Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 – Anticipazione fascicolo
Intelligenza artificiale e nuove vulnerabilità

Investimenti esteri diretti nelle infrastrutture digitali e nelle tecnologie critiche alla luce dell'eccezione di sicurezza nazionale nel panorama europeo

Davide Vaira*

SOMMARIO: 1. Introduzione. – 2. L'evoluzione della disciplina delle infrastrutture critiche nell'Unione europea. – 3. Gli investimenti esteri diretti e il rischio di ingerenze economiche e politiche da parte di Stati terzi. – 4. I meccanismi di controllo degli investimenti esteri diretti alla luce del regolamento (UE) 2019/452. – 5. L'eccezione di sicurezza nazionale e la sua giustiziabilità. – 6. Conclusioni.

1. *Introduzione*

Nel mese di novembre 2025, il Consiglio Supremo di Difesa si è riunito al Palazzo del Quirinale per discutere in merito a situazioni di conflitto, concrete o potenziali, in Europa e in Paesi extra-europei[1]. Tra

* Assegnista di ricerca in Diritto internazionale presso l'Università degli Studi di Cagliari. Il presente contributo è stato realizzato grazie al finanziamento del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) per il progetto di ricerca PRIN 2022 PNRR F53D23011940001 intitolato «*Minacce ibride e resilienza democratica: un pacchetto di strumenti analitici e pratici (HYDRA)*».

[1] Consiglio Supremo di Difesa, Il Ministro della Difesa, Guido Crosetto, ha presentato il non-paper *"Il contrasto alla Guerra ibrida: una strategia attiva"*, Roma, 17

gli argomenti oggetto di discussione, particolare rilevanza ha assunto la tematica delle minacce ibride[2], intese come rischio per la sicurezza e l'integrità delle democrazie occidentali[3].

Nel considerare l'efficacia di tali minacce, si è manifestata una particolare preoccupazione per il settore delle infrastrutture critiche, sia in quanto bersaglio primario degli attacchi, soprattutto digitali, sia in quanto potenziale strumento attraverso il quale gli Stati terzi, tramite investimenti, possono attuare una coercizione geo-economica, politica e strategica sullo Stato *target*[4].

L'occasione, nel corso della quale si è sottolineata la necessità, da parte degli Stati membri, di reagire alle minacce ibride con tempestività e coesione, attraverso l'individuazione di strumenti a tutela delle infrastrutture critiche, ha evidenziato il primario interesse degli Stati e delle Istituzioni europee per queste ultime.

Le infrastrutture critiche, intese come «un elemento, un impianto, un'attrezzatura, una rete o un sistema o una parte di [essi] necessari per la fornitura di […] un servizio fondamentale per il mantenimento di funzioni vitali della società, di attività economiche, della salute e della

novembre 2025, consultabile al link www.difesa.it/primopiano/consiglio-supremo-di-difesa/83696.html.

[2] Nel 2018, l'Unione europea, con l'ausilio del Servizio europeo per l'azione esterna, ha tentato di fornire una propria definizione, intendendo, come ibride, quelle minacce che «combinano attività convenzionali e non convenzionali, militari e non militari, che possono essere usate in modo coordinato dagli Stati o da attori non statali per raggiungere specifici obiettivi politici […] [e che] prendono di mira le vulnerabilità critiche e cercano di creare confusione che impedirebbe un processo decisionale rapido ed efficace». Servizio Europeo per l'Azione Esterna, A Europe that Protects: Countering Hybrid Threats, giugno 2018, disponibile sul sito www.eeas.europa.eu/sites/default/files/hybrid_threats_en_final.pdf.

[3] G. CROSETTO, *Il contrasto alla Guerra Ibrida: una strategia attiva*, novembre 2025. Il documento è disponibile al sito www.difesa.it/assets/allegati/83696/non-paper_il_contrasto_alla_guerra_ibrida.pdf.

[4] *Ivi*, p. 21.

sicurezza pubbliche e dell'ambiente»[5], ricoprono un ruolo di primo piano per il funzionamento e per lo sviluppo economico e sociale dei Paesi[6].

Il concetto di infrastruttura critica si estende a una pluralità di settori "tradizionali" – trasporti, energia, comunicazioni –, ai quali, in tempi recenti, si è affiancato il settore digitale che utilizza le infrastrutture per la trasmissione e la conservazione dei dati[7].

L'ambito digitale – con le relative infrastrutture critiche[8] – rappresenta, nello specifico, un settore strategico per gli Stati, in quanto inevitabilmente legato al funzionamento di altri settori essenziali per la società, quali la sanità, i trasporti o l'istruzione[9].

L'Unione europea, pertanto, da ultimo, ha concentrato la sua attenzione sulle infrastrutture digitali, al fine di garantire la sicurezza nel funzionamento dei settori essenziali ed evitare, come si vedrà nel

[5] Tale definizione normativa è data dalla lettura del combinato disposto tra i nn. 4) e 5) dell'art. 2, par. 1, della direttiva (UE) 2024/2557. La medesima definizione normativa è stata recepita, nell'ordinamento italiano, all'art. 2 del d.lgs 4 settembre 2024 n. 134. Per approfondimenti sulla definizione si veda altresì V. VIVERA, *Security and power in the cyberspace*, Bucharest, 2017, pp. 7-9.

[6] O. E. IACOB, *Concerns at the Level of the European Union for the Protection of Critical infrastructures,* in *Acta Universitatis Danubius*, vol. 20, n. 2, 2024, pp. 115-123, spec. p. 116.

[7] Il dominio digitale è stato equiparato dalla NATO ai domini terrestre, marittimo, aereo ed extra-atmosferico, estendendo anche alle ipotesi di cyberattacco le conseguenze previste dall'art. 5 del Trattato Nord Atlantico. Per approfondimenti al riguardo si veda NATO, Cyber Defence, 30 luglio 2024. Disponibile a www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=Allies%20also%20recognised%20that%20the%20impact%20of,North%20Atlantic%20Treaty%2C%20on%20a%20case%2Dby%2Dcase%20basis.

[8] Queste possono essere sia fisiche virtuali e ricomprendono, *ex multis*, i cavi per la trasmissione dei dati, i server per la loro conservazione, le reti 5g, i data center, le piattaforme digitali o gli strumenti utili per il cloud computing. L'elenco delle infrastrutture digitali è in costante aggiornamento. Sul punto si veda l'approfondimento del Ministero dell'Interno disponibile a www.interno.gov.it/mininterno/export/sites/default/it/sezioni/sala_stampa/notizie/protezione_civile/0867_2008_02_14_app_infrastrutture_critiche.html#:~:text=Le%20infrastrutture%20critiche%20sono%20le,salute%2C%20la%20sicurezza%20e%20il.

[9] Commissione europea, *EU Cybersecurity Strategy*, 1° luglio 2025, disponibile a www.digital-strategy.ec.europa.eu/it/policies/cybersecurity-policies. Nello stesso senso si è orientato anche il dialogo con la NATO, che tramite la EU-NATO *Task Force on the resilience of critical infrastructures* ha confermato tali settori come essenziali e strettamente dipendenti dalle infrastrutture critiche sia fisiche che digitali. Sul punto si veda EU-NATO Task Force, *Final Assessment Report on strengthening our resilience and protection on critical infrastructure*, press release, 29 giugno 2023, disponibile a www.ec.europa.eu/commission/presscorner/detail/en/ip_23_3564.

presente studio, influenze da parte di Stati terzi, promotori di valori che non sempre coincidono con quelli europei[10].

L'importanza delle infrastrutture critiche per il funzionamento della società ha reso le stesse sensibili non solo agli attacchi tradizionali, ma anche alle minacce ibride, volte a destabilizzare un Paese *target*[11] pur rimanendo collocate in una "zona grigia"[12], senza mai sconfinare in un vero e proprio attacco armato[13].

Il presente lavoro ha come oggetto l'analisi di una delle minacce ibride più atipiche nel panorama attuale, derivante dagli investimenti esteri diretti che, pur essenziali per un rapido ed efficace sviluppo delle infrastrutture e tecnologie critiche – le quali, in maniera del tutto peculiare, come si vedrà, non costituiscono in questo caso un *target*, bensì un mezzo –, comportano il rischio di indebite ingerenze

[10] Quest'orientamento, già espressamente adottato nella *EU Security Union Strategy* 2020-2025, è stato poi confermato nella nuova strategia denominata *ProtectEU*, che da aprile 2025 ha sostituito la precedente. Per approfondimenti si vedano comunicazione della Commissione al Parlamento europeo e al Consiglio, Settima relazione sui progressi compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza, Bruxelles, 15 maggio 2024, COM (2024) 198 definitivo; comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Protect EU*: strategia europea di sicurezza interna, Strasburgo, 1° aprile 2025, COM (2025) 148 definitivo.

[11] L'eterogeneità delle attività che compongono le minacce ibride – da cui il concetto di "*Weaponization of Everything*" – ha indotto a tentativi volti a individuarne le caratteristiche comuni che, tuttavia, si sono rivelati vani, soprattutto per l'affiorare, negli ultimi anni, di vulnerabilità e nuovi meccanismi di destabilizzazione. Tali caratteristiche sono state ravvisate: nella "negabilità plausibile", intesa come possibilità per uno Stato di negare il proprio coinvolgimento nell'attività, in modo da evitare ritorsioni; nella "asimmetria", intesa come scelta di attuare una minaccia ibrida in un dominio in cui lo Stato target mostra particolari vulnerabilità; nella "intensità" dell'attacco, intesa come impatto sullo Stato target entro una soglia che, rimanendo in una zona grigia, non sconfini in attacco armato. Per approfondimenti, si veda M. GALEOTTI, *The Weaponization of Everything*, Yale, 2023; I. CAPAUL, *A Taxonomy of Hybrid Threats*, in *CSS Analyses in Security Policy*, n. 352, dicembre 2024.

[12] Si parla al riguardo anche di comportamenti cosiddetti "sotto-soglia". Il concetto di "soglia" è stato recepito anche all'interno dell'Unione europea come elemento utile ad individuare e distinguere le minacce ibride da altre tipologie di attacco. Si veda al riguardo comunicazione congiunta della Commissione europea e Alto Rappresentante dell'Unione per gli Affari Esteri e la Politica di Sicurezza al Parlamento Europeo e al Consiglio, Quadro congiunto per contrastare le minacce ibride, la risposta dell'Unione Europea, Bruxelles, 6 aprile 2016, JOIN (2016) 18 definitivo, p. 2. Disponibile a www.eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex:52016JC0018.

