Indonesia Media Law Review, Volume 4 Issue 2 (December 2025), pp. 244-283
ISSN 2829-7628 (Print) 2829-7423 (Online)
https://doi.org/10.15294/imrev.v4i2.37742.
Indonesia Media Law Review is Journal for Media, Press Law and Ethics in Journalism
Published biannually by the Faculty of Law, Universitas Negeri Semarang, Indonesia and managed by Law Student Press Community and Press and Journalism Law Studies Center, Faculty of Law Universitas Negeri Semarang, INDONESIA

Bilateral Investment Treaties in the Digital Era: Implications for Technology and Media Regulation

Mira Nila Kusuma Dewi*

Universitas Indonesia Timur, Indonesia

Nurul Miqat

Universitas Tadulako, Indonesia

Susi Susilawati

Universitas Tadulako, Indonesia

Ashar Ridwan

Universitas Tadulako, Indonesia

Abd. Basir

Universitas Indonesia Timur, Indonesia

**Corresponding author's email: miranila@gmail.com*

ABSTRACT: This article examines the evolution of BITs in the digital era using a normative juridical method, focusing on how international investment law interacts with technology and media regulation. Through analysis of key jurisprudence, particularly *Yahoo! Inc. v. LICRA and UEJF* and the *Schrems I & II* decisions of the Court of Justice of the European Union (CJEU), the study demonstrates that the digital ecosystem demands more adaptive treaty frameworks capable of balancing investor protection with legitimate regulatory objectives such as privacy, cybersecurity, and content governance. The article also evaluates Indonesia's regulatory landscape, including the Information and Electronic Transactions Law (Undang-Undang tentang Informasi dan Transakis

Elektronik / UU ITE) and the Personal Data Protection Law (Undang-Undang Perlindungan Data Pribadi / UU PDP), to illustrate national perspectives on digital governance within the broader BIT reform movement. Ultimately, this research argues that BITs must incorporate explicit digital-era provisions-such as data governance carve-outs, cybersecurity exceptions, and right-to-regulate clauses-to safeguard state sovereignty and public interests while maintaining a predictable investment environment.

KEYWORDS: Bilateral Investment Treaty (BIT), technology and media regulations, digital sovereignty, Investor-State Dispute Settlement (ISDS), cybersecurity

I. INTRODUCTION

The global digital transition has fundamentally reshaped economic activity, enabling unprecedented cross-border flows of information, services, and capital. At the forefront of this transformation are technology and media corporations whose business models depend heavily on intangible assets, including software, algorithms, databases, user-generated content, and digital platforms. While these assets drive economic growth and innovation, they also challenge traditional legal frameworks governing international investment, particularly Bilateral Investment Treaties (BITs). Historically, BITs were drafted with a focus on capital-intensive, tangible forms of investment such as manufacturing facilities, natural resources, and infrastructure. However, in the digital era, investments increasingly consist of data-driven infrastructures, cloud systems, content-hosting services, and digital advertising platforms-assets that transcend territorial boundaries and disrupt established assumptions about jurisdiction, sovereignty, and regulatory power.[1]

This shift has intensified debate over the adequacy of BITs in addressing technological and media-related investments. Many BITs contain broadly worded definitions of investment, but their application to intangible digital assets remains ambiguous. Arbitrators and scholars have expressed concern that without explicit digital provisions, BITs may be interpreted in ways that constrain legitimate state regulation of data protection, cybersecurity,

[1] Peter T. Muchlinski, *Multinational Enterprises and the Law*, 2nd ed. (Oxford: Oxford University Press, 2007); Stephan W. Schill, "Reforming Investment Law in the Digital Era," *Journal of International Economic Law* 22, no. 3 (2019): 403–427.

platform accountability, and digital sovereignty.[2] Such uncertainty becomes more pronounced when states take measures that affect the operations of global technology firms, potentially triggering investor–state dispute settlement (ISDS) claims involving allegations of indirect expropriation or violation of fair and equitable treatment. At the same time, states increasingly rely on technology regulation to protect fundamental rights, ensure national security, and maintain democratic integrity-objectives that may require strong limitations on corporate practices.[3]

Two landmark cases exemplify these tensions: *Yahoo! Inc. v. LICRA and UEJF*[4], which explored cross-border conflicts between platform operations and national regulations; and *Schrems I* and *Schrems II* ,[5] which reshaped global data-transfer mechanisms by invalidating the EU–US Safe Harbor and Privacy Shield frameworks.[6] Although not BIT disputes, these cases illustrate how conflicts between territorial regulation, corporate autonomy, and transnational digital flows can escalate into legal dilemmas closely related to investment law. The principles emerging from these cases-particularly regarding data protection, jurisdiction, and extraterritorial enforcement-highlight the need for BITs to more clearly delineate the relationship between investor rights and a state's authority to regulate in the public interest.

This article argues that BITs must evolve to address the strategic importance of digital assets and the complex power relations embedded in the global technology ecosystem. In recent years, states have increasingly incorporated right-to-regulate clauses, public-interest carve-outs, cybersecurity exceptions, and data-protection safeguards into modern investment

---

[2] J. Kurtz, *The WTO and International Investment Law: Converging Systems* (Cambridge: Cambridge University Press, 2016); Marc Jacob et al., "Big Data and Investment Protection: Towards a New Paradigm," *Journal of World Investment and Trade* 21, no. 2 (2020): 245–270.

[3] Julie Cohen, *Between Truth and Power: The Legal Construction of Information Capitalism* (Oxford: Oxford University Press, 2019); Laura DeNardis, *The Global War for Internet Governance* (New Haven: Yale University Press, 2014).

[4] *Yahoo! Inc. v. LICRA and UEJF*, 433 F.3d 1199 (9th Cir. 2006); Court of Justice of the European Union

[5] *Schrems v. Data Protection Commissioner* (C-362/14), ECLI:EU:C:2015:650; Court of Justice of the European Union, *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems* (C-311/18), ECLI:EU:C:2020:559.

[6] Christopher Kuner, "The Schrems Judgments and the Future of EU–US Data Transfers," *German Law Journal* 18, no. 4 (2017): 881–906

agreements.[7] These reforms signal a departure from the highly investor-centric approach that dominated treaty drafting throughout the 20th century and demonstrate a growing recognition that technology and media industries implicate sovereignty, security, and human rights in ways that require more nuanced regulatory frameworks.

The Indonesian legal landscape provides a valuable context for examining these developments. Indonesia's Information and Electronic Transactions Law (UU ITE), Personal Data Protection Law (UU PDP), and related regulations reflect the state's increasing assertiveness in governing digital activity. These domestic frameworks intersect with Indonesia's participation in international economic agreements, raising questions about how future BITs should be designed to preserve regulatory autonomy while ensuring a conducive environment for digital-sector investment.

The purpose of this research is threefold. First, it seeks to explain how the digital era has transformed the nature of investment and challenged the doctrinal foundations of BITs. Second, it analyzes key jurisprudence and doctrinal debates relevant to technology and media regulation, illustrating the importance of balancing investor protections with digital-era regulatory priorities. Third, it evaluates Indonesia's legal approach and the implications for reforming BITs to accommodate the realities of digital governance.

This study answers the following questions:

1. How does the rise of digital technologies challenge traditional BIT concepts of "investment," regulatory space, and investor–state relations?
2. What lessons can be drawn from *Yahoo! v. France* and the *Schrems I & II* cases for the future design of BITs in the context of technology and media governance?
3. How should Indonesia's investment treaties evolve to address digital-era concerns while preserving regulatory sovereignty?

This research contributes to the field of international investment law by providing a normative analysis of how BITs should be restructured to address challenges posed by media platforms, data governance, and global digital interdependence. It also bridges technology law, media regulation, and

[7] United Nations Conference on Trade and Development (UNCTAD), *World Investment Report 2023: Investing in Sustainable Energy for All* (New York: United Nations Publications, 2023).

investment law-fields that have historically been treated separately despite their increasing convergence. For policymakers, the findings highlight the need for treaty reforms that incorporate digital-era safeguards without undermining the stability and predictability of investment protection.

Bilateral Investment Treaties emerged in the mid-20th century as instruments designed to protect foreign investors from political risks in host states. Traditional BITs were constructed around core standards such as **fair and equitable treatment (FET)**, **national treatment (NT)**, **most-favored-nation (MFN)** obligations, and **protection from direct and indirect expropriation**.[8] These instruments were strongly investor-centric, reflecting a period when developing states sought to attract foreign capital and global economic activity was dominated by tangible asset investment.

However, beginning in the 1990s-and accelerating in the 2010s-the global economy shifted toward **knowledge-intensive industries**, **information services**, and **digital infrastructures**, creating new forms of assets with little physical manifestation. [9] The international investment regime faced mounting criticism due to expansive interpretations of investor protections and ISDS mechanisms, which sometimes limited the capacity of states to enact public-interest regulations.[10] This culminated in a wave of modern BIT reforms emphasizing balance, regulatory sovereignty, and sustainable development.

