

Guidebook on Digital Enforcement to Improve Fight Trademark Counterfeiting

APEC Intellectual Property Rights Experts Group

May 2025



**Asia-Pacific
Economic Cooperation**



**Asia-Pacific
Economic Cooperation**

Guidebook on Digital Enforcement to Improve Fight Trademark Counterfeiting

APEC Intellectual Property Rights Experts Group

May 2025

APEC Project: IPEG 201 2023A

Produced by
Oscar Montezuma Panez

and Project Overseer
Angela Vizcarra Pacheco
National Institute for the Defense of Competition and the Protection of
Intellectual Property (INDECOPI)

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

© 2025 APEC Secretariat

APEC#225-CT-03.2

INDEX

ACRONYMS LIST	3
EXECUTIVE SUMMARY	6
INTRODUCTION	8
BACKGROUND.....	13
1. <i>Importance of e-commerce worldwide.....</i>	<i>13</i>
2. <i>Importance of e-commerce in the APEC region</i>	<i>18</i>
3. <i>The evolution of trademark counterfeiting in the global landscape</i>	<i>23</i>
4. <i>Main definitions on enforcement in the digital environment.....</i>	<i>26</i>
ANALYSIS OF THE CURRENT TRADEMARK COUNTERFEITING LANDSCAPE AND KEY BARRIERS.....	30
1. <i>Key trademark counterfeiting modalities in the digital environment.....</i>	<i>30</i>
2. <i>Main barriers and challenges to combat the digital counterfeiting of trademarks in e-commerce platforms</i>	<i>41</i>
3. <i>Highlights from surveys results</i>	<i>46</i>
RECOMMENDATIONS.....	49
1. <i>Assessing the liability of online intermediaries</i>	<i>49</i>
2. <i>Guidelines and voluntary documents for digital platforms</i>	<i>55</i>
3. <i>Digital forensics for IP rights enforcement.....</i>	<i>60</i>
4. <i>IP owners and digital platforms collaboration.....</i>	<i>64</i>
5. <i>Cooperation between private stakeholders and government authorities.....</i>	<i>71</i>
6. <i>Coordination between private stakeholders and Top-Level Domains operators to combat trademark counterfeiting.....</i>	<i>78</i>
7. <i>Common frameworks alignment to combat trademark counterfeiting</i>	<i>82</i>
8. <i>Enforcement mechanisms across jurisdictions for cross-border measures in the digital environment</i>	<i>86</i>
9. <i>Detection and monitoring tools.....</i>	<i>90</i>
10. <i>Tracking and IP protection technologies.....</i>	<i>97</i>
CASES OF STUDY	101
1. <i>Aura Blockchain</i>	<i>101</i>
2. <i>Collaboration through INTA To Go.....</i>	<i>109</i>
3. <i>Alibaba Anti-Counterfeiting Alliance (AACA)</i>	<i>118</i>
4. <i>KIPO's Anti-Counterfeit Council.....</i>	<i>127</i>
5. <i>Indecopi - Mercado Libre Cooperation Agreement</i>	<i>135</i>
CONCLUSION.....	141

REFERENCES	143
ANNEX 1: APEC SURVEY FOR IP OWNERS AND CONSUMERS.....	147
<i>People's Republic of China.....</i>	<i>148</i>
<i>Republic of Korea.....</i>	<i>159</i>
<i>Peru.....</i>	<i>170</i>
<i>The Philippines.....</i>	<i>239</i>
<i>Chinese Taipei.....</i>	<i>306</i>
ANNEX 2: APEC SURVEY FOR IP POLICY MAKERS	316
<i>Australia.....</i>	<i>317</i>
<i>Chile.....</i>	<i>332</i>
<i>Hong Kong, China.....</i>	<i>347</i>
<i>Japan.....</i>	<i>362</i>
<i>Republic of Korea.....</i>	<i>379</i>
<i>Mexico.....</i>	<i>392</i>
<i>Papua New Guinea.....</i>	<i>403</i>
<i>Peru.....</i>	<i>418</i>
<i>The Philippines.....</i>	<i>435</i>
<i>Chinese Taipei.....</i>	<i>506</i>
<i>United States.....</i>	<i>519</i>

ACRONYMS LIST

A

Alibaba Anti-Counterfeiting Alliance: AACA
Agreement on Trade-Related Aspects of Intellectual Property Rights: TRIPS Agreement
Anti-Counterfeiting Group: ACG
Application Programming Interface: API
Artificial intelligence: AI
Asia-Pacific Economic Cooperation: APEC
Automated content recognition: ACR

B

Business-to-Consumer: B2C
Business-to-Government: B2G
Business-to-Business: B2B

C

Civil society organizations: CSOs
Compound annual growth rate: CAGR
Consumer-to-Consumer: C2C
Country code Top-Level Domain: ccTLD

D

Digital Services Act: DSA
Domain Name System: DNS

E

European Registry for Internet Domains: EURid
European Union: EU
European Union Intellectual Property Office: EUIPO
European Union's Intellectual Property Enforcement Portal: IPEP

G

General Trade-Related Index of Counterfeiting for Products: GTRIC-p
Generic Top-Level Domains: gTLDs
German Network Information Center: DENIC
Gross Domestic Product: GDP

I

Information Technology: IT
Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act:
INFORM Consumers Act
Intellectual property: IP
Intellectual Property Rights Experts Group: IPEG
International Anti-Counterfeiting Coalition: IACC
International Trademark Association: INTA
Internet Corporation for Assigned Names and Numbers: ICANN
Internet Domain Registration Netherlands Foundation: SIDN
Internet of things: IoT

Internet Services Providers: ISPs
Interpol Intellectual Property Crime Action Group: IIPCAG

J

Japan Patent Office: JPO

K

Korean Intellectual Property Office: KIPO

M

Massachusetts Institute of Technology: MIT
Memorandum of Understanding: MoU
Micro, small and medium-sized enterprises: MSMEs
Mexican Institute of Industrial Property: IMPI

N

National Institute for the Defense of Competition and the Protection of Intellectual Property: Indecopi
National Bureau of Investigation: NBI
National Institute of Standards and Technology Glossary: NIST
Non-governmental organizations: NGOs

O

Online dispute resolution: ODR

P

Pacific Economic Cooperation Council: PECC
Pay per action: PPA
Proof-of-Authority: PoA
Public-Private Partnership: PPP

S

Search Engine Marketing: SEM
Search Engine Optimization: SEO
Software as a Service: SaaS
Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce: SHOP
SAFE Act

T

The Onion Router: TOR
Trademark Administrators: TMA
Trademark Clearinghouse: TMCH

U

Uniform Domain Name Dispute Resolution Policy: UDRP
United Nations Commission on International Trade Law: UNCITRAL
United Nations Development Program: UNDP
Uniform Resource Locators: URLs

V

Very large online platforms: VLOPs

Very large online search engines: VLOSEs

W

World Customs Organization: WCO

World Trade Organization: WTO

World Intellectual Property Organization: WIPO

EXECUTIVE SUMMARY

The objective of this Guidebook is to improve the capability of Asia-Pacific Economic Cooperation (APEC) economies to implement, enhance, and develop measures to combat trademark counterfeiting in the digital environment. As a result, this will have an impact on strengthening the digital enforcement system for the protection of trademark rights in e-commerce throughout the region and increasing confidence in digital commerce.