[13] NATO, *Countering Hybrid Threats*, 7 maggio 2024, disponibile a www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.

economiche, geopolitiche e strategiche da Stati terzi, tali da mettere in pericolo la salvaguardia dei valori democratici[14].

Di qui, i limiti e le restrizioni che gli Stati destinatari possono applicare sugli investimenti esteri diretti e il rischio di misure protezionistiche, dovute a un potenziale uso abusivo dell'eccezione di sicurezza nazionale, cui fanno da contraltare, da un lato il tentativo, da parte dell'Unione europea, di disciplinare, tramite il regolamento (UE) 2019/452, il controllo degli investimenti esteri diretti rivolti alle infrastrutture critiche e, dall'altro, la giustiziabilità dell'eccezione di sicurezza nazionale che i Paesi possono invocare.

Il lavoro, per motivi di brevità, non si estende al tema delle minacce ibride rivolte alle infrastrutture intese come *target,* quali le minacce finalizzate ad acquisire o sfruttare illecitamente i dati, o quelle volte a perturbare o interrompere i mezzi di comunicazione e la trasmissione di dati, o, ancora, quelle con finalità di distruzione delle infrastrutture critiche[15].

Nelle conclusioni si tenterà una riflessione sull'effettivo valore degli strumenti di contrasto alle minacce ibride, adottati nell'Unione europea nel contesto delle infrastrutture digitali e tecnologie critiche, e sulle attuali competenze degli Stati.

2. *L'evoluzione della disciplina delle infrastrutture critiche nell'Unione europea*

La definizione di infrastruttura critica è fortemente influenzata dalle esigenze dei singoli Stati membri, sia perché il concetto stesso di infrastruttura critica è legato allo sviluppo e al funzionamento della società di ogni Paese, sia per motivi di sicurezza nazionale, in quanto definire critiche alcune infrastrutture piuttosto che altre – arrivando, in

[14] G. GIANNOPOULOS, H. SMITH, M. THEOCHARIDOU, *The Landscape of Hybrid Threats: A conceptual model*, in *Publications Office of the European Union*, 2021, pp. 27 e 28.

[15] Per un approfondimento sulle stesse si rinvia alla comunicazione della Commissione, del 31 marzo 2011, relativa alla protezione delle infrastrutture critiche informatizzate, realizzazione e prossime tappe: verso una sicurezza informatica mondiale, Bruxelles, COM (2011) 163 definitivo.

alcuni casi, a mantenere confidenziale la lista che le comprende – permette ai singoli Stati di circoscrivere e gestire meglio la loro tutela[16].

Tuttavia, a causa del pericolo sempre maggiore di minacce idonee a determinare impatti transfrontalieri, si è rivelata, come impellente, la necessità di un coordinamento tra gli Stati volto a individuare, prevenire e contrastare, in maniera congiunta, le stesse[17].

---

[16] P. TESSARI, K. MUTI, *Strategic or Critical Infrastructures, a way to interfere in Europe: state of play and recommendations*, in European Parliament Policy Department for External Relations and Directorate General for External Policies of the Union, 2021, pp. 4-5.

[17] Comunicazione della Commissione, del 12 dicembre 2006, relativa a un programma europeo per la protezione delle infrastrutture critiche, Bruxelles, COM (2006) 786 definitivo, p. 9. Più di recente, raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cybersicurezza su vasta scala. Riferimenti a sistemi di allarme rapidi che permettono una risposta coordinata da parte degli Stati membri possono essere individuati anche in tempi recenti*, ex multis*, per il settore digitale nel *Cyber Solidarity Act* e per le tecnologie critiche – tra cui l'IA – nell'*Economic Security Strategy*. In tal senso comunicazione della Commissione al Parlamento europeo e al Consiglio, Settima relazione sui progressi compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza, Bruxelles, 15 maggio 2024, COM (2024) 198 definitivo, pp. 4-5. Infine, va ricordato che nel 2004, al programma europeo per la protezione delle infrastrutture critiche (EPCIP) e alla rete informativa di allarme sulle infrastrutture critiche (CIWIN) si è aggiunta la costituzione dell'Agenzia Europea per la Cybersicurezza (ENISA) che ha lo scopo di prevenire, contrastare e rispondere a problemi di sicurezza della rete e dell'informazione, e di suggerire, agli Stati membri, soluzioni. Si veda, al riguardo, regolamento CE 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione e Libro Verde, del 17 novembre 2005, relativo a un Programma europeo per la protezione delle infrastrutture critiche, Bruxelles, COM (2005) 576 definitivo. Più in generale la cooperazione intracomunitaria per il contrasto alle minacce provenienti dall'esterno e la tutela delle infrastrutture critiche è stata una costante in numerose iniziative UE. Il concetto di cooperazione tra gli Stati e a livello pubblico-privato è infatti affrontato nell'*EU Cybersecurity Strategy* – strategia comune ai Paesi che condividono valori di democrazia, *rule of law* e tutela dei diritti umani e mira alla cooperazione per implementare un "*open cyberspace*"–, nel *Data Governance Act* che persegue, come si vedrà infra, i propri obiettivi tramite lo sviluppo del "data sharing" e nella nuova strategia denominata "*ProtectEU*", che prevede una cooperazione più intensa e una maggiore condivisione delle informazioni tra gli Stati Membri, sotto la supervisione dell'ENISA, nonché un rafforzamento del coordinamento nelle risposte tramite l'implementazione di un Programma UE per le infrastrutture critiche e un Programma UE per la cybersicurezza. In tal senso si veda Commissione europea, *EU Cybersecurity Strategy*, 1 luglio 2025, disponibile a www.digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy; Commissione europea, *European Data Governance Act*, 10 ottobre 2024, disponibile a www.digital-strategy.ec.europa.eu/en/policies/data-governance-act; comunicazione della Commissione al Parlamento europeo e al Consiglio, Settima relazione sui progressi

Quanto al profilo normativo, nel diritto dell'Unione europea, la direttiva 2008/114/CE[18], pur essendo rivolta alla sola tutela delle infrastrutture critiche attinenti ai settori dell'energia e dei trasporti e applicabile esclusivamente alle infrastrutture condivise da almeno due Stati membri[19], ha avuto il merito di individuare una prima, espressa e unitaria definizione di infrastruttura critica[20] che si è ulteriormente evoluta[21] con la successiva direttiva (UE) 2022/2557[22].

Quest'ultima, che ha abrogato la precedente, ha ricompreso espressamente nella definizione di infrastruttura critica anche quelle digitali[23] e ha individuato nuovi modelli di cybersicurezza, idonei ad affrontare non solo gli attacchi "tradizionali", ma anche i rischi derivanti dalle minacce ibride[24].

L'Unione europea ha riconosciuto, inoltre, il potenziale strategico dell'IA[25] per la protezione delle infrastrutture critiche, prevalentemente

compiuti nell'attuazione della strategia dell'UE per l'Unione della sicurezza, Bruxelles, 15 maggio 2024, COM (2024) 198 definitivo.

[18] Direttiva 2008/114/CE del Consiglio, dell'8 dicembre 2008, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

[19] Si veda in tal senso Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), Bruxelles, 22 giugno 2012, SWD (2012) 190 definitivo.

[20] L'art. 2 della direttiva 2008/114/CE definiva le infrastrutture critiche come «un elemento, un sistema o una parte di questo, ubicato negli Stati membri, che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini e il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni».

[21] V. *supra* nota 6.

[22] Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio.

[23] Considerando n. 5 della direttiva (UE) 2022/2557, specificato nell'Allegato della medesima direttiva.

[24] G. GONZÀLEZ FUSTER, L. JASMONTAITE, *Cybersecurity Regulation in the European Union: The Digital, the Critical and the Fundamental Rights*, in M. CHRISTEN, B. GORDIJN, M. LOI (eds.), *The Ethics of Cybersecurity, The International Library of Ethics, Law and Technology*, Cham, 2020, pp. 97-115, spec. pp. 98, 100, 103 e 113.

[25] All'inizio del nuovo millennio, tra Francia, Germania, Italia, Regno Unito, Spagna e Svezia è stato siglato il "*Framework Agreement concerning measures to facilitate the restructuring and operation of the European defence industry*", del 27 luglio 2000 (che ha poi portato all' *Implementing Arrangement on Security of Supply pursuant to the Framework Agreement* del 18 dicembre 2003), nel quale, per la prima volta, sono state indicate le attività strategiche "chiave", intese come limitate aree di capacità

ma non esclusivamente digitali[26], attraverso il monitoraggio, in tempo reale, dei rischi e la gestione predittiva degli stessi mediante l'analisi di dati utili a rilevare eventuali anomalie o vulnerabilità[27].

Di conseguenza, nell'aprile 2025, l'IA è stata riconosciuta come valido strumento di sviluppo e protezione delle infrastrutture critiche nei settori inerenti all'assistenza sanitaria, all'istruzione, all'industria e alla sostenibilità ambientale[28].

La stretta sinergia tra Intelligenza Artificiale e infrastrutture digitali deriva dalla circostanza che la prima per poter funzionare necessita delle seconde e che, oggi, la maggior parte dei dati che viaggiano attraverso le infrastrutture digitali vengono elaborati e interpretati dall'IA[29], situazione che, se da un lato aumenta il rischio di cyberattacchi, e incrementa la complessità e l'efficacia di questi ultimi[30], dall'altro

---

tecnologiche necessarie per la sicurezza e, dunque, come «attività funzionali al mantenimento o al ripristino di specifiche tecnologie nazionali considerate vitali o essenziali per la sicurezza nazionale e che pertanto risultano essere necessarie a esigenze operative essenziali e a specifici impegni nazionali». A seguito dello sviluppo delle nuove tecnologie, le aree sono state ampliate e si è posta particolare attenzione alle infrastrutture per l'energia, i trasporti, le telecomunicazioni, in quanto necessarie ad assicurare l'approvvigionamento minimo e l'operatività dei servizi pubblici essenziali e di rilevanza strategica per l'interesse e la difesa nazionale. Ancora, nel 2017, nella definizione sono stati ricompresi anche i settori ad alta intensità tecnologica e, nell'anno 2019, quelli attinenti all'IA. In tal senso Segretariato Generale degli Armamenti, Direzione Generale degli Armamenti, *Direttiva interna sugli offset*, 2 luglio 2012; F. BASSAN, *Dalla golden share al golden power: il cambio di paradigma europeo nell'intervento dello Stato sull'economia*, in *SIE*, 2014, pp. 57-80, p. 69; L. BELVISO, *Golden Power - profili di diritto amministrativo*, Torino, 2023, p. 119.