As digital technologies proliferated, disputes began to involve investments such as data centers, content platforms, digital advertising services, algorithms, and online intellectual property. Scholars argue that intangible assets are now central to the value of multinational technology corporations, suggesting that BIT protections must evolve to cover these new categories of investment.[11]

Yet ambiguity persists. Many BITs contain broad investment definitions-e.g., "every kind of asset"-but do not explicitly list **data**, **software**, or

[8] Kevin Muhammad Haikal, "Foreign Investment Protection Post – Indonesia's Bilateral Investment Treaties Regime", Research Paper, Tilburg University, 2017, 17-20

[9] UNCTAD, *World Investment Report 2023*.

[10] Schill, "Reforming Investment Law in the Digital Era,"418.

[11] **Beauden John & Adam Rajuroy,** *Data as Capital: Integrating Digital Intangible Assets into Enterprise Value and Investment Decision-Making* (Dec 07, 2025), https://www.researchgate.net/publication/392774137

algorithms as protected assets. This leads to doctrinal uncertainty in arbitration proceedings, particularly when states regulate digital platforms or impose data-protection measures that may negatively impact foreign investors.[12]

Digital sovereignty refers to the ability of states to assert control over digital infrastructures, data-processing activities, and online content within their territory. [13] With cross-border data flows becoming essential to global commerce, many states increasingly assert regulatory power through digital policies such as:

1. data localization requirements,
2. cybersecurity certification rules,
3. platform content moderation laws, and
4. personal data protection frameworks.

Such policies often collide with the interests of global technology firms whose business models rely on data mobility and uniform operational frameworks.[14] The resulting tensions highlight the need for BITs to address the boundaries between investor rights and a state's regulatory sovereignty in the digital domain.

Two landmark cases- *Yahoo! Inc. v. LICRA and UEJF* and *Schrems I & II*- have become central references in discussions about digital sovereignty and cross-border regulation.

First, *Yahoo! Inc. v. LICRA and UEJF*[15] raised complex questions regarding territorial jurisdiction over online content, after French courts sought to impose national hate-speech regulations on a U.S.-based internet platform. The case illustrates how conflicting national laws challenge digital businesses operating globally.[16]

---

[12] Marc Jacob et al., "Big Data and Investment Protection: Towards a New Paradigm," *Journal of World Investment and Trade* 21, no. 2 (2020): 245–270.

[13] Julie Cohen, *Between Truth and Power: The Legal Construction of Information Capitalism* (Oxford: Oxford University Press, 2019)

[14] Anu Bradford, Robert Jackson, and Alek Orlov, "The Digital Governance Challenge: Data, Competition, and Global Regulation," *Yale Journal on Regulation* 38, no. 4 (2021): 502–548.

[15] *Yahoo! Inc. v. LICRA and UEJF*, 433 F.3d 1199.

[16] Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006), 45

Second, the CJEU's *Schrems I*[17] and *Schrems II*[18] decisions reshaped international data transfer law by invalidating the EU–US Safe Harbor and Privacy Shield frameworks due to insufficient privacy protections in the United States.[19] These rulings underscore the legal tensions between free data flow, national surveillance regimes, and fundamental rights protections-issues highly relevant to BIT negotiations.

Indonesia's digital legal regime consists of the Information and Electronic Transactions Law (UU ITE), the Personal Data Protection Law (UU PDP), Government Regulation No. 71/2019 on Electronic System Operation (PP PSTE), and a range of ministerial regulations governing data centers, cloud services, and platform liability. These laws demonstrate Indonesia's growing emphasis on digital sovereignty and national regulatory control.[20] Given Indonesia's participation in international trade and investment agreements-including CEPA negotiations with various countries-aligning domestic digital regulation with future BIT obligations is essential to safeguard regulatory space.

II. METHODS

This study employs a **normative juridical** research method, to analyze legal norms, principles, treaties, jurisprudence, and doctrinal debates. The method is for examining normative tensions between international investment law and domestic regulatory sovereignty, in connection with Indonesian BITs .

The research combines **statute approach by** reviewing BITs, treaties, and digital-era legal instruments; **case approach** by analyzing *Yahoo! v. France*, *Schrems I*, and *Schrems II*; **conceptual approach** by evaluating scholarly theories of digital sovereignty, data governance, and investment law; **comparative approach**: contrasting Indonesia's digital regulations with international models.

---

[17] Court of Justice of the European Union, *Schrems I* (C-362/14).
[18] Court of Justice of the European Union, *Schrems II* (C-311/18).
[19] Kuner, "The Schrems Judgments," 889.
[20] Laura Siregar, "Digital Sovereignty in Indonesia's Regulatory Shift," *Journal of Southeast Asian Cyber Law* 4, no. 2 (2022): 112–140.

The study relies on **primary legal materials** such as BITs, CJEU judgments, UU ITE, UU PDP, PP PSTE; secondary **legal materials**: books, peer-reviewed journals, UNCTAD reports, doctrinal texts; and **tertiary materials**: academic commentaries, digital law reports.
Legal materials are analyzed qualitatively through **normative interpretation**, including: **textual interpretation**: examining treaty language; **systematic interpretation**: placing BIT provisions in the context of broader digital regulation; **teleological interpretation**: assessing treaty objectives in light of digital-era needs;
The analysis aims to construct a coherent normative argument for reforming BITs to align with digital governance imperatives.

III. DISCUSSION

I. The Transformation of Investment in the Digital Era

The global economy has undergone a structural shift in which intangible assets-such as data, software, machine-learning models, cloud infrastructures, and digital advertising systems-have overtaken tangible assets as primary drivers of value creation. Digital platforms today rely on the continuous extraction, processing, and monetization of user data, which has become a new form of capital. [21] This transformation challenges the original architecture of BITs, which were conceived to protect traditional investments such as factories, natural resource concessions, or physical property.[22]

International investment law has struggled to keep pace with this evolution. The typical BIT definition of "investment" includes broad language like “every kind of asset,” yet arbitrators have historically interpreted this framework with physical assets in mind.[23] Digital assets-particularly data, user bases, ad-targeting algorithms, or content-distribution networks-do not fit neatly into classical categories. As Jacob

[21] Jathan Sadowski, “When Data is Capital: Datafication, Accumulation, and Extraction”, Big Data & Society 6, 2019, No. 1, 1-12, https://doi.org/10.1177/2053951718820549
[22] Muchlinski, *Multinational Enterprises and the Law*, 213.
[23] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law*, 3rd ed. (Oxford: Oxford University Press, 2012), 101-103.

et al.[24] argue, intangible digital assets often lack clear territoriality, making it difficult to determine their situs for the purpose of investment protection. This is one of negative impacts of BITs in the digital era.

The borderless nature of data flows complicates ownership, jurisdiction, and state control. For instance, a single cloud-based platform may store data in multiple jurisdictions, process information across different regions, and deliver services globally. In such cases, determining whether an investment is protected under a BIT-and whether a host state's regulations qualify as expropriation-becomes highly complex.[25]

The challenge is compounded by the fact that digital platforms frequently operate as **multi-jurisdictional entities**, raising questions such as "Where is the investment actually located?", "Which state is considered the host state?", "Can a regulator's actions in one jurisdiction affect an investment technically located in another?"

These questions illustrate why BITs need clearer digital-era provisions, including Indonesian BITs which have not been regulated in Indonesian regulation.

II. The Rise of Digital – Era Regulatory Measures

Data protection frameworks have emerged as expressions of state sovereignty aimed at protecting citizens' rights and regulating transnational technology corporations. The EU's General Data Protection Regulation (GDPR) is the most well-known example, establishing strict standards for cross-border data transfers and extraterritorial obligations.[26]

The GDPR model has influenced many countries, including Indonesia, whose Personal Data Protection Law (UU PDP) codifies principles such as lawfulness, fairness, transparency, data minimization, and security obligations.[27] These frameworks represent the state's right to

[24] Jacob et al., "Big Data and Investment Protection," 260.
[25] Bradford, Jackson, and Orlov, "Digital Governance Challenge," 530.
[26] Christopher Kuner, "International Data Transfers and Fundamental Rights After Schrems," *International and Comparative Law Quarterly* 66, no. 4 (2017): 870–904.
[27] Article 16 paragraph 2 point a (Personal Data collection is carried out in a limited and specific manner, legally valid, and transparently); and article 14 (The collection of Personal Data is carried out in a limited and specific manner, legally and fairly, with the knowledge and consent of the Personal Data owner)

regulate, even when such regulation may impose compliance burdens on foreign investors.

States increasingly adopt cybersecurity frameworks requiring digital service providers to implement security measures, report breaches, undergo audits, or store critical data domestically. For example, in Indonesia's PP 71/2019 divides electronic system operators into public and private categories,[28] imposing different obligations.[29]

These measures may affect the operational models of foreign investors and could be misinterpreted under traditional BIT language as discriminatory or unfair, which can affect to declining interest in digital investors, increasing the risk of regulatory unpredictability and potential treaty shopping avoidance by foreign investors.