Indeed, this document aims to enhance APEC economies' capabilities to design, implement, or improve measures to combat trademark counterfeiting, thereby increasing trust in digital transactions. The approach employed involves a review of legislative frameworks and scholarly literature, statistical analysis, surveys of intellectual property (IP) enforcement authorities and other relevant stakeholders, and in-depth interviews to collect qualitative perspectives. Case studies from selected APEC and non-APEC economies demonstrate successful enforcement actions and joint efforts.

The document begins with an overview of the importance of e-commerce internationally and within the APEC region, assesses the current situation and key findings, and examines counterfeiting methods and key barriers to combating digital trademark counterfeiting. It concludes with recommendations and best practices, supported by case studies, and summarizes lessons learned.

The Guidebook provides 10 recommendations to address different challenges. These can be divided into three groups, including legal enforcement, digital enforcement and stakeholder cooperation recommendations.

The goal of the legal enforcement recommendations is to establish a robust legal framework that enhances the ability of stakeholders in APEC economies to combat trademark counterfeiting in the digital environment. This group includes recommendations such as:

- Assessing the liability of online intermediaries
- Guidelines and voluntary documents for digital platforms
- Common frameworks alignment to combat trademark counterfeiting
- Enforcement mechanisms across jurisdictions for cross-border measures

The digital enforcement recommendations aim to leverage advanced technologies to enhance the detection, monitoring, and enforcement of IP rights in the digital ecosystem. This group includes recommendations such as:

- Digital forensics for IP rights enforcement
- Detection and monitoring tools
- Tracking and IP protection technologies

The stakeholder's cooperation recommendations emphasize the importance of collaborative efforts between various entities, including IP owners, digital platforms, government authorities, and local code top-level domain operators. This group includes recommendations such as:

- Collaboration between trademark owners and digital platforms
- Cooperation between private stakeholders and government authorities
- Coordination between private stakeholders and Top-Level Domains operators to combat trademark counterfeiting

Finally, the case studies included in the Guidebook serve to illustrate the diverse and innovative approaches that can be employed to combat trademark counterfeiting in the digital environment. These examples highlight the practical application of advanced technologies, collaborative efforts, and strategic partnerships.

By showcasing successful initiatives from various stakeholders, the case studies provide actionable insights and best practices that can be adopted by APEC economies. This helps to reinforce the Guidebook's main objective of enhancing the capabilities of stakeholders to effectively address and mitigate the challenges posed by digital trademark counterfeiting.

INTRODUCTION

The global marketplace has undergone drastic changes year after year, and as companies have adapted to new challenges, e-commerce has become a vital lifeline, enabling businesses of all sizes—from major department stores to small local shops—to connect with customers. Consumer behavior and corporate practices have been permanently transformed by this digital revolution, which has proven to be far more than a temporary solution. The growth of online shopping and the reliance on digital platforms and social media for transactions have fundamentally reshaped commerce.

However, this shift has brought challenges. Alongside legitimate businesses, criminal organizations have discovered profitable opportunities in the internet marketplace. Primarily involved in the production and distribution of counterfeit goods, these groups have quickly adapted their operations to exploit the online space.

The anonymity, relative ease of establishing online stores, and reduced operational costs have made it easier for counterfeiters to reach unsuspecting and vulnerable customers. This creates a dual problem: while e-commerce offers consumers unprecedented access to products, the online presence of counterfeit goods increases the risk for consumers of encountering these products, compromising both their safety and brand integrity.

Enforcement agencies tasked with protecting trademark rights face significant challenges in the rapidly evolving digital landscape. Many existing policies and procedures are rooted in traditional business models, which often struggle to accommodate the unique dynamics of online transactions.

Limited resources and capacity constraints further complicate the monitoring and enforcement of regulations against online market players, enabling counterfeiters to operate with varying degrees of impunity. This not only undermines consumer trust but also jeopardizes the reputation and financial stability of IP owners.

However, upon recognizing these challenges, some economies have swiftly taken action to enhance and strengthen digital enforcement against trademark counterfeiting. A notable example is the strategy implemented by the Peruvian National Institute for the Defense of Competition and the Protection of Intellectual Property (Indecopi), who promote cooperation

agreements with major online marketplace platforms, such as "Mercado Libre". This collaboration enables coordinated efforts to identify and combat instances of digital trademark infringement. Through this joint approach, Peruvian authorities have made significant strides in curbing online trademark counterfeiting, demonstrating the positive impact of mutual support between authorities and key private sector players.

Within this context, it was precisely the experience of cooperation between Indecopi and Mercado Libre that aroused the interest of Peru to develop a project which addresses the problem around trademark counterfeiting in digital marketplaces and other platforms related to e-commerce.

Indeed, the project titled IPEG_201_2023A: "Guidebook on digital enforcement to improve fight trademark counterfeiting" seeks to address this problem by developing a comprehensive Guidebook, offering a valuable resource for APEC economies. The expected outcomes of this project are, in the first instance, to strengthen the capacity of APEC economies' officials to implement, enhance and develop effective measures to combat the increasing prevalence of trademark counterfeiting in the digital environment. Secondly, to increase the knowledge of APEC economies on how to address the challenges of regulating e-commerce in order to help them strengthen the digital enforcement system throughout the region and enhance confidence in digital commerce.

As an end product of the project, this Guidebook has been elaborated, which encompasses a thorough investigation into the current landscape of trademark counterfeiting in the digital environment. It aims to provide a comprehensive overview of existing enforcement mechanisms and highlight successful strategies adopted by different economies, both APEC members and non-members. By focusing on public and private sector initiatives, this Guidebook fosters a deeper understanding of how various stakeholders can collaborate effectively to combat counterfeiting online.

To fulfill these objectives, a comprehensive methodology is employed, incorporating various research methods and data collection techniques. This approach ensures that the Guidebook is grounded in solid evidence and reflects the diverse experiences of APEC economies.