[26] Libro Bianco, del 19 febbraio 2020, sull'Intelligenza Artificiale – un approccio europeo all'eccellenza e alla fiducia, Bruxelles, COM (2020) 65 definitivo.

[27] Si veda al riguardo comunicazione della Commissione europea, del 16 dicembre 2020, congiunta al Parlamento europeo e al Consiglio – Le strategie dell'UE in materia di cybersicurezza per il decennio digitale, Bruxelles, JOIN/2020) 18 definitivo; Commissione europea: Piano Coordinato sull'intelligenza artificiale 2021, Bruxelles, 21 aprile 2021, COM (2021) 205 definitivo.

[28] Piano d'azione per il continente dell'IA, aprile 2025, disponibile a www.digital-strategy.ec.europa.eu/en/factpages/ai-continent-action-plan.

[29] M. BRKAN, M. CLAES, C. RAUCHEGGER, *European Fundamental Rights and Digitalization,* in. *MJECL*, n. 6, 2020, p. 697.

[30] Esempi in tal senso possono essere ad esempio l'uso dell'IA per hackerare veicoli a guida autonoma – per esempio droni – al fine di condurre attacchi materiali contro infrastrutture critiche fisiche quali ad esempio centrali elettriche, oppure l'utilizzo dell'IA per individuare nuove vulnerabilità o incrementare esponenzialmente il danno causato dall'azione di una singola persona. E. VIGANÒ, M. LOI, E. YANGHMAEI,

consente l'uso dell'IA anche per incrementare la sicurezza nazionale nel settore delle infrastrutture[31].

Di qui il riconoscimento dell'IA come "tecnologia critica", utile per la sicurezza dell'Unione europea e di ciascuno Stato membro e la considerazione che le minacce ibride rivolte alle infrastrutture critiche digitali possano ripercuotersi anche sulle tecnologie critiche[32].

3. *Gli investimenti esteri diretti e il rischio di ingerenze economiche e politiche da parte di Stati terzi*

Tra le possibili minacce ibride nel settore delle infrastrutture e delle tecnologie critiche, meritano particolare attenzione, in vista del potenziale lesivo per la sicurezza nazionale degli Stati *target* e per la

Cybersecurity of Critical Infrastructures, in M. CHRISTEN, B. GORDIJN, M. LOI (eds.), *op. cit.*, pp. 157-177, pp. 166-169.

[31] L'utilizzo benevolo dell'Intelligenza Artificiale, alla luce della natura spesso transfrontaliera delle infrastrutture critiche digitali, ha indotto i governi degli Stati a incrementare la cooperazione e lo scambio di informazioni[31] e, al contempo, a implementare la sicurezza e la resilienza di tali tecnologie con investimenti considerati, a tutti gli effetti, essenziali per la sicurezza nazionale.
In tal senso, il libro bianco del 2020 della Commissione Europea sottolinea come, anche da un punto di vista economico, la cooperazione in materia di IA necessiti di attori internazionali, pubblici e privati, che condividano con l'UE i valori democratici e l'attenzione per la tutela dei diritti fondamentali, prospettando, contestualmente, i rischi derivanti da rapporti economici con attori che non si allineano ai valori europei. In tal senso Libro bianco sull'Intelligenza artificiale – un approccio europeo all'eccellenza e alla fiducia, Bruxelles, 19 febbraio 2020, COM (2020) 65 definitivo; P. MEYER, *Norms of Responsible State Behaviour in Cyberspace*, in M. CHRISTEN, B. GORDIJN, M. LOI (eds.), *op. cit.*, pp. 347-360 e E. VIGANÒ, M. LOI, E. YANGHMAEI, *op. cit*., p. 170.

[32] La definizione di "tecnologia critica" è stata espressamente attribuita all'intelligenza artificiale, come si vedrà infra, nell'art. 4 par. 1 lett. b) del regolamento (UE) 2019/452. Tuttavia, il riconoscimento dell'importanza dell'Intelligenza artificiale per la tutela di settori critici connessi a tecnologie emergenti è stato più volte evidenziato anche in altre occasioni. *Ex multis* si ricordano il parere della Commissione per gli Affari Esteri, del 9 marzo 2023, destinato alla Commissione per l'industria, la ricerca e l'energia "Tecnologie critiche per la sicurezza e la difesa: situazione attuale e sfide future", (2022/2079(INI)) e la raccomandazione della Commissione, del 3 ottobre 2023, sui settori tecnologici critici per la sicurezza economica dell'UE per un'ulteriore valutazione dei rischi con gli Stati Membri, C(2023) 6689 definitiva, che riconosce una lista di dieci tecnologie critiche, inserendo l'intelligenza artificiale tra le quattro più importanti per la difesa e la sicurezza dell'Unione Europea, in quanto altamente suscettibile di presentare i rischi più sensibili e immediati legati alla sicurezza e alla fuga di segreti industriali.

difficoltà di inquadramento, gli "investimenti esteri diretti"[33] (IDE) di un Paese nel territorio di un altro, idonei a determinare indebite ingerenze di tipo politico e/o economico del primo nei confronti del secondo[34], anche attraverso aziende private[35].

Si tratta dell'unica minaccia ibrida che non considera le infrastrutture critiche come *target*, bensì come potenziale strumento.

Esplicativa, al riguardo, è la circostanza che gli investimenti esteri diretti non danneggiano *ex se* le infrastrutture critiche, né ne influenzano negativamente l'utilizzo, ma rappresentano uno dei principali strumenti volti all'implementazione e allo sviluppo delle stesse.

---

[33] La definizione di investimento estero diretto è contenuta nell'art. 2 del regolamento (UE) 2019/452, secondo cui con tale definizione si intende «un investimento di qualsiasi tipo da parte di un investitore estero inteso a stabilire o mantenere legami durevoli e diretti tra l'investitore estero e l'imprenditore o l'impresa cui è messo a disposizione il capitale al fine di esercitare un'attività economica in uno Stato membro, compresi gli investimenti che consentono una partecipazione effettiva alla gestione o al controllo di una società che esercita un'attività economica». Si è cercato, a livello UE, sia di definire un *framework* comune per l'individuazione e la gestione degli investimenti esteri diretti – che ha portato all'identificazione di criteri certi e formali, grazie ai quali un investimento estero può dirsi diretto se effettuato non solo da imprese estere, ma anche da imprese di altri Stati membri, controllate da Paesi terzi
Si parla, al riguardo, di "rapporto di filiazione" e la proposta di regolamento (COM(2024) 23 definitivo) citata richiama la definizione data dall'art. 22, par. 1, della direttiva 2013/34/UE del Parlamento Europeo e del Consiglio, del 26 giugno 2013, relativa ai bilanci d'esercizio, ai bilanci consolidati e alle relative relazioni di talune tipologie di imprese, recante modifica della direttiva 2006/43/CE del Parlamento Europeo e del Consiglio e abrogazione delle direttive 78/660/CEE del Consiglio, basata su criteri quali la maggioranza dei diritti di voto, l'influenza dominante, la partecipazione in qualità di socio o azionista o la nomina della maggioranza degli organi di governance. Sulla questione si è espressa nello stesso senso anche la Corte giust. 13 luglio 2023, C-106/22, *Xella Magyarorszàg épìtòanyagipari kft./Innovàciòs és technològiai Miniszter*.

[34] Risoluzione del Parlamento europeo, del 9 marzo 2022, sulle ingerenze straniere in tutti i processi democratici dell'Unione europea, inclusa la disinformazione, Strasburgo, 9 marzo 2022, 2020/2268(INI), parr. BA, BB, 73, 78, 79, 80, 94.

[35] La necessità di un rapido sviluppo di queste tecnologie, dovuto anche alla competizione con attori internazionali tecnologicamente più avanzati – quali Stati Uniti e Cina – determina il rischio di totale affidamento degli Stati a compagnie private straniere, con la conseguente concentrazione di potere nelle mani di privati, soggetti ad altre giurisdizioni, che può generare un'indiretta ingerenza di Paesi extra-europei, con perdita di sovranità e autonomia strategica, nonché rischi derivanti dal transito, attraverso queste infrastrutture critiche, di dati utili per la sicurezza nazionale. In tal senso J. P. DARNIS, *Space as a Key Element of Europe's Digital Sovereignity*, in *Ifri*, 2020, pp. 8, 15, 17, 19 e 20.

Un esempio di ingerenza economica e geopolitica da parte di uno Stato, derivante dagli investimenti nelle infrastrutture critiche digitali, utile per comprendere l'evoluzione della posizione dell'Unione europea sul tema, si rinviene nella *Digital Silk Road* cinese, parte della più ampia strategia denominata *Belt and Road Initiative* (BRI), che consiste nel finanziare e nell'installare infrastrutture digitali di ultima generazione nei Paesi *target* da parte della Cina.

La BRI, annunciata per la prima volta nel 2012 come un progetto dalle implicazioni prevalentemente economiche, si è poi rivelata come strumento di influenza logistica, politica e culturale nei confronti dei Paesi aderenti[36], anche in settori solo marginalmente collegati alla stessa, attraverso linee guida, raccomandazioni e *soft law* – cd. *Informal International Law* – predisposte dalla Cina che, pur non vincolanti, devono essere rispettate dai Paesi che intendono mantenere la partecipazione all'iniziativa[37].

Il progetto della Cina di creare o modernizzare, con ingenti investimenti di denaro, infrastrutture, anche digitali, nei Paesi che la BRI attraversa per raggiungere i mercati occidentali, potrebbe generare il rischio di ingerenze indebite[38], soprattutto a causa dei valori e degli standard differenti da quelli dei Paesi destinatari, che, in questo modo, indirettamente li subiscono[39], nonché dei rischi per la sicurezza

[36] L. VON HAUFF, *Towards a new quality of cooperation? The EU, China and Central Asian Security in a Multipolar Age*, in *Asia Eur. Journal*, vol. 17, 2018, pp. 195-210. Si segnala, che attualmente i Paesi membri della BRI sono circa 150, di cui 17 facenti parte dell'Unione Europea. Per un elenco dettagliato si rinvia a Countries of the Belt and Road Initiative, disponibile a greenfdc.org.