Article 2 Number 2 Indonesia's PP 71/2019 mentions that electronic system operators are divided into public and private one. This measure could affect to violation of different treatment principle between public electronic system operator and private one which is violation of Fair and Equitable Treatment (FET), which could rise to indirect expropriation because of discrimination to electronic system operators.

Governments worldwide now regulate digital content, misinformation, and media concentration. Indonesia's ITE Law includes provisions on digital content, intermediary liability, and platform obligations. Concerning digital contents, article 27 prohibits immoral content, gambling, defamation/insults, and blackmail; article 28 prohibits the spread of disinformation that incites hatred or hostility (SARA); article 29 prohibits threats and blackmail; articles 30-34 prohibits illegal access, illegal interception, data/system interference, and misuse of equipment. Concerning intermediary liability, article 16 regulates the general obligations of PSE to operate systems that meet data security, integrity and authenticity standards; article 40 regulates the obligation

[28] Article 2 number 2: "Electronic System Providers as referred to in paragraph (1) include:
a. Public Electronic System Providers; and
b. Private Electronic System Providers."

[29] Article 4 (obligation to fulfill minimum requirement), article 5 (electronic information content), article 6 (registration), article 7 (security), article 8 (security and reliability), article 9 (source code and documentation for the Software), article 10 (competency in Electronic Systems or Information Technology), article 11 (service level agreement; information security agreement; information security and internal communication facilities), article 12 (risk management),

to cut off access to illegal content after a request from the competent authorities. Concerning platform obligations, article 26 of the ITE Law concerning personal data protection has been revoked and replaced by Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), which regulates platform obligations in more detail. While these regulations aim to protect public order and social stability, they may significantly impact foreign-owned platforms and give rise to investment disputes if not carefully aligned with BIT obligations.[30]

III. BITs AND THE BALANCE BETWEEN INVESTOR RIGHTS AND REGULATORY SOVEREGNTY

Traditional investment protections—such as the **Fair and Equitable Treatment (FET) standard**, the **Most-Favoured-Nation (MFN) clause**, and protection against **indirect expropriation**—were originally formulated within bilateral and multilateral investment treaty regimes to provide foreign investors with a stable, predictable, and legally secure environment, thereby assuring them that sudden political shifts, discriminatory measures, or arbitrary regulatory interventions by host States would not unjustifiably erode the economic value of their investments. These safeguards were primarily designed with conventional, asset-based investments in mind, such as factories, natural resources, or physical infrastructure, where the risks faced by investors typically stemmed from overt state action, including nationalisation or abrupt changes in ownership rules.[31]

However, when these traditional standards are extended to **technology-driven business models**, whose core value lies not in tangible assets but in **algorithmic decision-making, cross-border data flows, and large-scale digital platforms**, their application becomes considerably more complex and potentially problematic. Technology companies often rely on the continuous collection, processing, and transfer of data across jurisdictions, and their profitability is closely linked to regulatory environments governing data protection, cybersecurity, competition law, and digital sovereignty. In this context, regulatory measures

[30] David Tambini, *Media Freedom: A Short Introduction* (Cambridge: Polity Press, 2021), 68-72.
[31] Kurtz, *The WTO and International Investment Law*, 225–233.

adopted by States for legitimate public interests—such as protecting personal data, ensuring national security, preventing market dominance, or promoting ethical uses of artificial intelligence—may be challenged by investors as violations of FET, MFN, or as forms of indirect expropriation.

As a result, these investment protections, while intended to prevent arbitrary or discriminatory state conduct, may unintentionally **restrict the regulatory autonomy of States**, creating a "regulatory chill" in which governments hesitate to adopt or update digital regulations for fear of exposure to investor–State dispute settlement claims. Consequently, the application of traditional investment standards to technology companies risks transforming protections that were meant to foster investor confidence into legal constraints on legitimate and necessary state regulation, particularly in rapidly evolving technological sectors where public policy objectives and regulatory frameworks must remain flexible and responsive.

New-generation investment agreements increasingly reflect a deliberate shift away from the rigid, investor-centric approach of earlier bilateral investment treaties (BITs) by expressly incorporating **regulatory exceptions** that preserve the sovereign right of States to regulate in pursuit of legitimate public policy objectives. In particular, these agreements recognize that States must retain sufficient regulatory space to adopt and enforce measures aimed at protecting **public health**, **personal data and privacy**, **national security**, **public order**, and **cybersecurity**, even where such measures may incidentally affect foreign investments. Rather than treating all regulatory interference as a potential breach of investment obligations, modern treaties clarify that non-discriminatory, good-faith regulations adopted for these purposes should not, in themselves, give rise to State responsibility under standards such as fair and equitable treatment or indirect expropriation.[32]

[32] United Nations Conference on Trade and Development (UNCTAD), *World Investment Report 2015: Reforming International Investment Governance* (Geneva: UNCTAD, 2015), 98–103.

The inclusion of public health exceptions has become especially prominent following global health crises, reflecting the understanding that States must be able to impose emergency measures, regulate pharmaceuticals, digital health services, or platform-based activities without fear of investor claims.[2] Similarly, explicit carve-outs for **personal data protection**acknowledge that in the digital economy, data has become a strategic and sensitive resource, and that regulations governing data localisation, cross-border data transfers, and privacy standards are essential to protect fundamental rights and public trust.[3] In the same vein, exceptions relating to **national security and public order** allow governments to respond to threats posed by foreign control of critical digital infrastructure, artificial intelligence systems, or communication networks, while cybersecurity exceptions recognize the necessity of preventive and responsive regulatory action against cyberattacks, data breaches, and systemic digital risks.

Collectively, these safeguards are designed to ensure that BIT obligations do not generate so-called **"regulatory chilling effects,"** whereby States refrain from adopting necessary regulations out of concern that such measures could trigger costly investor–State dispute settlement proceedings. By expressly balancing investment protection with regulatory autonomy, new-generation investment agreements seek to align international investment law with contemporary governance needs in highly regulated and technologically dynamic sectors, thereby reaffirming that investment protection should not come at the expense of essential public interests.[33]

IV. Case Study Analysis: *Yahoo! Inc. v. LICRA and UEJF*

A. Case Background

[33] Andrew Newcombe and Luís Paradell, *Law and Practice of Investment Treaties: Standards of Treatment* (Alphen aan den Rijn: Kluwer Law International, 2009), 494–496.

The *Yahoo!* case concerned an order by French courts requiring Yahoo!, a U.S.-based company, to prevent the sale of Nazi memorabilia accessible through its platform to French users. The French court imposing fines for non-compliance, asserting jurisdiction over Yahoo!'s activities despite the company operating primarily from the United States. Yahoo! sought a declaratory judgment in U.S. federal court to prevent enforcement of the French order, resulting in a complex jurisdictional conflict.

B. Jurisdictional Implications for Digital Investments

The **Yahoo! case** vividly illustrates the structural difficulties faced by digital platforms operating in a borderless online environment when multiple States simultaneously assert regulatory authority over the same online conduct. In *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisémitisme (LICRA)*, French courts ordered Yahoo!, a United States–based company, to restrict access by French users to online auctions of Nazi memorabilia, despite the fact that the content was hosted on servers located outside France and was lawful under U.S. law. [34] This dispute exposed the **ambiguity of territoriality** in cyberspace, where online activities cannot be easily confined to a single jurisdiction and where traditional concepts of territorial sovereignty struggle to accommodate the global reach of digital platforms. Unlike physical commerce, online content is simultaneously accessible in multiple States, making it unclear which State's laws should prevail and on what jurisdictional basis regulatory authority may legitimately be exercised.[35]

The *Yahoo!* case vividly underscores the structural and legal challenges faced by digital platforms operating in a global online environment where multiple states simultaneously assert regulatory authority over the same online activities. Because digital content is inherently borderless, online platforms frequently become subject to overlapping, and sometimes conflicting, national laws. This situation exposes a

[34] *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisémitisme (LICRA)*, Tribunal de Grande Instance de Paris, 22 May 2000; affirmed in part, Court of Appeal of Paris, 6 December 2000.
[35] Goldsmith and Wu, *Who Controls the Internet? Illusions of a Borderless World*, 1–3.

fundamental tension between the territorial foundations of public international law and the deterritorialized nature of cyberspace. In the *Yahoo!* case, French authorities sought to enforce domestic hate speech and public order regulations against content hosted by a U.S.-based company, illustrating how national regulators increasingly extend their jurisdiction beyond physical borders when online activities produce effects within their territory.[36]

From the perspective of investment law, the case highlights three interrelated legal difficulties. First, it demonstrates **territoriality ambiguity**, as traditional jurisdictional principles struggle to determine where an online activity legally "occurs." Unlike conventional investments tied to a specific geographic location, digital services operate simultaneously across multiple jurisdictions, making it difficult to apply territorial concepts such as place of conduct, place of harm, or location of investment.[37] This ambiguity complicates the identification of the applicable legal regime and creates uncertainty for foreign investors regarding which domestic laws may govern their operations.