A. Doctrine, regulations, and literature analysis

A thorough examination of relevant legal frameworks and academic literature is conducted to inform best practices in digital enforcement. This includes reviewing existing laws related to IP, as well as scholarly articles that discuss the impact of e-commerce on trademark enforcement.

B. Review of statistical information

A detailed analysis of statistical data related to trademark counterfeiting and enforcement helps establish a clearer understanding of the current state of the digital marketplace. This quantitative data highlights trends in counterfeiting activities and enforcement outcomes, informing recommendations for effective action.

C. Research and data collection surveys

Two targeted surveys were distributed among APEC economies. The first survey focused on IP enforcement authorities and private sector representatives who are directly engaged in implementing measures to combat trademark counterfeiting in the digital environment. This survey gathers insights on existing strategies, successes, and challenges faced in enforcement efforts.

The second survey aimed at IP right owners and e-commerce consumers seeks to understand their experiences with enforcement measures and their perceptions on the effectiveness of various strategies taken.

By collecting data from both enforcement authorities and stakeholders directly affected by trademark counterfeiting, the Guidebook ensures a comprehensive understanding of the issue from multiple perspectives.

D. Selection of economies for case studies

Based on the expressed interest of economies and the findings of the literature review, case studies were selected to showcase successful enforcement initiatives and collaborative efforts that have made a meaningful impact in combating trademark counterfeiting in the digital space. These case studies not only provide practical insights

into the implementation of effective strategies but also serve as a valuable foundation for the recommendations proposed in this Guidebook.

E. In-depth interviews

Where necessary, in-depth online interviews were conducted to gather qualitative insights from stakeholders involved in IP enforcement and e-commerce. These interviews provided a deeper context and allowed discussions on best practices, challenges faced and the impact of specific anti-counterfeiting measures.

The resulting Guidebook will serve not only as an information repository but also as a practical tool for APEC economies seeking to enhance their enforcement efforts. It will provide voluntary recommendations tailored to the unique challenges faced by various economies in the digital marketplace.

The Guidebook will encompass a range of topics, including a clear overview of the importance of e-commerce both globally and within the APEC region, along with an overview of the evolution of trademark counterfeiting in the digital environment. Following this, an analysis of the current situation will be presented, highlighting key findings, identifying relevant counterfeiting modalities, and addressing the primary barriers and challenges to combating digital trademark counterfeiting.

After this opening section, the Guidebook will focus on providing recommendations and identifying best practices, each aimed at enhancing knowledge on combating trademark counterfeiting in the digital sphere. Successful experiences will be illustrated through notable case studies, culminating in the overall conclusions of the research and lessons learned throughout the process.

The project's overall goal is to catalyze positive change within APEC economies, boosting their capacity to combat digital trademark counterfeiting while fostering the exchange of successful cases and experiences. By strengthening digital enforcement systems and promoting collaboration between the public and private sectors, the project aims to enhance consumer confidence in e-commerce, enabling individuals to engage in online transactions with the assurance of purchasing genuine products.

Ultimately, this initiative seeks to create a safer, more reliable digital marketplace where innovation and commerce can thrive without the threat of counterfeit goods undermining legitimate businesses and eroding consumer trust. Through actionable insights and by fostering collaboration among APEC economies, the Guidebook aspires to make a significant contribution to the ongoing fight against trademark counterfeiting in the digital environment.

BACKGROUND

1. Importance of e-commerce worldwide

The rise of the Internet in the mid to late 1990s laid the groundwork for the e-commerce revolution, a period that quickly captured the attention of law and policymakers around the world. Early predictions highlighted the potential benefits of e-commerce, particularly in terms of improving the efficiency of various business functions such as inventory management, supply chain operations and customer service.

For consumers, e-commerce promised improved access to information and the possibility of more direct involvement in key business activities, including product design. In addition, the digital space was expected to reduce the distance between producers and consumers, thereby eliminating traditional intermediaries such as retailers and wholesalers, which would reduce costs and facilitate market entry for new firms (OECD, 2019, p. 15).

A digital space devoid of hierarchies and centralized controls was ideal for all kinds of information transmission without any barriers, including those that could pose a risk to the protection of IP rights.

However, the idea that e-commerce would completely replace traditional intermediaries was soon tempered by the recognition that new types of intermediaries were needed to establish trust in online transactions. Authentication and certification services emerged as essential tools for securing e-commerce environments. At the same time, analysts began to raise concerns about the growing importance of customer data, which, while valuable for competitive advantage, also presented significant privacy risks. In addition, network externalities and economies of scale were expected to create competitive challenges, with the potential to stifle innovation as large players consolidated market power (OECD, 2019, p. 16).

From the early days of e-commerce, analysts predicted that the decentralization of commercial activity across geographic and political borders would introduce significant policy challenges. The digital nature of these transactions, especially those involving intangible products, blurred the lines between domestic and foreign commerce, making regulatory oversight more difficult. The analysts identified four key areas where government policies could potentially limit the growth of e-commerce: access, trust, regulatory uncertainty, and logistical issues. In addition, they recognized that the lack of physical interaction with products could increase information

asymmetries, placing consumers at a disadvantage if they cannot evaluate goods first-hand (OECD, 2019, p. 18).

With the rapid acceleration of digital transformation, many of these predictions have materialized. However, the pace at which e-commerce has evolved has likely surpassed even the most optimistic expectations. Today, the landscape is more dynamic than ever, offering new opportunities to drive economic growth and improve consumer welfare. Realizing these benefits, however, requires a nuanced understanding of modern e-commerce, how it is measured, and what policies foster further innovation and development in this rapidly changing market (OECD, 2019, p. 16).

In this context of rapid digitization, developing economies risk being left behind and missing out on key opportunities in digital trade and the broader digital economy. The gap can be significant: in Europe, for example, more than 80% of internet users shop online, while in many least developed economies less than 10% do so. This disparity in digital readiness not only limits the participation of developing economies in the global digital marketplace, but also threatens to exacerbate existing digital gaps (OECD, 2021, p. 69).

Moreover, the existence of this gap makes it more difficult to increase the level of enforcement of the law on digital spaces in less digitally ready economies. Indeed, governments in these regions often face a lack of specialized resources, as they prioritize basic infrastructure over the specific tools and personnel needed for effective digital enforcement. Additionally, the low adoption of e-commerce by local businesses reduces the demand for robust digital legal frameworks. Finally, limited online participation weakens their integration into global digital networks, complicating cross-border cooperation that is essential to address legal challenges in digital trade.