[37] D. W. P. RUITER, R. A. WESSEL, *The legal nature of Informal International Law: A Legal Theoretical Exercise*, in *Informal International Law-Making Conference*, *NIAS*, 17-19 maggio 2021; J. PAUWELYN, *Informal International Lawmaking: Framing the Concept and Research Questions*, in J. PAUWELYN, R. WESSEL, J. WOUTERS (eds.), *Informal International Lawmaking*, Oxford, 2013.

[38] Sul punto ci permettiamo di rinviare a D. VAIRA, *Trillion Dollar Baby: l'importanza strategica dell'Afghanistan nel contesto degli strumenti giuridici della Belt and Road Initiative Cinese*, in *OIDU,* 2021.

[39] Un esempio è costituito dal *China Standards 2035 Industry Policy Plan,* orientato a favorire la creazione, da parte della Cina, di standard tecnologici, in materia di Intelligenza Artificiale, Internet of Things e infrastrutture 5G, da esportare in altri Paesi attraverso la *Belt and Road Initiative*. Sul punto J. E. GRAY, *The Geopolitics of Platforms: the TikTok challenge*, in *Internet Policy Review*, 11 May 2021, p. 18; P. TRIOLO, R. GREENE, *Will China control the global internet via its Digital Silk Road?*, in *Supchina* (website), 8 maggio 2020, disponibile a

nazionale derivanti dalla possibilità, per lo Stato investitore, di incidere direttamente sul funzionamento delle infrastrutture o di utilizzare, in maniera poco trasparente[40], i dati raccolti dalle stesse[41].

www.supchina.com/2020/05/08/will-china-control-the-global-internet-via-its digital-silk-road/amp/. L'imposizione al Paese target di valori e standard attraverso accordi commerciali, e le possibili ingerenze derivanti da questi ultimi, genera il rischio di incompatibilità con altri mercati che, in casi estremi, può sfociare nella formazione di blocchi contrapposti di Stati, definita "Guerra Fredda Digitale", intesa come situazione di instabilità tra i Paesi (specialmente tra i contrapposti blocchi di Stati Uniti e Cina). S. SHACKEFORD, A. CRAIG, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, in *Stanford Journal of International Law*, vol. 50, 2014, pp. 119-184, spec. p. 125.

[40] L'art. 7 della China Intelligence Law, ad esempio, non solo obbliga i privati e le aziende a cooperare, previa richiesta, con il governo cinese e a fornire anche il supporto materiale per la trasmissione dei dati, ma impone anche il silenzio in merito all'esistenza di questi rapporti. Sul punto M. ROGERS, D. RUPPERSBERGER: *Investigative Report on the U.S. National Security issues posed by Chinese Communications Companies Huawei and ZTE*, US House of Representatives, 8 ottobre 2012. Disponibile al sito www.intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[41] Un esempio in tal senso, che ha avuto una risonanza globale, è stato costituito dal caso Huawei, accusata dell'acquisizione surrettizia per conto del governo cinese di dati tramite installazione di backdoors nelle infrastrutture, che ha portato ad una diversa risposta da parte degli Stati target, che in alcune occasioni hanno impedito all'azienda di poter operare in determinati territori, arrivando a limitarne gli investimenti nelle infrastrutture critiche digitali, non adottando però il medesimo trattamento per imprese domestiche che operavano nello stesso modo. Nello specifico, negli Stati Uniti si diffuse l'idea che l'azienda cinese, attraverso l'infrastruttura 5G, da essa stessa fornita e gestita, fosse in grado di acquisire surrettiziamente i dati personali degli utenti relativi non solo a informazioni sensibili ma anche ad abitudini, orientamenti politici, da cui derivava la rischiosa compromissione della sicurezza nazionale. Tale idea, rafforzata dalla convinzione che il governo cinese stesse adottando meccanismi di cooperazione con le proprie aziende diretti a creare un database utile a conoscere le abitudini dei cittadini americani, in modo da rafforzare e facilitare le attività di intelligence e sorveglianza, venne condivisa da altri Paesi, quali l'Australia e il Canada e, in Europa, la Francia, la Germania, la Polonia e la Repubblica Ceca. Si ritenne pertanto esservi il rischio che tutte le tecnologie che sfruttavano le reti 5G di Huawei per trasmettere i propri dati potessero generare una falla nella sicurezza in relazione a un numero indefinito di prodotti e servizi. L'azienda Huawei fu considerata un potenziale "cavallo di Troia", attraverso il quale il governo cinese avrebbe voluto e potuto inserirsi nelle infrastrutture digitali operanti non solo negli Stati Uniti, ma anche in altri Paesi per condurre attività di spionaggio con modalità difficilmente individuabili. Per approfondimenti si vedano: R. D. WILLIAMS, *Beyond Huawei and TikTok: Untangling U.S. Concerns over Chinese tech Companies and Digital Security,* Working Paper for the Penn Project on the Future of U.S. China Relations, 2021, pp. 8 e 9, disponibile al sito www.brookings.edu/articles/beyond-huawei-and-tiktok-untangling-us-concerns-over-chinese-tech-companies-and-digital-security/; E. WILKING HÄGER, C. DACKÖ,

Di qui il cambio di atteggiamento assunto nei confronti dell'iniziativa dall'Unione europea[42], i cui Stati membri, dopo un iniziale interesse condiviso dai più, si sono divisi tra quanti hanno abbandonato il progetto o posto limiti allo stesso – anche a causa della convergenza di vedute politiche tra Cina e Russia[43] – e quanti, invece, continuano ad aderirvi[44], rimanendo destinatari degli investimenti nel settore delle infrastrutture critiche, nonostante il rischio di un controllo dei *critical asset* da parte della Cina[45], e dunque di infiltrazioni strategiche e ingerenze, nocive per la coesione interna e per la sicurezza dell'UE, strettamente legata a quella dei singoli Stati che ne fanno parte[46].

Cybersecurity Law Overview, Stockholm, aprile 2017, pp. 3 e 7; K. KASKA, H. BECKVARD, T. MINÀRIK, *Huawei, 5G and China as a Security Threat*, NATO Cooperative Cyber Defence Centre of Excellence, Tallin, 2019, p. 8; M. SHOEBRIDGE, *Chinese Cyber Espionage and the National Security Risks Huawei Poses to 5g Network*, in *Macdonald-Lauriel Institute Publication*, novembre 2018, p. 2; M. ROGERS, D. RUPPERSBERGER, *Investigative Report on the U.S. National Security issues posed by Chinese Communications Companies Huawei and ZTE*, US House of Representatives, 8 October 2012 disponibile al sito www.intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[42] G. MOHAN, *Europe's Response to the Belt and Road Initiative*, in *The German Marshall Fund of the United States*, n. 14, 2018, pp. 1-6, spec. p. 2.

[43] L'idea di una "*partnership with no limits*" avanzata nel 2022 dalla Cina pochi giorni prima dell'invasione russa dell'Ucraina ha poi trovato, nei successivi anni, diverse conferme. Si veda in tal senso *Moscow-Beijing partnership has 'no limits'*, in *Reuters*, 4 febbraio 2022 e *China's Xi affirms 'no limits' partnership with Putin in call on Ukraine war anniversary*, in *Reuters*, 24 February 2025.

[44] I Paesi dell'Unione Europea che si sono dimostrati scettici verso la BRI sono prevalentemente quelli collocati ad occidente – tra cui l'Italia, che nel 2023 ha abbandonato il progetto – e a nord del continente, nonostante anche alcuni Paesi centro-orientali come la Repubblica Ceca, la Slovacchia, l'Estonia, la Lettonia e la Lituania abbiano abbandonato il progetto. I Paesi che invece sono favorevoli alla BRI risultano prevalentemente collocati nella zona balcanica, tra cui si segnala la Croazia, che ha ricevuto numerosi investimenti in infrastrutture critiche dalla Cina negli ultimi anni. Sul punto N. CASARINI, *The future of the Belt and Road in Europe: How China's Connectivity Project is Being Reconfigured across the Continent – and what it means for the Euro-Atlantic Alliance*, in *IAI Papers*, February 2024, pp. 1-22, spec. pp. 10 e 11.

[45] J. KOCIUBINSKI, *The Eu Framework for the Screening of Foreign Direct Investment as a Response to the Belt and Road Initiative in the Post-COVID Era*, in *Studies in European Affairs*, vol. 3, 2023, pp. 87-104, spec. pp. 87-89.

[46] L'Unione europea pur non essendo titolare di un proprio ordine pubblico – distinto da quello degli Stati membri – o di una sicurezza sovranazionale, negli ultimi anni ha sollecitato le Istituzioni a considerare la possibilità di uniformare o, quantomeno, armonizzare il concetto di sicurezza, al fine di garantire una risposta unitaria da parte degli Stati Membri, stimolando le stesse ad attenzionare le tecnologie critiche anche a

La necessità di bilanciare la tutela della sicurezza nazionale con la libera circolazione dei capitali[47], ha indotto l'Unione europea a promuovere un controllo armonizzato degli investimenti esteri diretti, adottando il regolamento (UE) 2019/452.

4. *I meccanismi di controllo degli investimenti esteri diretti alla luce del regolamento (UE) 2019/452*

La difficoltà di individuare una disciplina unitaria in materia di restrizioni agli investimenti esteri diretti, deriva principalmente dalla riluttanza con la quale gli Stati cedono le prerogative in settori rilevanti per la sicurezza nazionale, quale quello delle infrastrutture critiche.

A livello europeo, infatti, se da un lato l'art. 63 TFUE vieta le restrizioni al libero movimento di capitali tra gli Stati membri e tra questi ultimi e i Paesi terzi, dall'altro l'art. 4 TUE attribuisce espressamente competenza esclusiva agli Stati in materia di sicurezza nazionale.

Ciò – in uno con la circostanza che le scelte attinenti alla sicurezza nazionale spesso sono influenzate da motivi politici o interessi propri del singolo Stato, nonché caratterizzate da una confidenzialità delle informazioni che rende complesso alle controparti opporsi[48] – ha determinato, in tempi recenti, lo sviluppo diversificato non solo del concetto di sicurezza nazionale, ma anche dell'importanza da attribuire

livello unionale. La proposta, avanzata dalla Commissione, di regolamento del Parlamento europeo e del Consiglio, relativo al controllo degli investimenti esteri nell'Unione, che abroga il regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 24 gennaio 2024 (COM(2024) 23 definitivo) cita più volte il concetto di ordine pubblico e sicurezza con riferimento all'Unione europea, dimostrando la volontà di indirizzarsi in tale direzione e prevedendo, all'art. 13, che gli investimenti esteri incidenti su infrastrutture critiche o tecnologie critiche debbano essere sottoposti a controlli ulteriori in quanto potenzialmente incisivi sull'ordine pubblico e la sicurezza. Diversamente, nell'ambito del Consiglio d'Europa, un concetto di ordine pubblico delle democrazie esiste sin dagli anni '60, ed è finalizzato a salvaguardare l'eredità comune degli Stati sottoscrittori della CEDU in materia di tradizioni politiche, ideali, libertà e rule of law. In tal senso Commissione EDU, 11 gennaio 1961, ric. n. 788/60, *Austria/Italia*, p. 18.