Second, the case illustrates **cross-border regulatory conflict**, where compliance with one state's legal requirements may directly contradict the laws or constitutional protections of another. In the *Yahoo!* dispute, U.S. free speech protections clashed with French public order and anti-hate speech norms. Such conflicts place digital investors in a precarious position, as adherence to one legal system may expose them to liability in another.[38]This regulatory fragmentation increases compliance costs and undermines legal predictability, both of which are central concerns in international investment protection.

Third, the case raises the risk of **exposure to multiple and potentially inconsistent legal obligations**. Digital platforms may face simultaneous enforcement actions by several states, each asserting jurisdiction based on effects doctrine, nationality of users, or

[36] Goldsmith and Wu, *Who Controls the Internet? Illusions of a Borderless World*, 3–6.
[37] Dan Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford: Oxford University Press, 2017), 45–47.
[38] Joel R. Reidenberg, "Technology and Internet Jurisdiction," *University of Pennsylvania Law Review* 153, no. 6 (2005): 1951–1954.

accessibility of content. This cumulative exposure creates a regulatory environment in which investors cannot realistically comply with all applicable rules at once, thereby increasing legal and financial risk.[39] In investment law terms, such conditions may indirectly affect the value, operation, or viability of a foreign investment.

When analyzed under a Bilateral Investment Treaty (BIT) framework, the enforcement of foreign content or media laws could theoretically be framed as a state measure adversely affecting a foreign investment. For instance, an investor might argue that mandatory content restrictions, filtering obligations, or penalties imposed by a host state amount to indirect expropriation, a breach of fair and equitable treatment (FET), or an unreasonable regulatory measure.[40] From this perspective, digital platforms could attempt to characterize regulatory enforcement as discriminatory, arbitrary, or disproportionate, particularly when it imposes significant economic or operational burdens.

However, allowing such claims without restraint would severely limit states' regulatory autonomy, especially in sensitive areas such as public order, cultural policy, and media regulation. Public international law has long recognized that states retain sovereign authority to regulate within their territory to protect fundamental societal interests, including public morals, national security, and social cohesion.[41] If investment tribunals were to consistently prioritize investor interests over these regulatory objectives, BITs could be transformed into instruments that chill legitimate regulation, particularly in the digital and media sectors. This would undermine the balance between investment protection and the sovereign right to regulate—a balance that contemporary investment law increasingly seeks to preserve.[42]

---

[39] Anupam Chander, "Globalization and Distrust," *Yale Law Journal* 114, no. 6 (2005): 1193–1196.

[40] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law*, 2nd ed. (Oxford: Oxford University Press, 2012), 145–148.

[41] UNCTAD, *World Investment Report 2012: Towards a New Generation of Investment Policies* (Geneva: United Nations, 2012), 119–121.

[42] Stephan W. Schill, "The Right to Regulate in International Investment Law," in *International Investment Law and Comparative Public Law*, ed. Stephan W. Schill (Oxford: Oxford University Press, 2010), 512–515.

C. Lessons for BIT Reform

Three key insights emerge from the increasing interaction between international investment law and the regulation of digital platforms, particularly in the media and content sector. These insights are especially relevant for the future design and interpretation of Bilateral Investment Treaties (BITs), as traditional investment protection standards were not originally conceived for borderless digital activities.

First, BITs must clarify how the principle of **territoriality applies to digital platforms**. Classical investment treaties assume that an investment is territorially anchored within the host state, whether through physical assets, personnel, or infrastructure. Digital platforms, however, operate through decentralized networks, cloud-based services, and cross-border data flows that blur the connection between investment and territory. As a result, uncertainty arises regarding whether jurisdiction should be determined by the location of servers, the nationality of users, the place where content is accessed, or the economic effects of online activities.[43] Without clear treaty language addressing these issues, arbitral tribunals may adopt inconsistent approaches, thereby undermining legal certainty for both investors and host states. Clarifying territorial nexus requirements in BITs would help define the scope of treaty protection while preventing excessive assertions of jurisdiction over purely extraterritorial digital conduct.[44]

Second, **regulatory sovereignty in media matters must be explicitly preserved** within BIT frameworks. Media and content regulation is closely linked to fundamental state interests, including the protection of public order, cultural identity, national security, and democratic discourse. Unlike many commercial sectors, media regulation often reflects constitutional values and societal norms that vary significantly across states.[45] If BITs fail to expressly safeguard regulatory autonomy

---

[43] Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* (Oxford: Oxford University Press, 2017), 52–56.

[44] Jack L. Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006), 25–28.

[45] Monroe E. Price, *Media and Sovereignty: The Global Information Revolution and Its Challenge to State Power*(Cambridge, MA: MIT Press, 2002), 67–71.

in this area, host states may face investor claims alleging treaty breaches whenever content moderation, censorship, or licensing requirements affect the operations of foreign digital platforms. Explicit treaty language reaffirming the state's right to regulate media content is therefore essential to prevent investment law from encroaching upon sensitive areas of domestic governance.[46]

Third, **content regulation should be exempt from claims of indirect expropriation or violations of the fair and equitable treatment (FET) standard**. In investment arbitration, indirect expropriation claims typically arise when regulatory measures substantially deprive an investor of the economic value of its investment. Similarly, FET claims are often based on allegations of regulatory unpredictability or disproportionality. Applying these standards to content regulation risks transforming legitimate public interest measures into compensable treaty violations. [47] Content-related measures—such as takedown orders, restrictions on harmful speech, or obligations to comply with local media standards—are generally non-discriminatory regulations enacted in pursuit of legitimate public objectives. Treating such measures as expropriatory or unfair would severely constrain states' ability to govern the digital public sphere.[48]

Together, these three insights support the inclusion of **media-specific carve-outs in future BITs**. Such carve-outs would explicitly exclude media content regulation from the scope of certain investment protection standards or from investor–state dispute settlement altogether. Comparable exclusions already exist in some trade and investment agreements, particularly in relation to cultural industries and

[46] UNCTAD, *World Investment Report 2012: Towards a New Generation of Investment Policies* (Geneva: United Nations, 2012), 119–122.

[47] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law*, 2nd ed. (Oxford: Oxford University Press, 2012), 101–105, 145–148.

[48] Stephan W. Schill, "The Right to Regulate in International Investment Law," in *International Investment Law and Comparative Public Law*, ed. Stephan W. Schill (Oxford: Oxford University Press, 2010), 512–516.

audiovisual services.[49] By extending similar carve-outs to digital media platforms, states can ensure that investment treaties do not undermine domestic media policies while still providing adequate protection for genuine commercial investments. In this way, media-specific carve-outs serve as a structural mechanism to rebalance investment protection with sovereign regulatory authority in the digital age.

V. CASE STUDY ANALYSIS: SCHREMS I & II

A. Case Background

The *Schrems* litigation represents one of the most significant legal challenges to transatlantic data governance and highlights the tension between data protection as a fundamental right in the European Union and national security–driven surveillance practices in the United States. Initiated by Max Schrems, an Austrian privacy activist, the cases fundamentally reshaped the legal framework governing EU–US transfers of personal data and underscored the limits of international regulatory cooperation in the digital age.

In *Schrems I* (2015), the Court of Justice of the European Union (CJEU) examined the validity of the EU–US Safe Harbor framework, which had allowed U.S. companies to receive personal data from the EU by self-certifying compliance with certain privacy principles. Schrems argued that U.S. law did not ensure an adequate level of protection for EU citizens' personal data, particularly in light of U.S. intelligence agencies' broad surveillance powers revealed by Edward Snowden. The CJEU accepted this argument and held that Safe Harbor failed to meet the requirements of EU law because it did not effectively limit U.S. public authorities' access to personal data nor provide EU data subjects with enforceable legal remedies.[50] As a result, the Court invalidated the European Commission's adequacy decision

[49] Mira Burri, "Cultural Diversity and International Economic Law," in *Research Handbook on Cultural Diversity and International Economic Law*, ed. Valentina Vadi and Hilde Van den Bossche (Cheltenham: Edward Elgar, 2015), 46–49.

[50] Court of Justice of the European Union, *Case C-362/14, Maximillian Schrems v Data Protection Commissioner*, Judgment of 6 October 2015, paras. 94–98.

underpinning the Safe Harbor framework, emphasizing that fundamental rights to privacy and data protection under EU law could not be compromised by international arrangements.[51]

The *Schrems I* judgment established several important legal principles. First, it reaffirmed that the standard of "adequate protection" under EU law requires a level of protection that is essentially equivalent to that guaranteed within the EU itself. Second, it confirmed the independence and authority of national data protection authorities to review international data transfer mechanisms, even where the European Commission has adopted an adequacy decision.[52] These principles significantly strengthened the constitutional status of data protection within the EU legal order and limited the discretion of political institutions in negotiating international data transfer frameworks.