In fact, if digital transformation is not managed effectively, businesses in these regions could fail to integrate into global value chains and miss out on the growing opportunities of digital trade. The widening gap underscores the urgent need for international cooperation, especially as current levels of development assistance are insufficient to address these challenges.

Innovative partnerships among the global community, including bilateral development agencies, are essential to closing such gaps. Strengthening legal frameworks to build online trust, developing skills for the digital economy, fostering digital entrepreneurship, and promoting digital financial inclusion are all critical steps that, while time-consuming, must be

prioritized to ensure that developing economies are not excluded from the digital future (OECD, 2021, p. 71).

The rise of e-commerce is not merely a trend but a fundamental transformation in the way people shop and interact with the market. By 2024, 20.1% of retail purchases worldwide took place online. This shift marks a broader movement away from physical stores as more consumers are fully embracing the convenience and accessibility of digital platforms. Businesses that recognize this evolution are decisively shifting their strategies, reallocating investments from brick-and-mortar locations to strengthening their online presence. The ability to offer a seamless and engaging online shopping experience is quickly becoming essential for survival in the modern retail landscape (Snyder, 2024). It should be noted that the growing attractiveness of e-commerce as the main form of commerce has not only reached legitimate retailers but also those business models based on counterfeiting.

Figure N° 1

Growth in retail e-commerce sales worldwide 2022-2027 (in trillions)



Source: Forbes Advisor, 2024, “35 E-Commerce Statistics of 2024”.

Looking ahead, the rapid growth of online shopping shows no indication of losing momentum. By 2027, it is estimated that 23% of all retail purchases will be made online, confirming that

this shift is not temporary. Furthermore, e-commerce growth extends beyond just retail, reflecting a broader digital transformation across industries.

In 2024, e-commerce sales increased by 8.8%, creating significant opportunities for businesses that took advantage of this growth. This outcome underscores both the current and future importance of this market dimension, as companies that succeeded in creating a streamlined and intuitive online experience positioned themselves to thrive in this rapidly evolving landscape (Snyder, 2024).

By the end of 2024, the e-commerce market reached a staggering USD 6.3 trillion, a significant leap from USD 5.8 trillion in the previous year. This surge reflects the virtually limitless potential for businesses to tap into new demographics beyond local boundaries, capitalizing on the accessibility of online platforms.

The ability to cater to diverse consumer bases, both locally and internationally, has become a cornerstone of modern retail strategies. By 2027, the global e-commerce market is expected to surpass USD 7.9 trillion, emphasizing the urgency for companies to establish or strengthen their online presence sooner rather than later. Those who invest early stand to reap considerable long-term benefits as digital commerce continues to evolve (Snyder, 2024).

Moreover, the global nature of e-commerce is evident in consumer behavior, with 52% of online shoppers making purchases from both local and international retailers. The ease of cross-border transactions and improvements in shipping logistics have diminished traditional geographic barriers, allowing consumers to access a wider variety of products. For businesses, including owners of trademarks and other IP rights, this presents an opportunity to tailor their offerings to international markets, expanding their customer base through strategic shipping options and localized online experiences (Snyder, 2024).

Due to the widespread use of mobile technologies, the e-commerce landscape has been significantly reshaped, making smartphones a central tool for online shopping. In fact, 91% of consumers now use their smartphones to make online purchases, underscoring the importance of optimizing digital platforms for mobile users.

While a seamless desktop shopping experience remains crucial, it's increasingly essential to prioritize mobile-friendly designs that ensure functionality and ease of use across devices. Businesses that fail to adapt to mobile trends risk alienating a substantial portion of their

customer base, as more consumers rely on their phones for everyday shopping activities (Snyder, 2024).

In the foreseeable future, the dominance of mobile commerce is only expected to grow. By 2027, mobile sales are projected to account for 62% of all retail e-commerce transactions, up from 56% in 2018. This shift highlights the need for businesses to invest in responsive web designs and mobile optimization strategies that cater to the growing number of mobile shoppers.

Simple navigation, thumb-friendly interfaces, and fast load times are now essential components of a successful e-commerce site. Those who adapt to these best practices will be well-positioned to capitalize on the booming mobile commerce market (Snyder, 2024). It must be considered, however, that the proliferation of e-commerce channels, such as mobile technologies, has also led to an increase in the marketing of counterfeit goods, as well as the emergence of new business models based on counterfeit goods.

Online marketplaces have emerged as a dominant force within the global e-commerce landscape, offering consumers unprecedented access to a vast array of products and third-party sellers. These platforms enhance the shopping experience by integrating features such as review systems, secure payment options, and efficient shipping services. Many also offer additional perks, including memberships and subscriptions, which further incentivize consumer loyalty. Notably, Amazon leads in global website traffic, while Taobao, operated by Alibaba, commands the highest value in goods sold through third-party sellers, highlighting the immense influence these platforms wield in the digital marketplace (OECD, 2022, p. 6).

While online marketplaces provide unparalleled convenience and a wide variety of choices, their misuse by certain individuals can introduce significant risks. Issues such as deceptive marketing, fraudulent schemes, counterfeit goods, and manipulated reviews have become more prevalent, especially as the COVID-19 pandemic has increased reliance on digital shopping. This shift has not only increased consumer exposure to these risks, but also exacerbated certain behavioral biases, further complicating the online shopping experience (OECD, 2022, p. 6). For example, manipulated reviews can lead consumers to trust information that matches their pre-existing beliefs about a product or service. Similarly, false claims of limited availability can deceive consumers and lead them to make hasty decisions.

2. Importance of e-commerce in the APEC region

Having laid out the facts that illustrate the rapid global growth of e-commerce and its inherent connection to trademark counterfeiting practices, it is crucial to underscore its significance for the economies within the APEC region. This focus will help us better understand the unique challenges faced by each economy and more effectively assess the escalating risks that online counterfeiting presents to them all.

Given the diverse membership of APEC, providing a detailed description of the situation in each economy is a challenge. Therefore, this analysis highlights the experiences of a selection of economies that offer valuable insights, both within the APEC region and their respective geographical areas: the People's Republic of China; Mexico; Peru; The Philippines; The Russian Federation; Singapore; and the United States.

The following section provides a concise overview of key aspects of trade in the digital environment, focusing on the size of the e-commerce market, growth rates, consumer behavior, such as preferred devices for online shopping, and the frequency of cross-border transactions.

A. People's Republic of China

China's business-to-consumer (B2C) e-commerce market, valued at USD 1.9 trillion, stands as the largest globally. Despite this, the potential for growth is clear, with e-commerce representing 30% of the economy's total retail trade, and users spending an average of USD 2,058 a year, which is only about half of what citizens of other e-commerce giants, such as the US and the UK, spend. The market maintained strong growth, achieving a compound annual growth rate (CAGR) of 16.6% through 2024. This expansion was fueled by the rapidly growing middle class, which had already reached 550 million people by 2022 (JP Morgan, 2024, p. 20).