[47] *Ibidem*, pp. 93-95.

[48] Z. VIG, *The Regulation of Screening of Foreign Direct Investments in the European Union*, in *Pro Futuro: A Jovo Nemzedekek Joga*, n. 4, 2020, pp. 9-24, p. 17.

agli investimenti stranieri e ai diversi meccanismi di *screening* degli stessi[49].

Ne è derivata, quindi, la tendenza ad attribuire allo Stato ospitante un ampio controllo sugli investimenti esteri diretti[50], tendenza che, nel corso degli anni, ha consentito lo sviluppo di normative nazionali tra loro eterogenee[51], che tali sono rimaste anche dopo l'interesse rivolto dall'Unione europea al settore delle infrastrutture critiche e delle tecnologie critiche.

Si assiste, pertanto, al permanere di una prerogativa degli Stati sul controllo degli investimenti esteri diretti sul proprio territorio, sino al punto da poterli inibire in tutto o in parte, così da mantenere il monopolio sui settori sensibili o, comunque, il controllo sui meccanismi per individuare gli stessi[52].

Nonostante lo stretto collegamento tra la libera circolazione dei capitali e gli investimenti esteri diretti, in passato si è registrata una dicotomia tra le competenze attribuite all'Unione europea e quelle attribuite agli Stati membri, solo parzialmente colmata.

Negli anni '70, la Corte di giustizia delle Comunità europee (attualmente Corte di giustizia dell'Unione europea), aveva esteso, in via interpretativa, la competenza delle Istituzioni europee in materia di politica commerciale anche ai rapporti con Stati terzi[53].

Successivamente, il Trattato di Maastricht – che ha incluso la materia degli investimenti nella politica commerciale[54] – e l'adesione all'Organizzazione Mondiale del Commercio hanno ampliato la competenza dell'Unione europea in materia di investimenti esteri diretti, lasciando tuttavia agli Stati membri prerogative in merito all'apertura dei

[49] A. G. DESSIE, *op. cit*., pp. 23, 44.
[50] *Ibidem*, p. 26.
[51] Una comparazione tra le normative nazionali, ad esempio, in materia di *screening* degli investimenti è stata fatta da Z. VIG, *op. cit.*, pp. 13-16.
[52] UNCTAD, *World Investment Report 2016: Investor-Nationality Policy Challenges*, 2016, pp. 97 ss. Il report è disponibile al sito www.unctad.org/system/files/official-document/wir2016_en.pdf.
[53] Corte giust. 31 marzo 1971, 22/70, *Commissione/Consiglio*. Successivamente, nello stesso senso, 5 novembre 2002, C-467/98, C-468/98, C-472/98, C-475/98 e C-476/98, *Commissione/ Danimarca, Svezia, Belgio, Lussemburgo, Austria e Germania*.
[54] Ad oggi, gli investimenti esteri diretti rientrano a pieno titolo nella politica commerciale comune, ai sensi dell'art. 3, par. 1, lett. 3) TFUE. Questa previsione è espressamente richiamata anche dal considerando n. 6 del regolamento (UE) 2019/452.

flussi di investimenti nei confini nazionali, alla luce delle esigenze di sicurezza di ciascuno[55].

A seguito dell'aumento degli investimenti esteri diretti, da parte della Cina e della Russia, negli Stati membri[56], si è osservata un'accelerazione della politica europea di controllo, culminata con l'adozione del regolamento (UE) 2019/452, finalizzato: alla procedimentalizzazione di meccanismi di controllo per gli investimenti esteri, a garanzia di una maggiore trasparenza non solo per gli Stati membri, ma anche per gli Stati terzi che intendono operare nell'Unione europea; all'individuazione di criteri oggettivi utili a rintracciare le operazioni degli investitori esteri che devono essere interdette o escluse dagli Stati membri; alla definizione di meccanismi di cooperazione tra le Istituzioni e gli Stati membri e tra questi ultimi; all'istituzionalizzazione di un sistema di controllo attraverso l'armonizzazione dei controlli in corso; alla progettazione di programmi di interesse per l'Unione europea[57].

[55] L'Unione europea pur non essendo titolare di un proprio ordine pubblico – distinto da quello degli Stati membri – o di una sicurezza sovranazionale, negli ultimi anni ha sollecitato le istituzioni a considerare la possibilità di uniformare o, quantomeno, armonizzare il concetto di sicurezza, al fine di garantire una risposta unitaria da parte degli Stati membri, stimolando le stesse ad attenzionare le tecnologie critiche anche a livello unionale. La proposta, avanzata dalla Commissione, di regolamento del Parlamento europeo e del Consiglio relativo al controllo degli investimenti esteri nell'Unione, che abroga il regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 24 gennaio 2024 (COM(2024) 23 definitivo) cita più volte il concetto di ordine pubblico e sicurezza con riferimento all'Unione europea, dimostrando la volontà di indirizzarsi in tale direzione e prevedendo, all'art. 13, che gli investimenti esteri incidenti su infrastrutture critiche o tecnologie critiche debbano essere sottoposti a controlli ulteriori in quanto potenzialmente incisivi sull'ordine pubblico e la sicurezza. Diversamente, nell'ambito del Consiglio d'Europa, un concetto di ordine pubblico delle democrazie esiste sin dagli anni '60, ed è finalizzato a salvaguardare l'eredità comune degli Stati sottoscrittori della CEDU in materia di tradizioni politiche, ideali, libertà e rule of law. In tal senso Commissione EDU, 11 gennaio 1961, ric. n. 788/60, *Australia/Italia*, p. 18.

[56] Secondo il Comitato economico e sociale europeo, nel parere – proposta di regolamento del Parlamento europeo e del Consiglio che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione europea, COM (2017) 487 definitivo – 2017/0224, gli investimenti cinesi nei territori europei sono aumentati di circa dieci volte rispetto al 2009, mentre gli investimenti europei in Cina sono diminuiti del 25%.

[57] Considerando n. 7 del regolamento (UE) 2019/452.

Il regolamento individua una lista meramente esemplificativa[58] di settori sensibili, rilevanti sotto un profilo strategico per la sicurezza nazionale e l'ordine pubblico[59], tra cui le infrastrutture critiche, anche digitali, e le tecnologie critiche, quali l'Intelligenza Artificiale, allo scopo di armonizzare i diversi meccanismi di *screening* già esistenti a livello nazionale e di mediare tra il rischio di erosione della sovranità nazionale in materia di sicurezza, attribuita alla competenza esclusiva degli Stati ai sensi dell'art. 4, par. 2, TUE, e quello di un'incontrollata applicazione, in aperto contrasto con il principio di libera circolazione dei capitali che l'UE promuove[60], di misure surrettiziamente economiche e protezionistiche da parte dei Paesi[61].

A tal fine, la Commissione, ribadito agli Stati membri l'invito a predisporre meccanismi nazionali di controllo degli investimenti esteri diretti, si è impegnata a promuovere l'armonizzazione dei processi legislativi nazionali sul tema[62].

Dalla lettura del regolamento risulta, per un verso, che – analogamente a quanto previsto dall'art. 4, par. 2, TUE, che attribuisce discrezionalità nell'individuare gli interessi essenziali di sicurezza[63] da tutelare in virtù dell'art. 346 TFUE – la decisione sul *se* e *in che misura* controllare un investimento estero diretto rimane nell'esclusiva competenza degli Stati membri[64]; per altro verso che, qualora gli Stati decidano di adottare meccanismi volti a limitare gli investimenti esteri

[58] La non tassatività della lista ha permesso ai legislatori nazionali di estendere in taluni casi il perimetro applicativo del regolamento. Sul punto D. GALLO, *Sovranità (europea?) e controllo degli investimenti esteri*, in questa *Rivista*, 2022, pp. 194-212.
[59] Considerando n. 19 e art. 4 del regolamento (UE) 2019/452.
[60] *Ivi*, considerando n. 2.
[61] F. MARCONI, *Regolamento (UE) 2019/452 e meccanismi di controllo degli investimenti esteri diretti: il vaglio europeo sul caso ungherese*, in *FSJ*, n. 1, 2023, pp. 181-205, pp. 192-193.
[62] Relazione della Commissione al Parlamento europeo e al Consiglio, *Prima relazione annuale sul controllo degli investimenti esteri diretti nell'Unione*, COM (2021) 714 definitiva e *Seconda relazione annuale sul controllo degli investimenti esteri diretti nell'Unione*, SWD (2022) 219 definitivo.
[63] A tal proposito occorre evidenziare che, pur se il considerando n. 13 del regolamento attribuisce sia agli Stati membri che alla Commissione la facoltà di analizzare i fattori pertinenti e le circostanze per valutare se un investimento estero diretto possa o meno incidere sulla sicurezza o l'ordine pubblico, il successivo considerando n. 17 ribadisce la competenza esclusiva degli Stati nella decisione in merito alle misure da applicare.
[64] Questa previsione emerge dalla lettura congiunta dell'art. 1, par. 3 e dell'ultima parte del considerando n. 8 del regolamento (UE) 2019/452.

diretti, dovranno rispettare gli obblighi di trasparenza, orientati a garantire un trattamento non discriminatorio verso gli investitori[65] e quelli di dotarsi di meccanismi di *enforcement,* e garantire, ai destinatari delle misure restrittive, la possibilità di impugnare le stesse là dove considerate sproporzionate o ingiustificate[66].

Il regolamento (UE) 2019/452, riconosciuta la competenza esclusiva degli Stati membri sul controllo degli investimenti, si concentra prevalentemente su aspetti di natura procedurale[67], incrementando la cooperazione tra gli Stati e le Istituzioni europee, attraverso i meccanismi previsti dagli articoli 6, 7, 8 e 9, relativi, rispettivamente, agli investimenti oggetto di un controllo già in corso, a quelli per i quali il procedimento di controllo non è ancora stato avviato[68], a quelli idonei ad incidere su progetti o programmi di particolare interesse per l'Unione[69], ai contenuti e alle modalità relativi agli obblighi di informazione.

