/2016); Rússia – Russia's Federal Assembly Federal Law nº 187-FL (26/06/2017); Reino Unido – Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards (03/2010) e UK Department for Digital, Culture, Media & Sport. Guidance: Cyber security CNI apprenticeships (26/01/2017); União Europeia – Council of the European Union. Council directive 2008/114/EC. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (23/12/2008); e OSCE – Good Practices Guide on Non Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace (2013).
Elaboração dos autores.

QUADRO A.2
IC na legislação brasileira

Setores	Agências envolvidas em cada setor	Órgãos e agências com atuação transetorial
Defesa	Comissão de Relações Exteriores e de Defesa Nacional (Creden), Estratégia Nacional de Defesa (END), Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, Sistema Brasileiro de Inteligência (Sisbin).	Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações.
Serviços públicos	Agência Nacional de Petróleo (ANP) e Agência Nacional de Vigilância Sanitária (Anvisa).	
Energia	Agência Nacional de Energia Elétrica (Aneel) e Comissão Nacional de Energia Nuclear (CNEN).	
Transporte	Agência Nacional de Transportes Terrestres (ANTT) e Agência Nacional de Transportes Aquaviários (Antaq).	
Águas	Agência Nacional de Águas (ANA).	
Comunicações	Agência Nacional de Telecomunicações (Anatel).	
Finanças	Banco Central do Brasil (BCB), Conselho Administrativo de Defesa Econômica (Cade) e Comissão de Valores Mobiliários (CVM).	BCB: registro de capital estrangeiro. Cade: análise de casos de defesa da concorrência.
Tratamentos de dados pessoais	Agência Nacional de Proteção de Dados (ANPD).	

Elaboração dos autores.

QUADRO A.3
IC na legislação de IAIEs de países selecionados

País	Definição de IC	Setores incluídos
Países que mencionam a IC de forma indireta		
Coreia do Sul	Um investimento estrangeiro pode estar sujeito a uma revisão e a um processo de aprovação se o investimento for visto como uma ameaça à segurança nacional, sem, no entanto, fazer uma menção direta a questões de IC (Jeon e Jung, 2016; Jang e Kim, 2021).	i) Fusão por investidores estrangeiros de empresas militares; ii) principais produtos agrícolas; iii) energia e recursos; iv) infraestrutura; v) transportes; vi) tecnologias-chave; vii) fabricação de equipamentos importantes que envolvam a segurança nacional; e viii) controle de acesso à informação.
Austrália	Os investimentos estrangeiros são permitidos, a não ser que sejas considerados nocivos ao interesse nacional (Esplugues, 2018).	Segurança cibernética.
África do Sul	A ementa legislativa Competition Amendment Act 18[1] de 2018 introduz a triagem de investimento estrangeiro direto (IED) no país com base no interesse nacional.	O uso ou a transferência de tecnologia sensível, a segurança de infraestrutura, o fornecimento de bens ou serviços essenciais.
China	A Lei de Investimento Estrangeiro de 2019 garante a revisão de investimentos que afetem ou tenham a possibilidade de afetar a segurança nacional, sendo que a definição de "segurança nacional" na legislação em questão é dada como "a ausência de ameaças ao poder do estado de governar, o bem-estar do povo, desenvolvimento econômico e social sustentável e outros interesses nacionais importantes, e a capacidade de garantir um estado de segurança contínuo".	Acesso a informação, comunicações, energia e água.
Países que mencionam a IC de forma direta		
Portugal	O Decreto nº 138/201 apresenta como um dos principais conceitos a salvaguarda de infraestrutura e ativos estratégicos essenciais para garantir a defesa e a segurança nacional, bem como a segurança do aprovisionamento do país em serviços fundamentais para o interesse nacional.	Nas áreas de energia, dos transportes e comunicações, enquanto interesses públicos fundamentais.
Alemanha	Atualmente, a regulamentação alemã permite transações econômicas com países estrangeiros, desde que não sejam expressamente proibidas por colocar em risco a ordem pública ou segurança.	Materiais que são usados nas indústrias automotiva, aeroespacial e nuclear e de energia.
Estados Unidos	ICs são sistemas e ativos, físicos ou virtuais tão essenciais que a incapacidade ou destruição de tais sistemas teria um impacto desestruturante na segurança nacional, na estabilidade econômica nacional, na saúde pública ou na combinação desses assuntos, no território dos Estados Unidos.	Energia, saúde digital, dados do consumidor, segurança cibernética.

(Continua)

(Continuação)

País	Definição de IC	Setores incluídos
Países que mencionam a IC de forma direta		
Japão	Exige notificação prévia para certos investimentos limitados que envolvem áreas específicas ou países específicos. Se o investimento se enquadrar nas categorias apresentadas, o investidor deve apresentar notificação ao Ministério das Finanças e aos ministérios relevantes através do Banco do Japão. Após a revisão, os ministérios podem ordenar a suspensão ou alteração do IED se acreditarem que o investimento pode prejudicar a segurança nacional, impedir a ordem pública, dificultar a proteção da segurança ou ter um efeito adverso sobre a economia japonesa.	Armas, aviões, energia nuclear, desenvolvimento espacial); infraestrutura pública (eletricidade, gás, água, telecomunicações, ferrovias); segurança pública (vacinas, segurança privada); e proteção da indústria doméstica (agricultura).
Canadá	-	Saúde pública ou envolvidas no fornecimento de bens e serviços críticos.

Elaboração dos autores.
Nota: [1] Disponível em: https://www.gov.za/documents/competition-amendment-act-18-2018-englishafrikaans-14-feb-2019-0000. Acesso em: 10 jan. 2022.

QUADRO A.4

Autoridades responsáveis por IAIE e por questões de IC em países selecionados

País	Autoridade responsável pelo IAIE	Autoridade responsável por questões de IC
Austrália	Foreign Investment Review Board (Firb)	Australian Cyber Security and Infrastructure Agency (ACSC)
Canadá	Investment Review Division (IRD)	Canadian Security Intelligence Service (CSIS)
Alemanha	Ministry of Economic Affairs and Energy (BMWi)	Agência Federal de Segurança da Informação (Bundesamt für Sicherheit in der Informationstechnik – BSI)
Reino Unido	National Cyber Security Centre (NCSC)	Department for Business, Energy, and Industrial Strategy (Beis)
China	Ministry of Commerce (Mofcom)	National Development and Reform Commission (NDRC)
Portugal	Council of Ministers	Autoridade Nacional de Emergência e Proteção Civil (ANEPC)
Japão	Ministry of Finance	National center of Incident readiness and Strategy for Cybersecurity (Nisc)
Estados Unidos	Committee on Foreign Investment in the United States (CFIUS)	Department of Homeland Security (DHS)
África do Sul	Foreign Investment Review Committee (Firc)	Department of Cooperative Governance and Traditional Affairs (COGTA)
México	Comisión Nacional de Inversiones Extranjeras (CNIE)	Coordenação Nacional de Proteção Civil (CNPC)
Coreia do Sul	Foreign Investment Committee (FIC)	Ministry of Public Safety and Security

Elaboração dos autores.