Following the invalidation of Safe Harbor, the European Union and the United States negotiated a replacement arrangement known as the EU–US Privacy Shield. This framework introduced additional safeguards, including written assurances regarding U.S. surveillance practices and the establishment of an Ombudsperson mechanism intended to provide redress for EU citizens. However, Schrems once again challenged the legality of EU–US data transfers, leading to the *Schrems II* judgment in 2020. In this decision, the CJEU struck down the Privacy Shield, finding that it suffered from structural deficiencies similar to those of its predecessor.[53]

In *Schrems II*, the Court concluded that U.S. surveillance laws—particularly those permitting bulk data collection for national security purposes—were not limited to what was strictly necessary and proportionate, as required by EU fundamental rights standards.

---

[51] Paul De Hert and Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" *Computer Law & Security Review* 32, no. 2 (2016): 179–181.

[52] Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," *German Law Journal* 18, no. 4 (2017): 881–884.

[53] Court of Justice of the European Union, *Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment of 16 July 2020, paras. 168–170.

Moreover, the Ombudsperson mechanism was deemed insufficiently independent and lacking binding decision-making power, thereby failing to provide effective judicial redress for EU data subjects.[54] The judgment reaffirmed that systemic access by public authorities to personal data, without robust oversight and enforceable remedies, is incompatible with EU data protection law.

Together, the *Schrems I* and *Schrems II* decisions illustrate the growing extraterritorial impact of EU data protection standards and the EU's willingness to condition international data flows on compliance with its constitutional values. The cases demonstrate that data protection has evolved from a regulatory concern into a central element of digital sovereignty and fundamental rights protection. At the same time, they expose the difficulties of reconciling divergent legal traditions and policy priorities—particularly between the EU's rights-based approach to privacy and the U.S. emphasis on national security and market-driven data governance.[55]

The *Schrems I* and *Schrems II* decisions had profound practical and legal consequences for the global digital economy, disrupting the operational models of thousands of companies that rely on cross-border data flows. Multinational technology firms, cloud service providers, social media platforms, and data-driven enterprises were particularly affected, as the invalidation of the EU–US Safe Harbor and Privacy Shield frameworks removed the primary legal bases upon which transatlantic data transfers had been conducted for years. These rulings forced companies to reassess their compliance strategies, restructure data processing operations, and, in some cases, localize data storage within the European Union.[56] The decisions thus demonstrate how judicial enforcement of fundamental rights can directly reshape global business practices in the digital age.

---

[54] Orla Lynskey, "Schrems II, Surveillance, and the Future of Transatlantic Data Transfers," *Common Market Law Review* 57, no. 6 (2020): 1725–1728.

[55] Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64, no. 3 (2015): 700–703.

[56] Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," *German Law Journal* 18, no. 4 (2017): 884–887.

First, the *Schrems* judgments illustrate the **increasing elevation of privacy to a fundamental rights issue** rather than a mere regulatory or consumer protection concern. The Court of Justice of the European Union (CJEU) consistently framed data protection as an essential component of the right to privacy and the protection of personal data enshrined in the EU Charter of Fundamental Rights.[57] By insisting that international data transfer mechanisms must ensure a level of protection "essentially equivalent" to that guaranteed within the EU, the Court constitutionalized privacy standards and placed them above economic or political expediency. This approach signals a broader shift in global digital governance, where privacy is treated as a non-negotiable normative value rather than a flexible policy variable.[58]

Second, these decisions reflect the **willingness of courts to restrict data flows even when economic concerns are significant**. The CJEU was fully aware that invalidating Safe Harbor and Privacy Shield would impose substantial compliance costs on businesses and potentially disrupt transatlantic trade. Nevertheless, the Court prioritized the protection of fundamental rights over economic efficiency, emphasizing that commercial convenience cannot justify systemic interference with individual rights.[59]This judicial stance challenges the assumption that economic integration necessarily requires the free flow of data and underscores the capacity of courts to act as guardians of constitutional values in the digital economy.

Third, the *Schrems* cases highlight the **role of state law and human rights norms in shaping digital-era investment conditions**. By invalidating international data transfer frameworks negotiated at the executive level, the CJEU reaffirmed the authority of constitutional and human rights law to constrain market access and investment conditions. This demonstrates that the legal environment for digital investments is

[57] Court of Justice of the European Union, *Case C-362/14, Maximillian Schrems v Data Protection Commissioner*, Judgment of 6 October 2015, paras. 39–41.

[58] Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order," *International and Comparative Law Quarterly* 63, no. 3 (2014): 576–579.

[59] Court of Justice of the European Union, *Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment of 16 July 2020, paras. 168–170.

not determined solely by trade liberalization or investment promotion policies, but also by domestic and supranational human rights obligations.[60] As a result, foreign investors operating in the digital sector must account for the possibility that host states, or regional legal orders such as the EU, may impose stringent regulatory requirements grounded in fundamental rights protection.

From an investment law perspective, *Schrems I* and *Schrems II* illustrate that **state-imposed privacy regulations may legitimately limit investor expectations**. In international investment arbitration, investors often invoke the fair and equitable treatment (FET) standard to argue that regulatory changes violated their legitimate expectations. However, the *Schrems* decisions suggest that expectations of regulatory stability cannot override a state's obligation to protect fundamental rights.[61] Where privacy and data protection are constitutionally entrenched, investors cannot reasonably expect a regulatory environment that prioritizes unrestricted data flows over human rights safeguards.

If a foreign investor were to argue that stringent privacy regulations amount to indirect expropriation, host states would have strong legal grounds to defend such measures as **necessary for the protection of human rights**. International investment law increasingly recognizes that non-discriminatory regulations enacted for legitimate public purposes—such as public health, environmental protection, or human rights—do not constitute compensable expropriation, even if they adversely affect the economic value of an investment.[62] In this context, privacy regulations following the *Schrems* jurisprudence can be characterized as bona fide regulatory measures pursuing a legitimate and internationally recognized objective. Consequently, the *Schrems* cases reinforce the principle that investment protection must be balanced

[60] Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64, no. 3 (2015): 700–704.
[61] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law*, 2nd ed. (Oxford: Oxford University Press, 2012), 133–136.

[62] Stephan W. Schill, "The Right to Regulate in International Investment Law," in *International Investment Law and Comparative Public Law*, ed. Stephan W. Schill (Oxford: Oxford University Press, 2010), 512–516.

against, and in some cases yield to, states' obligations to uphold fundamental rights in the digital era.

B. Implications for Global Data Transfers and Technology Investment

The decisions of the Court of Justice of the European Union (CJEU) in *Schrems I* (2015) and *Schrems II* (2020) profoundly disrupted the operational models of thousands of companies, including multinational technology firms whose business models depend on the continuous cross-border transfer of personal data. By invalidating the EU–US Safe Harbor and Privacy Shield frameworks, the Court removed the principal legal mechanisms that had enabled transatlantic data flows for many years. As a result, companies were compelled to reassess their compliance strategies, adopt alternative transfer mechanisms, implement costly supplementary safeguards, or restructure their data processing activities entirely.[63] These consequences illustrate how judicial decisions grounded in fundamental rights protection can have far-reaching economic and organizational impacts in the digital economy.

First, the *Schrems* decisions illustrate the **increasing elevation of privacy to a fundamental rights issue**. The CJEU consistently framed data protection not as a technical regulatory matter, but as an essential component of the fundamental rights to privacy and the protection of personal data guaranteed under the EU Charter of Fundamental Rights.[64] By requiring that international data transfer regimes ensure a level of protection "essentially equivalent" to that provided within the EU, the Court constitutionalized data protection standards and placed them at the apex of the legal hierarchy. This approach reflects a broader normative shift in which privacy is treated as a core human right that limits both governmental discretion and market-driven data practices.[65]

---

[63] Christopher Kuner, "Reality and Illusion in EU Data Transfer Regulation Post Schrems," *German Law Journal* 18, no. 4 (2017): 884–887.

[64] Court of Justice of the European Union, *Case C-362/14, Maximillian Schrems v Data Protection Commissioner*, Judgment of 6 October 2015, paras. 39–41.

[65] Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order," *International and Comparative Law Quarterly* 63, no. 3 (2014): 569–581.

Second, these rulings demonstrate the **willingness of courts to restrict data flows even when economic concerns are significant**. The CJEU was well aware that invalidating Safe Harbor and Privacy Shield would impose substantial compliance costs on businesses and potentially disrupt transatlantic trade and investment. Nevertheless, the Court held that economic efficiency and commercial convenience cannot justify systemic interferences with fundamental rights.[66] This judicial posture underscores the role of courts as guardians of constitutional values in the digital age, even where such protection entails tangible economic consequences. It also challenges the assumption that economic globalization necessarily entails unrestricted data mobility.

Third, the *Schrems* jurisprudence highlights the **role of state law and human rights norms in shaping digital-era investment conditions**. By invalidating international data transfer frameworks negotiated at the political and executive level, the CJEU reaffirmed that domestic and supranational human rights obligations can directly shape the legal environment in which digital investments operate. This demonstrates that investment conditions in the digital economy are not determined solely by liberalization commitments or market access policies, but are also constrained by constitutional and human rights norms embedded in state law.[67] For foreign investors, this means that regulatory risk in the digital sector is inseparable from the human rights frameworks of the jurisdictions in which they operate.