Le norme citate stabiliscono, in primo luogo, l'obbligo di notifica verso la Commissione e gli altri Stati membri da parte dello Stato destinatario dell'IDE[70], notifica che deve contenere tutte le informazioni utili per consentire ai destinatari di valutare l'impatto dell'investimento estero diretto e di formulare osservazioni – nel caso di Stati membri – o emettere un parere – nel caso della Commissione –[71], indirizzato allo

[65] Considerando nn. 7 e 8 e art. 3, par. 2, del regolamento (UE) 2019/452.
[66] *Ivi*, art. 3, par. 5.
[67] *Ivi*, art. 1.
[68] *Ivi*, considerando n. 16.
[69] *Ivi*, considerando n. 19.
[70] Tale notifica può riguardare sia gli investimenti oggetto di un controllo in corso da parte di uno Stato nel proprio territorio, che gli investimenti diretti in un altro Stato e non ancora oggetto di controllo, che lo Stato membro ritiene possano incidere sulla sicurezza o ordine pubblico nel proprio territorio. Artt. 6, par. 1 e 7, par. 1, del regolamento (UE) 2019/452.
[71] Il contenuto delle informazioni oggetto di notifica è indicato dall'art. 8, par. 2 e riguarda gli assetti proprietari degli investitori esteri, il valore approssimativo dell'investimento, i prodotti, servizi o attività cui l'investimento è diretto e la fonte del finanziamento.

Stato destinatario dell'investimento e titolare del controllo[72], che deve essere tenuto da questo in "debita considerazione"[73].

Diversamente, nell'ipotesi di investimento idoneo a incidere su programmi o progetti di interesse per l'Unione, il parere deve essere tenuto nella "massima considerazione"[74], così attribuendo, di fatto, alla Commissione il ruolo di co-decisore in merito alla restrizione dell'investimento estero, risultando arduo per lo Stato motivare l'adozione di un provvedimento divergente da quanto suggerito dalla Commissione[75].

Cosa potrebbe accadere nel caso in cui lo Stato *target* disattenda, senza adeguate motivazioni, i pareri della Commissione?

Ad avviso della dottrina[76], nel caso in cui il parere della Commissione sia disatteso, l'unica forma di tutela – neanche considerata particolarmente efficace nel caso di specie – che l'istituzione può esercitare è rappresentata dalla procedura di infrazione, di cui agli artt. 258 e 259 TFUE[77], in quanto alla Commissione, a differenza dei singoli

[72] Il parere espresso dalla Commissione sul meccanismo di controllo applicato dallo Stato rispecchia il controllo previsto dall'art. 348 TFUE da parte della Commissione, in quanto custode dei Trattati, in merito alle condizioni alle quali le eccezioni di sicurezza nazionale vengono apposte, così da evitare un'applicazione surrettiziamente economica delle stesse, finalizzata ad alterare la concorrenza nel mercato interno a vantaggio delle imprese domestiche, in violazione degli obblighi imposti dall'OMC, che l'Unione europea e gli Stati membri sono tenuti a rispettare.

[73] Considerando n. 17 del regolamento (UE) 2019/452.

[74] *Ivi*, considerando n. 19.

[75] A. SANDULLI, *La febbre del Golden Power*, in *RTDP*, 2022, p. 764.

[76] Sul punto G. D'AGNONE, *Il regolamento 2019/452 che istituisce un quadro per lo screening degli investimenti esteri diretti: uno strumento in evoluzione*, in questa *Rivista*, 24 ottobre 2024, p. 15; D. GALLO, *Sovranità (europea?) e controllo degli investimenti esteri*, in *Atti Convegni AISDUE*, 2022, p. 202; T. VERELLEN, *When Integration by Stealth Meets Public Security: the EU foreign Direct Investment Screening Regulation*, in *LIEI*, vol. 48, n. 1, 2021, pp. 19-42, spec. p. 36.

[77] Procedure di infrazione si sono avute verso gli Stati già relativamente al precedente strumento delle *Golden Shares*. *Ex multis* v. Corte giust. 23 maggio 2000, C-58/99, *Commissione/Italia*; 26 marzo 2009, C-326/07, *Commissione/Italia*. Per un approfondimento sul punto si vedano C. SAN MAURO, *La disciplina delle "Golden Shares" dopo la sentenza della Corte di Giustizia C-326/07*, in *Concorrenza e mercato*, n. 2, 2010, pp. 409-432; M. SALERNO, *Sulle golden shares l'Italia è costretta ad un nuovo passo indietro: troppa discrezionalità nell'esercizio dei poteri speciali*, in *DPCE*, 2009, p. 1358 ss.; I. DE MAURO, *La necessaria oggettività per l'esercizio dei poteri previsti dalla golden share*, in *GCOM*, n. 4, 2009, pp. 640 ss.

Stati, non è attribuito il potere di *enforcement* relativamente agli investimenti esteri diretti[78].

In conclusione, l'analisi del regolamento evidenzia che l'Unione europea, la cui normativa è volta all'armonizzazione dei controlli, si sta orientando verso l'uniformazione della disciplina, nel tentativo di recuperare terreno in un settore tradizionalmente presidiato dagli Stati membri, focalizzando tuttavia l'attenzione su aspetti meramente procedurali, senza sconfinare in quelli di natura sostanziale, nonostante la possibilità di attingere dalla disciplina dettata da legislazioni nazionali in materia[79].

5. *L'eccezione di sicurezza nazionale e la sua giustiziabilità*

Accanto ai meccanismi di controllo, di cui al regolamento (UE) 2019/452, che gli Stati utilizzano per valutare l'impatto di un investimento estero diretto sulle infrastrutture critiche, un altro efficace strumento di tutela è rappresentato dall'eccezione di sicurezza nazionale, che consente allo Stato che la invoca di porre limiti alla liberalizzazione degli scambi per salvaguardare interessi ritenuti essenziali per la sicurezza nazionale[80].

[78] G. D'AGNONE, *op. cit*., pp. 21-22.

[79] *Ex multis*, un esempio è dato dallo strumento dei *Golden Powers* previsti nell'ordinamento italiano. Meccanismi di controllo degli investimenti sono comunque presenti, seppur con alcune differenze, in quasi tutti gli Stati membri dell'Unione europea. Per un approfondimento al riguardo si veda Senato della Repubblica – Ufficio Valutazione Impatto, Poteri Speciali – Dalla *Golden Share* al *Golden Power*: in che modo i governi (tra cui il nostro) controllano le imprese nazionali strategiche, luglio 2023, disponibile a www.senato.it/application/xmanager/projects/leg19/attachments/documento/files/000/112/523/DA28_Focus_Golden_power.pdf. Sul punto si veda anche G. SCARCHILLO, *Golden Powers e settori strategici nella prospettiva europea: il caso Huawei. Un primo commento al regolamento (UE) 2019/452 sul controllo degli investimenti esteri diretti*, in *DCI*, n. 2, 2020, pp. 569-601, p. 600.

[80] P. DELIMATSIS, T. COTTIER in R. WOLFRUM, P.T. STOLL (eds.), *Max Planck Commentaries on World Trade Law*, vol. 6, Leiden-Boston, 2008, pp. 329-348.

Inserita in numerosi accordi internazionali, sia multilaterali[81] che bilaterali[82], e recepita, a livello europeo, dai citati articoli 346 e 347 TFUE, l'eccezione, inizialmente sollevata in ambiti strettamente legati al settore militare e a quello della difesa dello Stato, è stata via via estesa ad altri settori commerciali sino ad arrivare al settore degli investimenti esteri diretti[83].

Non a caso, la stessa è richiamata espressamente dal considerando n. 35 del regolamento (UE) 2019/452 che, nel citare l'art. XIV-*bis* GATS, evoca la possibilità per gli Stati di sollevare l'eccezione anche nel settore della libera circolazione dei capitali e degli investimenti esteri diretti.

---

[81] Il regolamento (UE) 2019/452, ribadendo all'art. 1 par. 2 la competenza esclusiva degli Stati in materia di sicurezza nazionale, nel considerando n. 35 richiama espressamente l'art. XIV lett. a) e l'art. XIV-*bis* del GATS, così prevedendo per gli Stati la possibilità di limitare gli investimenti esteri nel caso in cui ritengano che questi possano ledere la propria sicurezza nazionale, nel rispetto, tuttavia, di un bilanciamento con l'esigenza di libera circolazione di beni, servizi e capitali nel mercato interno volto a scongiurare l'ipotesi di protezionismo dissimulato.
Per un approfondimento in merito all'eccezione di sicurezza nazionale contenuta negli accordi multilaterali citati si veda R. P. ALFORD, *The Self-Judging WTO Security Exception*, in *Utah Law Rev.*, n. 687, 2011, pp. 697-759.

[82] Sul punto, un recente studio dell'UNCTAD ha dimostrato un aumento della presenza della clausola di eccezione relativa alla sicurezza nazionale negli accordi bilaterali, sul modello delle clausole inserite nel GATT e nel GATS. Nello specifico, l'eccezione di sicurezza nazionale è stata richiamata da numerosissimi "Model BITs", utilizzabili dai Paesi che li predispongono come modello orientativo per tutti gli accordi di investimento stipulati con Paesi terzi. *Ex multis*, l'eccezione è presente nei seguenti modelli: Art. 16 Italy Model BITs 2024 e 2022, nell'eccezione di sicurezza nazionale dell'EU Model BIT 2023, nell'Art. 13 del Bulgaria Model BIT 2023, nell'art. 22 del Canada Model BIT 2021, nell'art.14 dello Slovakia Model BIT 2019, nell'art.13 del Czech Republic Model BIT 2016, nell'art. 61 del Russian Federation Model BIT 2016, nell'art. 5 del Azerbaijan Model BIT 2016, nell'art. 33 dell'India Model BIT 2015 e nell'art.12 della sua precedente versione 2003, nell'art. 26 del Norway Model BIT 2015, nell'art.11 del Serbia Model BIT 2014, nell'art. 25.4 del SADC Model BIT 2012, nell'art. 18 dello United States Model BITs 2012 e 2004 e nell'art.14 delle versionic1998 e 1994, nell'art.4 del Turkey Model BIT 2009, nell'art.10 del Macedonia (precedentemente Yugoslav Republic) Model BIT 2009, nell'art.10 del Ghana Model BIT 2008, nell'art.2.3 del Colombia Model BIT 2008, nell'art.26 del Norway Model BIT 2007, nell'art.10.4 del Canada Model BIT 2004, nell'art. 7 dell'Israel Model BIT 2003, nell'art.12 del Kenya Model BIT 2003, nell'art.14 del Finland Model BIT 2001, nell'art.5 del Peru Model BIT 2000, nell'art.5.2 del Belgio-Luxembourg Model BIT, nell'art.4 del Senegal Model BIT, e nell'art.5.2 del Sudan Model BIT. I relativi testi sono disponibili al sito www.investmentpolicy.unctad.org/international-investment-agreements/model-agreements.