A key feature of the People's Republic of China e-commerce landscape is its mobile-first nature, with 64% of transactions conducted on smartphones. Among these, 65% are made through mobile apps, making app optimization crucial for businesses entering the market. The dominance of social super-apps, such as WeChat, Pinduoduo, and Douyin, has reshaped e-commerce by incorporating live streaming, especially in sectors like

beauty, where this feature has become a central marketing tool (JP Morgan, 2024, p. 20).

Despite the vast choices available in China's domestic market, cross-border shopping remains significant. Around 39% of Chinese online consumers have made international purchases, with cross-border e-commerce representing 13.5% of the total market. The economies where Chinese consumers shop more often are Australia (14%); Japan (24%); and the US (12%). To facilitate this, China has implemented a "positive list" for approved e-commerce products that can be imported with minimal customs and regulatory requirements, alongside a favorable tax rate of 9.1%. These items must be processed through bonded warehouses before being delivered to buyers (JP Morgan, 2024, p. 21).

B. Mexico

Mexico's B2C e-commerce sector has experienced rapid growth, expanding by at least 20% each year since 2017. By 2024, the market reached a valuation of USD 38.9 billion and continued its expansion at a steady compound annual growth rate (CAGR) of 12.4%. This growth is driven by an increase in online transactions of more than USD 1 billion per year. With e-commerce accounting for only 9% of Mexico's total retail sales, there is significant untapped potential for further expansion as more consumers embrace e-commerce (JP Morgan, 2024, p. 11).

Mobile devices dominate the e-commerce landscape in Mexico, accounting for 53% of online purchases. The mobile commerce market, valued at USD 20.6 billion, has reached a robust CAGR of 20.3% by the end of 2024. This growth was fueled by widespread reliance on mobile networks, as many households opt for mobile Internet due to limited fixed line penetration, which currently stands at only 62.8% (JP Morgan, 2024, p. 11).

Mexico also offers significant opportunities for international merchants, with 66% of online consumers making cross-border purchases. Cross-border shopping now accounts for 15% of Mexico's total e-commerce, with the US as the top shopping destination (51%), followed by China (27%), and Japan (9%). Chinese companies are increasingly investing in the region, with Alibaba, for example, launching thrice-weekly

flights to Latin America in 2020, cutting delivery times for Chile; Mexico; and Brazil from one week to just three days (JP Morgan, 2024, p. 12).

C. Peru

In Peru, e-commerce makes a significant contribution to the local economy, accounting for 5.4% of its Gross Domestic Product (GDP). According to a report published by the Peruvian Chamber of Electronic Commerce (2024), in 2023, Peru joined the group of the largest e-commerce markets in Latin America, with approximately 332,000 businesses operating online and a consumer base of 16.8 million. This means that almost half of the population was buying online. Despite this impressive reach, the growth rate in 2023 was modest, with e-commerce volume increasing by only 7%. This slow growth —the lowest in more than a decade— was attributed to economic contraction, a decline in consumer spending, the resurgence of physical retail, and the social and political crises that affected the economy in the first quarter of the year (CAPECE, 2024, p. 20).

In terms of retail market penetration, e-commerce accounted for 8.6% of the total retail sector in 2023, up slightly from 8% in 2022. Internet usage also increased, with penetration rates rising to 78%, an increase of 4% over the previous year (CAPECE, 2024, p. 20). The number of internet-connected mobile phones increased by about 9% in 2022, reaching 29 million and covering 87% of the local population (CAPECE, 2024, p. 38). In addition, mobile devices play a crucial role in Peruvian e-commerce, accounting for 64% of total online sales (PCMI, 2024, p. 3).

Domestic e-commerce dominated the market, accounting for 77% of total online sales, and grew by 34% by 2024. Meanwhile, cross-border e-commerce also experienced significant growth, with a rate of 33% over the same period. This reflected the increasing willingness of Peruvian consumers to engage with international merchants (PCMI, 2024, p. 3).

D. The Philippines

The B2C e-commerce sector in the Philippines was expected to grow 12.26% from 2023 to 2027, reaching USD 22.5 billion by 2027. In 2023 alone, the e-commerce market grew by 27.8%, reaching USD 20.6 billion, and it continued with another 23.3% of growth in

2024, reaching USD 25.4 billion, exceeding previous expectations. Despite this impressive growth, e-commerce accounts for only 7% of total retail transactions in the Philippines, indicating significant room for development as more consumers transition to online shopping (Research and Markets, 2023).

Mobile devices play a critical role in the growth of e-commerce in the Philippines. With the widespread adoption of smartphones, consumers can shop on the go using easy-to-use apps and mobile payment options. This accessibility has made mobile shopping a dominant force in the market, further driving e-commerce penetration. By 2023, 88.2% of Filipinos were shopping online, demonstrating the significant reach of digital retail platforms (Research and Markets, 2023).

As e-commerce becomes an integral part of the retail landscape, its share of total retail sales is projected to grow from 7.5% currently to 9.5% by 2028. This trajectory underscores the transformative impact of e-commerce on consumer behavior and retail dynamics. With continued investment in technology and logistics, the sector is poised for sustained expansion, creating opportunities for both local and international merchants looking to tap into this burgeoning market (Research and Markets, 2023).

E. The Russian Federation

In 2023, the Russian online retail market reached a value of USD 72 billion, driven by a remarkable 5.03 billion orders (Data Insight, 2024). The number of orders increased by 78%, while the market value in rubles grew by 44%. This growth mirrors the patterns observed in 2022, but slightly exceeds previous forecasts. The average amount per transaction was USD 14, representing an increase of 18%. The Russian e-commerce market continued its growing path, reaching USD 94 billion in 2024, accounting for an increase of 30% (Data Insight, 2024).

Focusing on the B2C sector, online retail in the Russian Federation involves the purchase of physical goods over the Internet, with the transaction being completed through either websites or mobile applications, regardless of the payment or delivery method. These figures include transactions by Russian buyers from domestic sellers but exclude cross-border purchases and peer-to-peer trade. The total market volume includes consumer spending on products and delivery but does not include revenue from additional services such as advertising or financial services (Data Insight, 2024).

Mobile connectivity plays a significant role in Russian e-commerce, with 219.8 million active mobile connections recorded in early 2024, representing close to 1.5 active mobile connections for each inhabitant. At the same time, this way of commerce holds a significant share of the market, accounting for 39% of total e-commerce activity, which is considered a strong presence (Konopliov, 2024).