From an international investment law perspective, *Schrems I* and *Schrems II* demonstrate that **state-imposed privacy regulations may legitimately limit investor expectations**. While investors frequently invoke the fair and equitable treatment (FET) standard to protect their legitimate expectations of regulatory stability, international investment law does not guarantee a frozen legal framework. In areas where regulation is closely linked to fundamental rights, investors cannot reasonably expect that host states will refrain from adapting or

[66] Court of Justice of the European Union, *Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment of 16 July 2020, paras. 168–170.

[67] Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64, no. 3 (2015): 700–704.

strengthening legal protections.[68]The *Schrems* decisions thus reinforce the view that legitimate expectations must be assessed in light of a state's duty to comply with constitutional and international human rights obligations.

If a foreign investor were to claim that privacy regulations amount to indirect expropriation, host states would be well positioned to defend such measures as **necessary for the protection of human rights**. Contemporary investment jurisprudence increasingly recognizes that non-discriminatory regulatory measures adopted for legitimate public purposes—such as public health, environmental protection, or the protection of fundamental rights—do not constitute compensable expropriation, even where they adversely affect the economic value of an investment.[69] In this context, privacy regulations inspired by the *Schrems* rulings can be characterized as bona fide exercises of regulatory authority aimed at safeguarding fundamental rights. Accordingly, these cases illustrate how investment protection standards must be balanced against, and in some instances yield to, states' obligations to protect human rights in the digital era.

C. Lessons for BIT Reform

The jurisprudence arising from *Schrems I* (2015) and *Schrems II* (2020) offers important normative and structural lessons for international economic law, particularly in relation to the interaction between data protection, human rights, and investment treaty obligations. Taken together, these decisions demonstrate a broader transformation in global legal ordering, in which fundamental rights increasingly shape and constrain economic governance.

First, the *Schrems* jurisprudence clearly demonstrates that **data protection is a fundamental right and cannot be undermined by investment obligations**. The Court of Justice of the European Union

---

[68] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law*, 2nd ed. (Oxford: Oxford University Press, 2012), 133–136.

[69] Stephan W. Schill, "The Right to Regulate in International Investment Law," in *International Investment Law and Comparative Public Law*, ed. Stephan W. Schill (Oxford: Oxford University Press, 2010), 512–516.

(CJEU) consistently framed the protection of personal data as an essential component of the rights to privacy and data protection guaranteed under Articles 7 and 8 of the EU Charter of Fundamental Rights.[70] By invalidating international data transfer frameworks that failed to ensure "essentially equivalent" protection, the Court made clear that economic arrangements—whether based on trade, investment, or regulatory cooperation—cannot justify systemic interferences with fundamental rights.[71] This approach signals that fundamental rights operate as normative limits on economic integration and cannot be contractually displaced by international economic commitments.

From the perspective of international investment law, this principle has significant implications. Investment treaties are designed to protect foreign investors from arbitrary or discriminatory state conduct, but they do not exist in a legal vacuum. Where host states are constitutionally or internationally obliged to protect fundamental rights, investors cannot legitimately expect regulatory environments that prioritize commercial convenience over rights protection.[72] The *Schrems*cases thus reinforce the hierarchy of norms in which human rights obligations take precedence over investment protections when the two come into conflict.

Second, the *Schrems* jurisprudence underscores that **BITs must include data governance exceptions to shield privacy laws from investor–state dispute settlement (ISDS) claims**. In the absence of explicit carve-outs or exceptions, foreign investors might attempt to challenge data protection measures as violations of standards such as fair and equitable treatment (FET) or indirect expropriation. Such claims could argue that restrictions on cross-border data flows, localization requirements, or enhanced compliance obligations frustrate

[70] Court of Justice of the European Union, *Case C-362/14, Maximillian Schrems v Data Protection Commissioner*, Judgment of 6 October 2015, paras. 39–41.

[71] Court of Justice of the European Union, *Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment of 16 July 2020, paras. 168–170.

[72] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law*, 2nd ed. (Oxford: Oxford University Press, 2012), 133–136.

legitimate expectations or substantially impair the value of digital investments.[73]

However, the *Schrems* rulings illustrate that privacy regulation is not a discretionary policy choice but a legal necessity grounded in fundamental rights. As such, exposing data protection laws to investment arbitration risks subjecting non-negotiable human rights obligations to economic balancing exercises conducted by arbitral tribunals.[74] To prevent this outcome, BITs should expressly incorporate data governance exceptions—similar to public policy or general exceptions clauses—that exclude privacy and data protection measures from the scope of certain treaty obligations or from ISDS altogether.[75] Such clauses would enhance legal certainty, reduce regulatory chill, and preserve states' ability to comply with their human rights duties without fear of investment claims.

Third, the *Schrems* jurisprudence demonstrates that **human rights norms influence international economic law and must be integrated into treaty drafting**. The decisions exemplify a broader trend in which courts, regulators, and treaty drafters increasingly recognize that economic agreements cannot be insulated from constitutional and human rights constraints. International investment law, traditionally focused on property protection and market access, is gradually evolving to acknowledge states' right—and duty—to regulate in pursuit of legitimate public objectives, including the protection of fundamental rights.[76]

Integrating human rights norms into BIT drafting may take several forms, including explicit references to human rights obligations in treaty preambles, interpretive clauses affirming regulatory autonomy, and

---

[73] Michele Potestà, "Legitimate Expectations in Investment Treaty Law: Understanding the Roots and the Limits of a Controversial Concept," *ICSID Review* 28, no. 1 (2013): 88–91.

[74] Stephan W. Schill, "The Right to Regulate in International Investment Law," in *International Investment Law and Comparative Public Law*, ed. Stephan W. Schill (Oxford: Oxford University Press, 2010), 512–516.

[75] UNCTAD, *World Investment Report 2015: Reforming International Investment Governance* (Geneva: United Nations, 2015), 137–139.

[76] Valentina Vadi, *Cultural Heritage in International Investment Law and Arbitration* (Cambridge: Cambridge University Press, 2014), 41–44.

substantive exceptions for measures adopted to protect fundamental rights.[77] The *Schrems* cases demonstrate that failing to integrate such norms risks normative conflict and legal fragmentation, particularly in the digital economy where data flows, privacy, and surveillance intersect directly with investment activities. By contrast, treaty frameworks that explicitly acknowledge the primacy of human rights can promote coherence between international economic law and public international law more broadly.

In sum, the *Schrems* jurisprudence provides a compelling illustration of how data protection has emerged as a constitutionalized human right that shapes, constrains, and reorients international economic governance. It confirms that investment obligations cannot override fundamental rights, that BITs must be carefully designed to shield privacy regulation from ISDS challenges, and that human rights norms must be systematically integrated into the drafting and interpretation of international economic treaties in the digital era.

VI. IMPLICATIONS FOR INDONESIA'S BIT FRAMEWORK

Indonesia has increasingly asserted its **digital sovereignty** through a comprehensive and evolving body of domestic legislation governing electronic systems, data protection, cybersecurity, and online content. Key instruments include Law No. 11 of 2008 on Electronic Information and Transactions (*UU ITE*), as amended; Law No. 27 of 2022 on Personal Data Protection (*UU PDP*); Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (*PP 71/2019*); and a series of Ministerial Regulations issued by the Ministry of Communication and Informatics (*Permenkominfo*) imposing obligations on digital platforms, including content moderation, system registration, and cooperation with

[77] UNCTAD, *Reforming Investment Dispute Settlement: A Stocktaking* (Geneva: United Nations, 2019), 63–66.

authorities.[78] Collectively, these laws are designed to protect **public order, personal data, cybersecurity, and national digital resilience**, all of which constitute core sovereign interests in the digital era.[79]

However, foreign technology investors subject to these regulations may attempt to challenge them under international investment agreements, alleging that such measures are discriminatory, violate the fair and equitable treatment (FET) standard, amount to indirect expropriation, or impose excessive regulatory burdens.[80] In the absence of explicit digital-era safeguards within Indonesia's bilateral investment treaties (BITs), there is a risk that investment tribunals could interpret investor protection standards expansively, thereby undermining Indonesia's regulatory autonomy in sensitive digital policy areas. This risk reflects broader structural tensions between traditional investment law—developed primarily for tangible, territorially anchored investments—and the intangible, cross-border nature of digital economic activity.[81]

To address these challenges, Indonesia should integrate a set of carefully designed provisions into future BITs that reflect the realities of digital governance while preserving legitimate investor protection.

Explicit Recognition of Digital Assets as Protected Investments

First, BITs should incorporate **modernized definitions of "investment"** that explicitly recognize digital assets, including data sets and databases, software and source code, algorithms and artificial intelligence (AI) models, cloud computing infrastructure, and digital platforms with their associated user networks.[82] Explicit recognition of these assets enhances legal certainty by reducing interpretive ambiguity before arbitral tribunals. At the same time, clarity in definition does not require the abandonment of regulatory authority; rather, it allows states

---

[78] Budi Agus Riswandi, *Hukum Siber dan Transformasi Digital di Indonesia* (Yogyakarta: UII Press, 2021), 112–118.