[83] G. SCARCHILLO, *op. cit.*, p. 592.

L'eccezione di sicurezza nazionale, nei termini stabiliti dai trattati multilaterali e recepiti dal diritto UE, soffre di ampia discrezionalità applicativa[84], in quanto prevede per ciascuno Stato la possibilità di limitare la liberalizzazione degli scambi di beni e servizi e la circolazione di capitali – tra i quali rientrano investimenti esteri diretti – attraverso le misure che «ritenga necessarie» per la tutela degli interessi essenziali alla propria sicurezza[85].

Caratterizzata da rapidità applicativa, la citata eccezione offre il fianco a rischi di abuso[86] soprattutto nel settore delle infrastrutture critiche digitali, nel quale la linea di demarcazione tra interessi economici – rispetto ai quali la stessa non è applicabile – e interessi di sicurezza – che ne consentono l'applicazione – è estremamente labile[87].

È quindi necessaria la previsione di un sistema che garantisca la tutela della sicurezza nazionale ma, al contempo, incentivi gli investimenti esteri diretti, così evitando che l'indiscriminata limitazione degli stessi induca gli Stati terzi a dislocarli altrove o rafforzi la concorrenza sleale[88].

---

[84] Va precisato, tuttavia, che esistono diversi orientamenti circa la portata effettiva di questa discrezionalità: a coloro che ritengono la norma pienamente *self-judging*, si contrappongono quanti reputano che la discrezionalità sia mitigata dall'obbligo di agire in buona fede e quanti, ulteriormente, considerando le condizioni applicative delle misure come suscettibili di *judicial review*. Per un approfondimento sul punto si veda R. P. ALFORD, *op. cit.*, p. 704. Sulla discrezionalità applicativa dell'eccezione di sicurezza nazionale da parte degli Stati si veda anche J.B. HEATH, *The New National Security Challenge to the Economic Order*, in *The Yale Law Journal*, vol. 129, 2020, pp. 1020-1098, pp. 1071-1072.

[85] M. SORNARAJAH, *The International Law on Foreign Investment*, Cambridge, 2018, p. 77.

[86] A. G. DESSIE, *A Scrutiny of Foreign Direct Investment Regulation in Light of Evolving National Security Concerns in International Investment Law*, in *Jimma University Journal of Law*, vol. 13, 2021, pp. 19- 46, p. 23. Nello stesso senso J. MA, *International Investment and National Security Review*, in *Vanderbilt Journal of Transnational Law*, n. 52, 2019, p. 899.

[87] R. BHALA, *National Security and International Trade Law: What the GATT Says, and what the United States Does Symposium on Linkage as Phenomenon: An Interdisciplinary Approach*, in *University of Pennsylvania Journal of International Law*, vol. 19, pp. 263-317, spec. p. 273.

[88] F. PRENESTINI, *Golden Power e meccanismi societari di difesa dall'acquisto del controllo*, in *federalismi.it*, n. 33, 2022, p. 72; D. ZAOTTINI, *Golden Power. La disciplina dei poteri speciali del governo*, in Documento di Analisi n. 28, Senato della Repubblica, 2023.

A tal fine, al netto di quanto previsto dal citato Regolamento, si è prospettata la possibilità di limitare l'eccezione di sicurezza nazionale[89] prevedendo la giustiziabilità della stessa alla luce dei principi di proporzionalità[90] e buona fede[91] e della connessa esigenza di bilanciamento tra l'interesse essenziale di sicurezza e la liberalizzazione del mercato[92].

Si tratta di una previsione che incontra non poche difficoltà in quanto nel settore delle infrastrutture critiche – a differenza di quanto avviene nel settore della difesa in cui è necessario dimostrare la sussistenza di un grave pregiudizio per gli interessi essenziali dello Stato –, per invocare l'eccezione di sicurezza nazionale è sufficiente che si verifichi una qualsiasi evenienza che possa rappresentare una minaccia per il

[89] Le difficoltà riscontrate nell'operazione di bilanciamento tra le esigenze di sicurezza nazionale e le contrapposte esigenze di liberalizzazione del mercato hanno sollevato dubbi applicativi anche a livello internazionale. La contrapposizione ha visto da un lato Paesi che sottolineavano la natura totalmente *self-judging* dell'eccezione di sicurezza nazionale, derivante dall'idea che la locuzione "interessi che lo Stato considera necessari" andasse a sottolineare la totale autonomia del paese nell'individuazione degli stessi, anche alla luce della natura a volte strettamente politica di tali interessi e, dall'altro, Paesi che ritenevano la incondizionata discrezionalità come contrastante con quanto stabilito dall'art. 23.1 DSU – secondo cui gli Stati membri dell'OMC hanno diritto alla riparazione dei danni causati da comportamenti che violano gli obblighi OMC –, nonché con i principi di prevedibilità e trasparenza previsti dall'OMC e con l'art. 31 della Convenzione di Vienna sul diritto dei trattati, sottolineando quindi la necessità di una giustiziabilità dell'eccezione. Sul punto OMC, Report of the Panel, 5 aprile 2019, WT/DS512/R, *Russia – Measures concerning Traffic in Transit*, par. 7, 54-56; 7.80.

[90] Giova precisare che il rispetto del principio di proporzionalità richiede una valutazione caso per caso. J. MA, *International Investment and National Security Review*, in *Vanderbilt Journal of Transnational Law*, vol. 52, n. 4, ottobre 2019, pp. 819-948, p. 934.

[91] Il principio di buona fede è basato sugli articoli 26 e 31(1) della Convenzione di Vienna sul diritto dei trattati, che richiedono agli Stati di adempiere ai propri obblighi secondo buona fede e interpretare i trattati in buona fede – vale a dire seguendo il significato ordinario attribuibile ai termini utilizzati nel trattato nel loro contesto e alla luce degli obiettivi e finalità dello stesso – Sul punto R. KOLB, *Principles as Sources of International Law (with special reference to good faith)*, in *Netherlands International Law Review*, vol. 53, 2006, p. 18.

[92] La Corte di giustizia, in più occasioni, ha ribadito che l'eccezione di sicurezza nazionale deve essere applicata in maniera delimitata e non estensiva e che gli Stati membri che intendono avvalersene devono provare che la sua invocazione è necessaria e proporzionata alla tutela degli interessi essenziali di sicurezza. Corte giust. 16 settembre 1999, C-414/97, *Commissione/Spagna*, punto 21, 22; 15 maggio 1986, 222/84, *Johnston*, punto 26.

funzionamento della rete o degli impianti[93], così da consentire più ampia libertà nell'applicare restrizioni agli investimenti esteri diretti.

Il rapporto tra investimenti esteri diretti nelle infrastrutture critiche e l'eccezione di sicurezza nazionale, pur non rappresentando un tema nuovo per la Corte di giustizia dell'Unione europea[94], è stato da questa affrontato solo trasversalmente.

Sul punto si ricorda, ad esempio, la recente pronuncia[95] relativa ai limiti alla libertà di stabilimento per imprese che operano in settori critici, nella quale la Corte, nonostante non si sia occupata in maniera specifica di investimenti esteri diretti, ha affermato che le restrizioni alla libera circolazione dei capitali nei settori critici – in cui vengono ricomprese anche le infrastrutture critiche[96], incluse quelle digitali – non possono essere giustificate da fini puramente economici e che, sebbene gli Stati vantino discrezionalità nell'individuare gli interessi essenziali di sicurezza da proteggere, questi ultimi devono essere intesi in senso restrittivo «in modo che la loro portata non [possa] essere determinata unilateralmente da ciascuno Stato membro senza il controllo delle Istituzioni dell'Unione»[97].

Il rapporto tra investimenti esteri diretti e sicurezza nazionale è stato affrontato anche dagli organi di risoluzione delle controversie del Centro Internazionale per il regolamento delle controversie relative ad

[93] J. SPORTOLETTI, *Il Golden Power, tra compatibilità europea e prospettive di riforma*, in *Nomos*, n. 3, 2023, p. 11.

[94] L'esigenza di orientamenti per bilanciare le contrapposte esigenze in materia di infrastrutture critiche era emersa già nel periodo antecedente i *Golden Powers*, con i *Golden Shares*. Si è assistito ad una serie di sentenze che hanno previsto la possibilità per gli Stati, a certe condizioni, di limitare gli investimenti esteri diretti o sottoporli a preventiva autorizzazione. Tra queste si segnalano: Corte giust. 4 giugno 2022, C-483/99, *Commissione/Francia*; 4 giugno 2022, C-503/99, *Commissione/Belgio*; 4 giugno 2022, C-367/98, *Commissione/Portogallo*; 13 maggio 2003, C-98/01, *Commissione/Regno Unito*; 13 maggio 2003, C-463/00, *Commissione/Spagna*; 2 giugno 2005, C-174/04, *Commissione/Italia*; 28 settembre 2006, C-282/04 e C-283/04, *Commissione/Olanda*.

[95] *Xella Magyarország épìtòanyagipari kft./Innovàciòs és technològiai Miniszter*, sopra citata.

[96] *Ivi*, punto 69.

[97] *Ivi*, punti 63-66.

Investimenti (ICSID), cui aderisce la quasi totalità dei singoli Stati membri dell'Unione europea[98].

In ambito ICSID, la giustiziabilità dell'eccezione di sicurezza nazionale è passata da un approccio c.d. *only way*, secondo il quale lo Stato deve dimostrare che l'eccezione adottata sia l'unico modo per affrontare la situazione emergenziale[99], a un approccio c.d. *less restrictive alternative*, secondo cui non è obbligatorio dimostrare l'assoluta indispensabilità dell'eccezione, ma è sufficiente, nel rapporto costi-benefici, che essa rappresenti la misura meno restrittiva tra le opzioni ragionevolmente disponibili per raggiungere l'obiettivo[100].