F. Singapore

Singapore's B2C e-commerce market, valued at USD 5.8 billion, has seen consistent year-on-year growth, although the COVID-19 pandemic temporarily disrupted this trend due to its impact on travel and tourism. E-commerce now accounts for 11% of total retail sales, and 68% of the population has made online purchases. Despite a relatively high penetration rate of online shoppers, e-commerce's share of total retail sales remained modest, leading to a conservative CAGR of 8.7% through 2024. However, Singaporeans demonstrated significant spending when shopping online, with an average annual basket of USD 1,442, positioning them among the highest spenders in the region (JP Morgan, 2024, p. 44).

In 2020, mobile commerce surpassed desktop-based shopping in Singapore, with 51% of e-commerce transactions conducted via mobile devices, representing a USD 3 billion market. This sector continued to grow at a CAGR of 10.1% through 2024 and is expected to grow further, bolstered by the Singapore government's initiative to roll out two ultra-fast 5G networks by the end of 2025, thereby enhancing mobile shopping capabilities (JP Morgan, 2024, p. 44).

Cross-border shopping is particularly prevalent in Singapore, where 78% of online consumers have made purchases from international merchants. In fact, Singaporeans are more likely to shop internationally than domestically, with cross-border e-commerce accounting for 55% of total online sales. The most popular economies for Singaporean consumers to shop from are China (47%); Republic of Korea (15%); and the United States (31%). In addition, Singapore's robust air and road infrastructure enables efficient delivery of international purchases, further facilitating the participation of this economy in global e-commerce (JP Morgan, 2024, p. 44).

G. United States

E-commerce plays a pivotal role in the US economy, accounting for 14% of total retail sales. With 77% of the population shopping online, the US market, valued at an impressive USD 1.1 trillion, is a vital space for international merchants. The US e-commerce sector continued its robust growth, achieving a CAGR of 11.2% through 2024. This expansion was driven in part by the increased adoption of app-based ordering and curbside pickup, practices that surged in popularity during the COVID-19 pandemic as legacy mall brands adapted to new consumer behaviors (JP Morgan, 2024, p. 14).

Mobile commerce, which accounted for 45% of all United States e-commerce, has surpassed desktop sales, growing at a CAGR of 18.2% through 2024 (JP Morgan, 2024, p. 14). Although cross-border shopping is less prevalent in the US than in other economies —likely due to the size of the domestic e-commerce market— international sales still represent a significant USD 76.9 billion market. While only 33% of US consumers shop abroad, the growth of cross-border e-commerce is notable, with sales up 42% year-over-year in May 2020, compared to just 1% growth in January of that year (JP Morgan, 2024, p. 15).

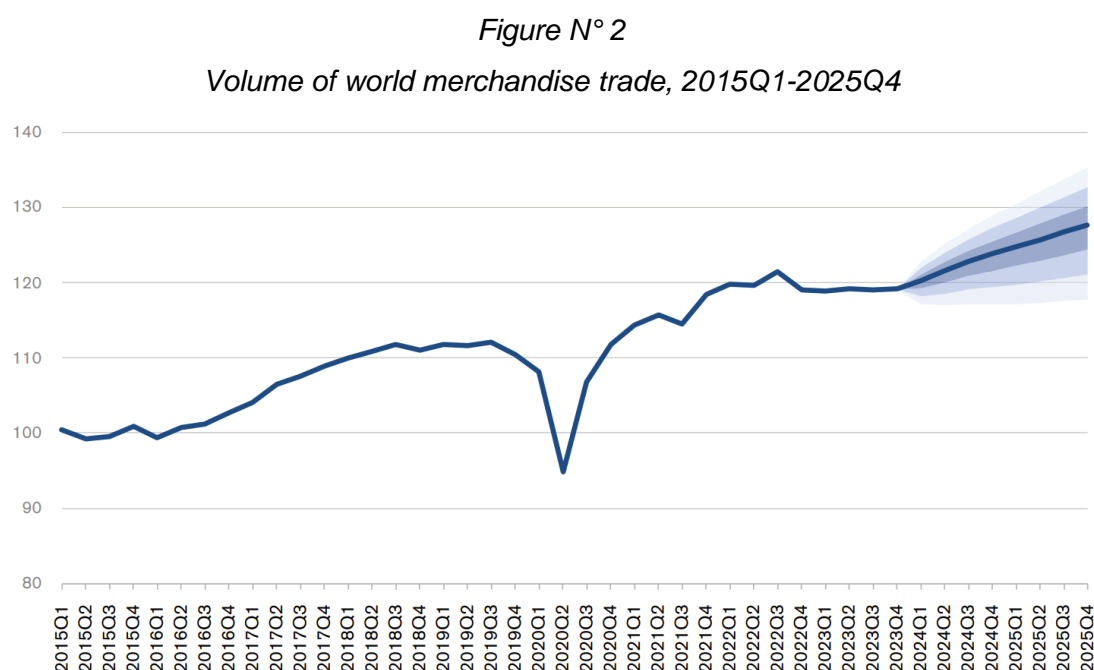
By examining the unique configuration of each economy's e-commerce market, we can better grasp the severity of IP rights violations in the APEC region. Trademark counterfeiting through digital channels, in particular, reveals a strong correlation between the scale of certain digital marketplaces and the increasing prevalence of these illegal activities. The following section delves into the global evolution of such practices over time, offering a broader perspective on this pressing issue.

3. The evolution of trademark counterfeiting in the global landscape

Global trade trends prior to the COVID-19 pandemic reveal a dynamic and changing market, particularly in relation to trade in infringing products. Over the past decade, economic developments have had a significant impact on the market for counterfeit goods, and these key trends are expected to shape the future of this illicit trade (OECD/EUIPO, 2021, p. 13).

During this decade, after the COVID-19 pandemic, the recovery of the volume of the world merchandise trade showed a significant recovery to pre-pandemic levels. Overall, it can be said that in 2022, the trade volume expanded by 3.0%, followed by a slight contraction of 1.2%, which turned into a plateau instead of continuing on a downward trajectory.