[79] Hikmahanto Juwana, "State Sovereignty and Digital Regulation in Indonesia," *Indonesian Journal of International Law* 18, no. 3 (2021): 345–348.

[80] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law*, 2nd ed. (Oxford: Oxford University Press, 2012), 133–136.

[81] Anupam Chander and Uyên P. Lê, "Data Nationalism," *Emory Law Journal* 64, no. 3 (2015): 700–704.

[82] OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (Paris: OECD Publishing, 2019), 33–35.

to delineate more precisely the scope of protection while preserving policy space through tailored exceptions and safeguards.[83]

Second, future Indonesian BITs should adopt **unequivocal right-to-regulate clauses** affirming that privacy protection, cybersecurity, digital sovereignty, public morals, public order, and national security constitute legitimate regulatory objectives. Such clauses should make clear that bona fide regulatory measures pursuing these objectives cannot be undermined by expansive interpretations of investor protections.[84] This approach aligns with contemporary treaty practice, including the EU–Canada Comprehensive Economic and Trade Agreement (CETA), which explicitly reaffirms states' right to regulate in pursuit of legitimate public policy goals.[85] It also reflects UNCTAD guidance advocating a rebalancing of investment protection and regulatory autonomy.[86]

Third, following the implications of *Schrems I* and *Schrems II*, BITs must contain **data protection carve-outs** specifying that a state's data protection laws cannot be challenged as indirect expropriation, that compliance requirements for cross-border data transfers fall within inherent regulatory powers, and that privacy is a fundamental right that supersedes purely economic interests.[87] Such provisions are essential to ensure that Indonesia's *UU PDP* remains fully enforceable without the chilling effect of potential ISDS claims. By explicitly shielding privacy regulation, BITs can prevent arbitral tribunals from subjecting non-negotiable human rights obligations to proportionality or compensation analyses.[88]

---

83 Stephan W. Schill, "The Right to Regulate in International Investment Law," in *International Investment Law and Comparative Public Law*, ed. Stephan W. Schill (Oxford: Oxford University Press, 2010), 512–516

84 UNCTAD, *World Investment Report 2015: Reforming International Investment Governance* (Geneva: United Nations, 2015), 137–139.

85 Comprehensive Economic and Trade Agreement (CETA) between Canada and the European Union, Art. 8.9.

86 UNCTAD, *Investment Policy Framework for Sustainable Development* (Geneva: United Nations, 2015), 91–94.

87 Court of Justice of the European Union, *Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment of 16 July 2020, paras. 168–170.

88 Orla Lynskey, "Schrems II and the Future of Transatlantic Data Transfers," *Common Market Law Review* 57, no. 6 (2020): 1725–1728.

Fourth, BITs should include **broad cybersecurity and national security exceptions** recognizing states' discretion to implement national cybersecurity regulations, network security certification schemes, data localization requirements for critical sectors, and defensive measures against foreign cyber intrusions.[89] Given the increasing frequency and sophistication of cyber threats, these measures must be treated as non-compensable exercises of state sovereignty, unless they are demonstrably discriminatory or abusive. This approach is consistent with general international law principles recognizing national security as an essential state function beyond ordinary investment protection scrutiny.[90]

Fifth, drawing lessons from cases such as *Yahoo! v. France*, BITs must include **media and content governance exceptions** ensuring that content moderation requirements, anti-disinformation laws, restrictions on harmful or extremist content, and platform obligations regarding illegal material cannot be interpreted as treaty violations.[91] Media regulation serves essential public interests, including democratic integrity, social harmony, and the preservation of national culture. Subjecting such regulation to investment arbitration risks undermining the state's ability to govern the digital public sphere in accordance with constitutional values.[92]

Beyond substantive provisions, Indonesia and other states should advocate for **procedural reforms in ISDS** to better align dispute settlement mechanisms with digital regulatory realities. These reforms may include limitations on claims challenging public-interest digital regulations, mandatory exhaustion of local remedies in digital regulatory disputes, enhanced transparency obligations, and the appointment of arbitrators with demonstrated expertise in digital law and technology regulation.[93] Such safeguards would reduce the risk of

---

89 Jack L. Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006), 68–72.

90 James Crawford, *Brownlie's Principles of Public International Law*, 9th ed. (Oxford: Oxford University Press, 2019), 747–749.

91 *LICRA and UEJF v Yahoo! Inc.*, Tribunal de Grande Instance de Paris, 20 November 2000.

92 Monroe E. Price, *Media and Sovereignty* (Cambridge, MA: MIT Press, 2002), 67–71.

93 UNCTAD, *Reforming Investment Dispute Settlement: A Stocktaking* (Geneva: United Nations, 2019), 63–66.

investor overreach and improve the legitimacy and coherence of investment adjudication in the digital age.

To ensure coherence, Indonesia must harmonize its domestic digital regulatory framework—particularly *UU PDP*, *UU ITE*, and *PP 71/2019*—with its BIT obligations. This does not imply subordinating sovereignty to investment treaties. Rather, it requires drafting BIT language that expressly permits Indonesia to continue enforcing its digital laws without legal uncertainty.[94] Properly designed treaties can function as instruments of legal coordination rather than constraints on sovereign policymaking.

Final Remarks

The emergence of digital technologies has transformed global economic relations and introduced unprecedented complexity into international investment law. Digital and media investments differ fundamentally from traditional investments, existing BIT frameworks are insufficiently equipped to address digital governance, and jurisprudence such as *Yahoo! v. France* and *Schrems I & II* underscores the urgency of reform. Indonesia's digital laws reflect legitimate sovereign interests that must be safeguarded in future BIT negotiations. As states move toward an increasingly interconnected digital future, investment treaties must evolve accordingly. Without comprehensive reform, the risk of conflict between investor protections and state sovereignty will continue to grow, potentially undermining public-interest regulation and democratic accountability.

IV. CONCLUSION

The rapid transformation of the global digital economy has fundamentally reshaped the conceptual foundations of international investment law. Bilateral Investment Treaties (BITs), originally drafted to protect physical, capital-intensive investments, increasingly confront new challenges posed by technology and media industries whose core assets are intangible, data-driven, and globally mobile. The rise of digital platforms, artificial

94 Valentina Vadi, *Cultural Heritage in International Investment Law and Arbitration* (Cambridge: Cambridge University Press, 2014), 41–44.

intelligence systems, cloud infrastructures, and cross-border data processing facilities demands a reconfiguration of investment protection standards to reflect the unique operational characteristics of digital enterprises. This article demonstrates that traditional BIT principles-most notably **fair and equitable treatment (FET)**, **national treatment (NT)**, **most-favored-nation (MFN)**, and **protection against indirect expropriation**-were never designed with digital assets in mind. Their historical interpretation often reflects assumptions rooted in territoriality and physical presence that no longer hold true in a world where digital platforms can operate across multiple jurisdictions without tangible infrastructure. As a result, applying classical BIT doctrines to digital-era investments creates profound legal uncertainties and risks undermining the regulatory sovereignty of host states. Analysis of jurisprudence at the intersection of digital regulation and cross-border legal conflict reinforces these challenges. The **Yahoo! Inc. v. LICRA and UEJF** case illuminates the complexity of reconciling territorially grounded media regulation with the borderless nature of online platforms. The case illustrates how multiple states may seek to assert jurisdiction over the same digital activity, imposing conflicting obligations on global media companies. If interpreted within the traditional BIT context, such regulatory assertions could mistakenly be construed as violations of investor protections, thereby discouraging legitimate public-interest regulation. Similarly, the landmark **Schrems I (2015)** and **Schrems II (2020)** decisions of the Court of Justice of the European Union (CJEU) underscore the importance of safeguarding fundamental rights-particularly data protection-in an era where surveillance, algorithmic governance, and digital profiling have become ubiquitous. These decisions demonstrate that states have both the duty and the authority to regulate cross-border data flows in order to protect privacy and national security. Crucially, such measures cannot be subordinated to investor expectations or narrowly interpreted treaty obligations. Instead, they illustrate the necessity for investment treaties to incorporate robust digital-era carve-outs and regulatory safeguards. This article further evaluates Indonesia's position in this evolving landscape. With the enactment of **UU PDP**, amendments to **UU ITE**, and the issuance of **PP 71/2019**, Indonesia has adopted a more assertive approach to digital sovereignty. These laws aim

to ensure that personal data, platform governance, and digital infrastructures are regulated to protect national interests, public order, and public morals. However, without appropriate adjustments to Indonesia's BIT framework, such domestic regulatory measures may expose the state to potential investor-state dispute settlement (ISDS) claims. Overall, the research concludes that BIT reform in the digital era is not merely advisable but essential. The strategic nature of digital technologies, the critical importance of data governance, and the heightened relevance of media content regulation necessitate a balanced treaty framework that adequately protects state sovereignty while also providing predictability for investors. Modern BITs must therefore evolve beyond their 20th-century origins to address 21st-century realities.