6. *Conclusioni*

Le minacce ibride, incidendo sul corretto funzionamento delle tecnologie digitali, sono considerate attività volte a destabilizzare i Paesi *target* e, pur non raggiungendo mai la soglia di un attacco armato, possono essere ricondotte al concetto di grave tensione internazionale[101] che, in via residuale rispetto alle altre ipotesi previste dagli artt. 346 e 347 TFUE, nonché dagli artt. XIV-*bis* GATS e XXI GATT[102], consente agli Stati di limitare o bloccare lo scambio con Paesi terzi di beni, servizi e, come sottolineato nel presente elaborato, anche capitali.

---

[98] Le regole dell'arbitrato ICSID sono state incorporate negli accordi di scambio e investimenti conclusi dall'Unione europea in tema di protezione degli investitori. In tal senso European Commission, *Proposal for a Council Decision on the position to be taken on behalf of the European Union in the International Centre for Settlement on Investment Disputes (ICSID)*, Brussels, 9 febbraio 2022, COM (2022) 38 final 2022/0025 (NLE).

[99] ICSID, *CMS Gas Transmission Co. V. Argentine Republic*, 12 maggio 2005, ARB/01/8, par. 316; *Sempra Energy Int'l v. Republic of Argentina*, 28 settembre 2007, ARB/02/16, parr. 347-350.

[100] ICSID, *Continental Casualty Co. v. Argentine Republic*, 5 settembre 2008, ARB/03/9, par. 195 ss.

[101] In tal senso si è espresso anche l'organo di risoluzione delle controversie dell'Organizzazione Mondiale del Commercio, 29 aprile 2019, *Russia – Measures Concerning Traffic in Transit*, WT/DS512/R e WT/DS512/R/Add.1.

[102] L'eccezione di sicurezza nazionale, per come prevista dagli articoli XXI GATT, XIV-bis GATS e 346 e 347 TFUE, può infatti essere applicata agli interessi relativi a materie fissili, traffico di armi, munizioni o qualsiasi altro articolo o materiale destinato direttamente o indirettamente all'approvvigionamento delle forze armate o, ancora, può riguardare le misure applicate in tempo di guerra o, in via residuale, quelle applicate in caso di grave tensione internazionale.

Ai continui tentativi dell'Unione europea di armonizzare le risposte degli Stati alle minacce ibride nel settore delle infrastrutture critiche, in particolare digitali, si contrappone l'approccio ancora frammentato all'utilizzo dell'eccezione di sicurezza nazionale da parte dei singoli Stati, che godono di ampia autonomia nell'individuare l'interesse essenziale di sicurezza e nel valutare la misura più idonea a proteggerlo.

All'ampia autonomia riconosciuta agli Stati nell'applicare l'eccezione di sicurezza nazionale in settori sensibili, quale quello delle infrastrutture critiche digitali, si aggiunge la tendenza degli stessi a concludere accordi preferenziali o bilaterali per la disciplina di settori innovativi, con conseguente frammentazione della regolamentazione[103], nonché l'esiguo numero di casi posti all'attenzione delle Corti e la limitata competenza delle stesse nel valutare la giustiziabilità dell'eccezione[104].

Si è ritenuto infatti che la giustiziabilità dell'eccezione di sicurezza nazionale non possa riguardare aspetti inerenti la valutazione di sussistenza di una violazione dell'interesse di sicurezza nazionale o la necessarietà della misura, ma possa afferire solo alla proporzionalità della stessa rispetto all'attacco subìto – invero, sempre particolarmente grave nel caso di infrastrutture critiche digitali –, nonché all'ottemperanza agli obblighi procedurali – fulcro della disciplina del regolamento (UE) 2019/452 –, quali, ad esempio, la corretta notifica della volontà di invocare l'eccezione di sicurezza nazionale da parte dallo Stato *target*, così da assicurare che l'eccezione rappresenti solo un

[103] J.Y. YOO, D. AHN, *Security exceptions in the WTO system: bridge or bottle neck for trade security?*, in *Journal of International Economic Law*, vol. 19, n. 2, 2016, pp. 417-444.

[104] Tale situazione vede inoltre, a livello internazionale, una crescente sfiducia negli organi di risoluzione delle controversie. Ne è un esempio il mancato riconoscimento delle pronunce dell'Appellate Body dell'OMC da parte degli Stati Uniti che di fatto permette, in caso di riscontrato abuso nell'esercizio dell'eccezione di sicurezza nazionale, di impugnare "nel vuoto" la pronuncia dell'organo di primo grado, sospendendone l'efficacia a tempo indeterminato. Sul punto K. HOPEWELL, *The (surprise) return of development policy space in the multilateral trading system: what the WTO Appellate Body blockage means for the developmental state,* in *Review of International Political Economy*, vol. 31, n. 4, 2024, pp. 1245–1270.

contrasto alla minaccia ibrida e non si riveli, invece, una misura surrettiziamente economica[105].

Quanto ai meccanismi di controllo degli investimenti esteri diretti previsti dal diritto UE, l'assenza di un reale potere di *enforcement* da parte della Commissione e l'ampia discrezionalità di cui gli Stati godono nell'individuare le misure necessarie da applicare, hanno indotto parte della dottrina[106] per un verso a inquadrare i provvedimenti emanati dai Governi nell'esercizio dei poteri loro attribuiti in materia nella categoria degli atti di alta amministrazione, confermando il limite della giustiziabilità ai soli aspetti formali e alla valutazione di proporzionalità dell'eccezione, con esclusione di quella sul merito, e, per altro verso, a sottolineare lo squilibrio tra la posizione dell'investitore estero e quella dello Stato destinatario dell'investimento, che gode di ampia discrezionalità sul *se* e *in che modo* invocare l'eccezione.

Alla luce di quanto analizzato è possibile concludere che le infrastrutture critiche digitali e le connesse tecnologie critiche, tra le quali anche l'IA, imprescindibili per il corretto sviluppo della società, rappresentano uno dei principali bersagli delle minacce ibride. Di qui, da un lato l'esigenza di armonizzare la disciplina a livello europeo, utile a garantire una risposta coordinata agli attacchi e, dall'altro, quella degli Stati di mantenere un controllo preponderante e immediato attraverso l'eccezione di sicurezza nazionale.

Il superamento di questa duplicità di esigenze non è semplice, tenuto conto dei costanti e rapidi aggiornamenti che la disciplina richiede, nonché della necessità di bilanciare la tutela degli interessi essenziali

---

[105] In questo senso R. P. ALFORD, *op. cit.*, p. 708; R. BHALA, *National Security and International Trade Law: What the GATT says and what the United States Does. Symposium on Linkage as Phenomenon: An Interdisciplinary approach*, in *University of Pennsylvania Journal of International Law*, vol. 19, 1998, pp. 263-317, spec. p. 279. Dottrina contrapposta ha invece ritenuto la possibilità di una parziale giustiziabilità nel merito dell'eccezione di sicurezza nazionale, valutandola alla luce del principio di buona fede, in tal senso C. LUCKIE, *The Invocation of article XXI of GATT 1994 and the question of jurisdiction. Where to?*, 30 aprile 2024, p. 3, disponibile sul sito www.ssrn.com/abstract=4836860.

[106] In tal senso G. NAPOLITANO, *L'irresistibile ascesa del Golden Power e la rinascita dello Stato doganiere*, in *GDA*, n. 5, 2019; R. GAROFOLI, *Golden Power: mercato e protezione degli interessi nazionali*, in *federalismi.it*, n. 31, 2022; R. CHIEPPA, *La nuova disciplina del golden power dopo le modifiche del decreto-legge n. 21 e della legge di conversione 20 maggio 2022*, *ivi*, n. 51, 2022; D. IELO, *Riflessioni sul sindacato del giudice amministrativo sui cosiddetti "golden powers"*, in *CERIDAP*, n. 4, 2021.

degli Stati con il mantenimento di un'apertura al mercato degli investimenti, bilanciamento reso ulteriormente complesso dai differenti approcci con i quali gli Stati affrontano il delicato settore della sicurezza nazionale, ancora fortemente influenzato dalla sovranità nazionale.

ABSTRACT (ITA)

Il presente contributo, ripercorsa l'evoluzione della disciplina delle infrastrutture critiche nel diritto dell'Unione europea, si pone l'obiettivo di individuare i potenziali rischi che derivano dagli investimenti esteri diretti alle infrastrutture stesse negli Stati membri e di analizzare gli strumenti volti a bilanciare la sicurezza nazionale con la libera circolazione dei capitali nel settore, ritenuto particolarmente sensibile dall'Unione europea e dai singoli Stati. Nello specifico, il contributo si sofferma sui meccanismi di controllo degli investimenti esteri diretti, disciplinati dal regolamento (UE) 2019/452, che mirano a garantire maggiore trasparenza e cooperazione e implementare i criteri utili a individuare gli investimenti esteri diretti che devono essere interdetti dagli Stati membri, tentando di conciliare la necessità di preservare la sovranità nazionale in materia di sicurezza con l'apertura dei mercati che l'UE promuove. Ancora, si sofferma sulle restrizioni che gli Stati target possono applicare agli investimenti esteri diretti mediante l'eccezione di sicurezza nazionale, non senza considerare la giustiziabilità della stessa alla luce dei principi di proporzionalità e buona fede, volta a prevenire il rischio di misure protezionistiche derivanti dal potenziale uso abusivo dell'eccezione.

ABSTRACT (ENG)

The present contribution, after tracing the evolution of the regulatory framework governing critical infrastructures within the European Union, seeks to identify the potential risks arising from foreign direct investments directed at such infrastructures within the Member States and to analyse the legal instruments designed to balance between national security and the free movement of capital, in a sector considered as particularly sensitive at both Union and national level. More specifically, the contribution focuses on the foreign direct investment screening mechanisms established by Regulation (EU) 2019/452, which aim to enhance transparency and to strengthen cooperation mechanisms and assessment criteria to identify foreign direct investments that should be prohibited by the Member States. In this regard, the Regulation

reflects an attempt to strike a delicate balance between the preservation of Member States' prerogatives in the field of national security, and the Union's objective of promoting an open market. Furthermore, the contribution examines the scope and limits of the national security exception as a legal basis for imposing restrictions on foreign direct investments, with particular attention to its justiciability in light of the principles of proportionality and good faith, aimed at preventing the risk of protectionist practices resulting from the potentially abusive invocation of such an exception.