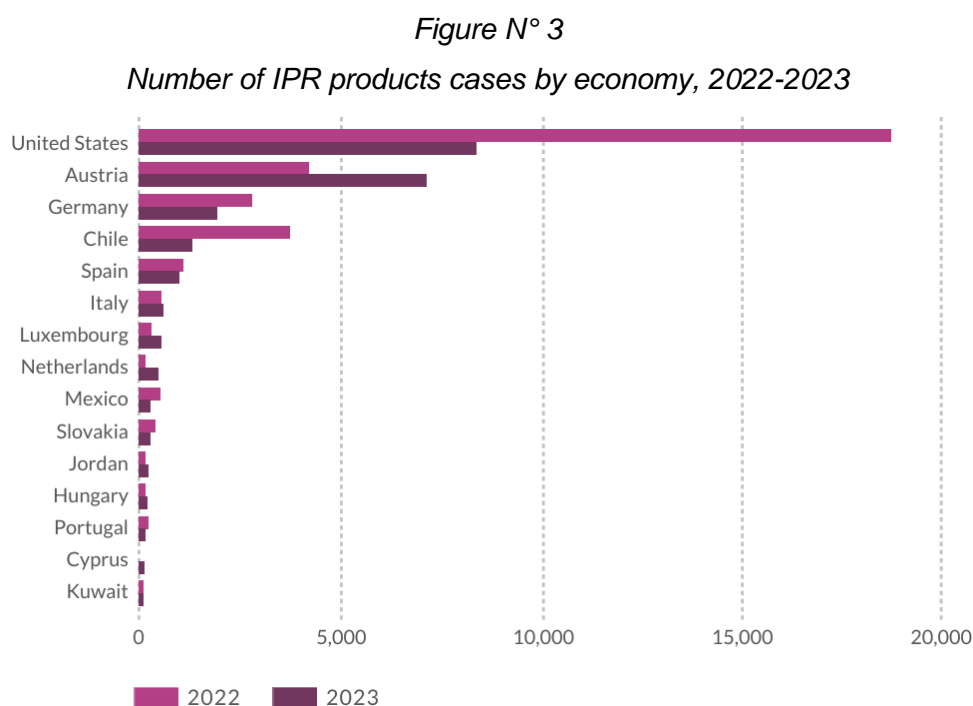
By the end of 2024, growth of 2.6% was again experienced and, thanks to the increase in demand, this figure is expected to grow to 3.3% by the end of 2025. Such fluctuation is best expressed in the following graph, which shows the volume of world trade on the vertical axis, and its progress over time by quarters on the horizontal axis.



Source: WTO (2024), Global Trade Outlook and Statistics. April 2024.

To deepen more in the evolution of this topic, the report “Enforcement and compliance: Illicit Trade Report 2023” prepared by the World Customs Organization (WCO) in 2022 and 2023, shows that the United States consistently reported the highest number of seizures of counterfeit goods, although these numbers decreased significantly from 18,509 in 2022 to 8,199 in 2023, a decrease of 55.7%. Austria followed as the second highest, with a significant increase in the number of cases, with a notable increase of 77.9% by 2023. Germany ranked third, but this economy saw a decrease of 30.2% (WCO, 2023, p. 172).

Chile ranks fourth with 1,195 cases, while Spain ranks fifth with a decrease of 7.6%. Italy experienced a growth of 8.8%, placing it in sixth place, while Luxembourg and the Netherlands showed remarkable increases of 76.2% and 185.3%, placing them in seventh and eighth positions, respectively. This evolution is made clear by the following graph (WCO, 2023, p. 172).

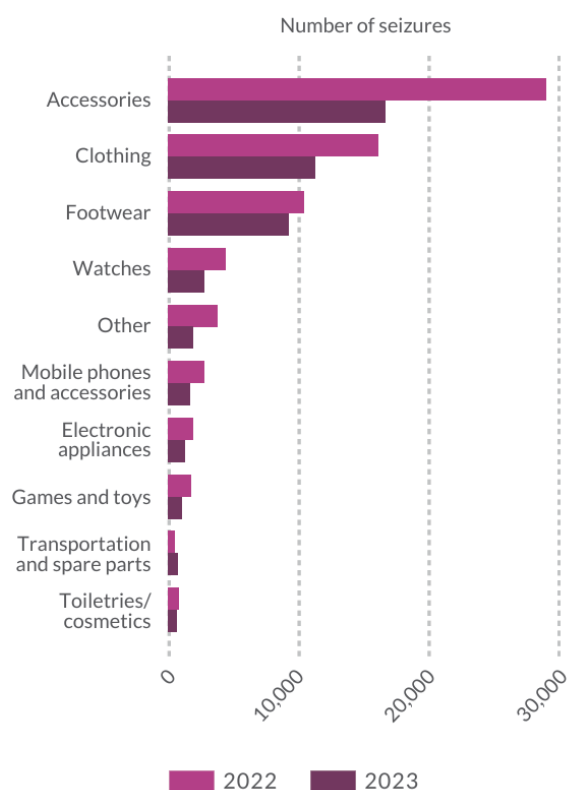


Source: WCO (2023), Enforcement and compliance: Illicit Trade Report 2023

In 2023, 62 economies reported a total of 48,061 seizures. While the number of seizures decreased by 36.6% compared to 2022, the majority of them were concentrated in accessories, clothing, and footwear, with accessories being the most frequently reported category (WCO, 2023, p. 173).

Accessories accounted for 16,761 seizures. Clothing came in second with 11,284 interceptions. Footwear was the third most seized category, with 9,275 seizures. These items were followed by watches with 2,767 seizures and items grouped under "other" with 1,902 interceptions (WCO, 2023, p. 173). This is better represented in the following figure.

Figure N° 4
Number of IPR seizures and number of pieces seized by category, 2022-2023



Source: WCO (2023), *Enforcement and compliance: Illicit Trade Report 2023*

Having considered the broader landscape of e-commerce globally and in some APEC economies, as well as the evolution of trademark counterfeiting within this context, we will now delve into key definitions that will inform and be helpful through the rest of this Guidebook.

4. Main definitions on enforcement in the digital environment

Before starting the substantive analysis, it is useful to define and clearly comprehend some concepts such as APEC region, digital environment, e-commerce, counterfeiting and enforcement measures. It should be clarified that although the definition of some of these terms is still part of the current academic debate, the definitions adopted here will be functionally useful for the purposes of this Guidebook.

A. APEC region

APEC is a regional economic forum established in 1989 to take advantage of the region's growing economic interconnections. APEC's 21 members are known as “economies” to reflect their commitment to work together for the promotion of inclusive,

balanced, and sustainable growth. APEC has its origins in earlier initiatives, namely the Pacific Economic Cooperation Council (PECC), a non-governmental body established to explore regional cooperation (Dutta, 1992, p. 5; APEC, 2020)¹.

B. Digital environment

This refers to a virtual space, accessible via the Internet, in which users interact with others and engage in a range of activities through a variety of devices, social media platforms or virtual reality technologies. This environment blurs the distinction between the physical and digital realms, with real implications for communication, actions, transactions and ethical considerations (Forrest and Wexler, 2003).