STATE OF THE ART AND NOVELTY

Scholarly discussions on the interaction between international investment law, digital technology, and state regulation have developed along several distinct but largely unintegrated trajectories. Existing literature can be broadly classified into three dominant strands: (1) traditional BIT doctrine, (2) digital sovereignty and data protection studies, and (3) internet and media regulation scholarship. While each strand contributes important insights, none provides a comprehensive framework addressing the regulatory implications of Bilateral Investment Treaties (BITs) in the context of technology and media governance.

1. Classical International Investment Law Scholarship

   One of the most influential works in this field is:

   Dolzer, Rudolf, and Christoph Schreuer. Principles of International Investment Law.

   First published in 2008 (2nd ed. 2012; 3rd ed. 2022). Oxford: Oxford University Press.

   This work represents the doctrinal cornerstone of international investment law, systematically elaborating core investment protection standards such as fair and equitable treatment, indirect expropriation, national treatment, and investor–state dispute settlement (ISDS). Investments are predominantly conceptualized as **tangible, territorially located, and**

capital-intensive economic activities, reflecting the industrial and extractive origins of BITs.

Despite its doctrinal sophistication, this scholarship does not engage with **digital investments as a qualitatively different category**. Intangible assets such as data, algorithms, platforms, and cloud infrastructures are not examined as central objects of investment protection, nor are the regulatory challenges arising from borderless digital business models addressed. As a result, classical BIT scholarship remains insufficiently equipped to explain regulatory conflicts in the digital and media sectors.

2. **Digital Sovereignty and Data Protection Literature**

A second strand of literature focuses on digital sovereignty and data protection, exemplified by:

Kuner, Christopher. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2013.

Kuner's work is a seminal contribution to global data protection scholarship, analyzing the regulation of cross-border data transfers, the protection of personal data as a fundamental right, and the extraterritorial reach of domestic privacy laws. The book situates data protection within constitutional law, human rights law, and internet governance, emphasizing states' increasing regulatory authority over digital infrastructures.

3. **Internet and Media Regulation Scholarship**

A third influential strand concerns internet governance and media regulation, particularly jurisdictional conflicts arising from online activities, as illustrated by:

Goldsmith, Jack, and Tim Wu, Who Controls then Internet? Illusions of a Borlerless World. Oxford: Oxford University Press, 2006.

Goldsmith and Wu challenge the notion of a borderless internet by demonstrating how states continue to assert regulatory authority over online content and platforms. Through case studies such as *Yahoo! Inc. v. LICRA*, the authors analyze conflicts of laws, territorial jurisdiction, and the reassertion of state sovereignty in cyberspace.

While foundational for understanding media regulation and internet jurisdiction, this literature does not address **digital platforms as foreign**

investors nor examine how regulatory measures might be reframed as violations of BIT standards. As such, the investment law dimension of media and platform regulation remains absent.

However, this body of literature largely remains **detached from international investment law**. Data protection measures are treated as autonomous regulatory instruments, without systematic consideration of how they may interact with BIT obligations or be challenged by foreign investors through ISDS. Consequently, the investment law implications of digital sovereignty remain underexplored.

Novelty of the Present Article

Against this fragmented state of the art, the article *"Bilateral Investment Treaties in the Digital Era: Implications for Technology and Media Regulation"* offers a **distinct and original contribution**.

First, unlike classical BIT scholarship, the article conceptualizes **digital investments as structurally different from traditional investments**, emphasizing data, platforms, algorithms, and digital infrastructures as core investment assets. It demonstrates that these characteristics undermine the territorial and physical assumptions embedded in existing BIT doctrines.

Second, in contrast to digital sovereignty and data protection literature, the article explicitly situates **privacy, cybersecurity, and data localization measures within the framework of international investment law**. By analyzing cases such as *Schrems I* and *Schrems II*, the article shows that data protection is not merely a policy preference but a constitutionalized regulatory obligation that must be safeguarded against potential investment claims.

Third, departing from internet and media regulation scholarship, the article reframes content moderation and platform regulation—illustrated through the *Yahoo!* case—as potential **investment treaty disputes**. This approach reveals how regulatory enforcement in the digital public sphere could expose states to ISDS claims in the absence of explicit treaty safeguards.

The core novelty of the article lies in its **integrative and reform-oriented framework**, which bridges international investment law, digital sovereignty, and media regulation. Rather than analyzing these domains in isolation, the

article demonstrates their intersection and proposes **explicit treaty-level carve-outs and exceptions** for data protection, cybersecurity, and media governance. In doing so, it advances both theoretical scholarship and policy-oriented debate on how BITs must evolve to remain legitimate and effective in the digital era.

REFERENCES

Bracha, O., & Pasquale, F. (2020). *Federalism and digital regulation: The growing role of states in the data economy*. Yale Journal on Regulation, 37(4), 1–35.

Bradford, A., Elsig, M., & Raess, D. (2021). *Digital economy governance: New frontiers in trade and investment policy*. Journal of International Economic Law, 24(2), 1–28.

Burri, M., (2015), *Cultural Diversity and International Economic Law*, in *Research Handbook on Cultural Diversity and International Economic Law*, ed. Valentina Vadi and Hilde Van den Bossche (Cheltenham: Edward Elgar.

Chander, A., (2005), *Globalization and Distrust*, Yale Law Journal 114, no. 6.

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism*. Oxford University Press.

Court of Justice of the European Union, *Case C-362/14, Maximillian Schrems v Data Protection Commissioner*, Judgment of 6 October 2015.

Court of Justice of the European Union, *Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment of 16 July 2020.

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Dolzer, R., & Schreuer, C. (2012). *Principles of international investment law* (2nd ed.). Oxford University Press.

Goldsmith, J., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford University Press.

Haikal, K.M., Foreign Investment Protection Post – Indonesia's Bilateral Investment Treaties Regime, Research Paper, Tilburg University.

Juwana, H., (2021), *State Sovereignty and Digital Regulation in Indonesia, Indonesian* Journal of International Law, 18, (3)

Jacob, M., Schill, S. W., & Wushke, A. (2020). *Modernizing international investment law: Reforming the definition of investment.* Journal of International Economic Law, 23(4), 1–25. Jacob, K., Peterson, L., & Rankin, D. (2020). Reforming ISDS in the digital age: A comparative analysis. Journal of International Economic Law, 23(4), 612–645.

John B. **& Rajuroy A.,** (2025), *Data as Capital: Integrating Digital Intangible Assets into Enterprise Value and Investment Decision-Making*, https://www.researchgate.net/publication/392774137

Kuner, C. (2017). *Transborder data flows and data privacy law*. Oxford University Press.

Kurtz, J. (2016). *The WTO and international investment law: Converging systems*. Cambridge University Press.

Lynskey, O., (2020), *Schrems II, Surveillance, and the Future of Transatlantic Data Transfers*, Common Market Law Review 57, 6.

Muchlinski, P. T. (2007). *Multinational enterprises and the law* (2nd ed.). Oxford University Press.

Newcombe A. and Paradell L., Law and Practice of Investment Treaties: Standards of Treatment (2009), Alphen aan den Rijn: Kluwer Law International.

Price, M. E., (2002), *Media and Sovereignty* (Cambridge, MA: MIT Press,

Reidenberg, J. R., (2005), *Technology and Internet Jurisdiction*, ˆ153, no. 6

Riswandi, B.A., (2021), Hukum Siber dan Transformasi Digital di Indonesia, Yogyakarta: UII Press.

Sadowski, J., (2019), *When Data is Capital: Datafication, Accumulation, and Extraction*, Big Data & Society 6, No. 1, 1-12, https://doi.org/10.1177/2053951718820549

Schill, S. W. (2019). *Reforming international investment law: Balancing investor protection and the right to regulate*. International and Comparative Law Quarterly, 68(4), 1–30.

Siregar, R. (2022). Indonesian data protection law and digital sovereignty. *Indonesia Law Review, 12*(1).

Svantesson, D., (2017), *Solving the Internet Jurisdiction Puzzle* , Oxford: Oxford University Press,

Tambini, D. (2021). *Media freedom, regulation, and the public sphere in the digital age*. Cambridge University Press.

Vadi, V., (2014), Cultural Heritage in International Investment Law and Arbitration, Cambridge: Cambridge University Press.

Zuboff, S. (2019). *Surveillance Capitalism and the Challenge of Collective Action*. New Labor Forum, 28(1), 10-29.

UNCTAD, (2012), *World Investment Report 2012: Towards a New Generation of Investment Policies* (Geneva: United Nations.

UNCTAD. (2023). *World investment report 2023: Investment in the digital economy*. United Nations Conference on Trade and Development.

Yahoo! Inc. v. LICRA and UEJF, 433 F.3d 1199 (9th Cir. 2006); Court of Justice of the European Union

Indonesian Regulations

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)* (beserta perubahannya).

Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP)*.

Pemerintah Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE)*.