In the digital environment, an information system is a structured set of elements that collects, stores, processes and disseminates data to provide information, knowledge and digital products (Chatterjee, 2016). However, for practical purposes, when we talk about the digital environment, we are referring specifically to the space occupied by e-commerce platforms.

C. E-commerce

In general, such a concept includes all the set of commercial activities conducted through electronic transmission of data over the Internet (Grandón and Pearson, 2004). However, regarding the purposes of this Guidebook, e-commerce refers specifically to the acts of buying and selling of goods and services over electronic networks, connected through the Internet (Xiong et al., 2012).

From this point of view the e-commerce activities depend on the channels for interaction and not on the type of product, the parties involved, the payment method, or the delivery mechanism (OECD, 2019, p. 14).

This modality of commerce encompasses a wide range of business relationships linking consumers, businesses, and governments in a variety of formats, including Business-to-Business (B2B) transactions, Business-to-Government (B2G) interactions such as

¹ In 1989, APEC transformed this initiative into an official ministerial-level forum, and in 1991 APEC expanded its membership to include the People's Republic of China; Hong Kong, China; and Chinese Taipei, completing the PECC vision and establishing itself as the premier Asia-Pacific economic forum (Dutta, 1992, p. 5; APEC, 2020).

government procurement. Notwithstanding, those involving consumers directly are becoming increasingly relevant, particularly B2C exchanges and peer-to-peer transactions between individuals (OECD, 2019, p. 14).

D. Trademark counterfeiting

A trademark is any distinctive sign that is used to identify and differentiate products or services from others in the marketplace, helping consumers to make clear and informed choices. It must be unique enough to represent a specific type of product or service, while distinguishing it from competitors, avoiding confusion and ensuring transparency in consumer choice (Maraví, 2014, p. 59; Arana, 2017, p. 22).

Considering this previous definition, this Guidebook defines trademark counterfeiting as the unauthorized production, offering, selling or distribution, of any product or service, identified with a sign that is identical to a previously protected trademark or substantially indistinguishable from it². This concept encompasses a long-established way to understand the trademark counterfeiting, present in the Trademark Law of the People's Republic of China³ and regulations such as the United States Code⁴ about Commerce and Trade.

It is clear that counterfeited trademarks can be considered a social and economic danger, as they can cause confusion among the consumers. However, for the purposes of this Guidebook, the general deceiving effect associated with counterfeit trademarks will be restricted to situations in which they are intentionally designed to closely resemble originals.

² It should be noted that in some economies, well-known trademarks may not require prior registration in order for the trademark owner's rights to be protected. In Peru, for example, well-known trademarks are protected without registration. However, this may vary from economy to economy and each economy will need to take this into account when applying the concepts and recommendations of this Guidebook to its own situation.

³ Chapter VII of the Trademark Law of the People's Republic of China.

Protection of the Exclusive Right to the Use of a Registered Trademark

Article 56.- The exclusive right to the use of a registered trademark shall be limited to trademarks which are registered upon approval and to goods the use of a trademark on which is approved.

(...)

(4) counterfeiting, or making without authorization, representations of another person's registered trademark, or selling such representations;

⁴ Title 15 of the United States Code, about Commerce and Trade:

1116 - Injunctive relief

Trademark counterfeiting is the act of producing, offering for sale, selling, or distributing a product or service with a "spurious mark which is identical to, or substantially indistinguishable from, a registered mark." 15 USC. §§ 1116(d)(1)(B)(I), 1127

E. Enforcement measures

Given the global trend towards strengthening IP rights, thanks to milestones such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), part of the agreements of the World Trade Organization (WTO), a number of standards for enforcement have been widely adopted (Ostergard, 2000, p. 349).

For the purposes of this Guidebook, when we talk about enforcement measures, we are referring to all types of measures taken by an economy or by a private party (from IP owners to e-commerce platforms). This includes not only regulations or public policies but also cooperation mechanisms between institutions and the adoption of technologies for these purposes.

After clarifying key definitions, we now turn to the next section of this Guidebook. This section offers a detailed analysis of the current counterfeiting landscape and underscores the key barriers that must be addressed before issuing any recommendations.

ANALYSIS OF THE CURRENT TRADEMARK COUNTERFEITING LANDSCAPE AND KEY BARRIERS

1. Key trademark counterfeiting modalities in the digital environment

In view of the main objectives of the project, our analysis of the current situation of trademark counterfeiting will first focus on understanding the main modalities of trademark counterfeiting in the digital ecosystem, then we will address one of the most debated areas related to the use of trademarks in the online space and its consequences.

Next, we will examine some of the key barriers to effectively combat this form of infringement. Finally, we will explore the perspectives of representatives from various APEC economies, highlighting the specific challenges they face in addressing this issue.

The rise of online marketplaces has significantly transformed the global trade in counterfeit goods, making it easier for criminal networks to distribute illicit products ranging from traditional luxury goods to a wider range of everyday products such as pharmaceuticals, electronics, and household items (EUIPO, 2019, p. 10).

Although the European Union (EU) is not part of the APEC region, the European Union Intellectual Property Office (EUIPO) report titled “*Research on online business models infringing intellectual property rights: Phase 1*” provides valuable insights into trademark counterfeiting trends and practices that have global relevance. The study highlights methods and tactics commonly used by counterfeiters, many of which are applicable to e-commerce platforms and international trade flows worldwide, including within APEC economies. Given the interconnected nature of global trade and the shared challenges in combating counterfeiting, examining findings from the EUIPO report can shed light on broader patterns and inform strategies that are adaptable to the APEC context (EUIPO, 2016).

Advances in production technology have enabled counterfeiters to cheaply reproduce a wide range of products, posing health risks to consumers through dangerous ingredients found in counterfeit cosmetics, batteries, and hygiene products. This illicit production is often intertwined with wider criminal operations, such as fraud and tax evasion, which rely on sophisticated smuggling tactics, such as importing labels separate from the products, to evade detection across international borders (EUIPO, 2019, p. 12).

The scope of trademark infringement has broadened, extending beyond counterfeit physical goods to encompass a rapidly growing market for infringing digital content in the media sector. To track this development, 2016 EUIPO's report analyzed online business models identifying at least twenty-five models that infringe IP.

These models operate both on the internet and on the darknet, and some use the same platforms to facilitate other illegal activities, such as phishing and malware distribution. The majority of cases involved trademark infringement, often extending to the misuse of domain names and other forms of IP infringement (EUIPO, 2016, pp. 13-14).

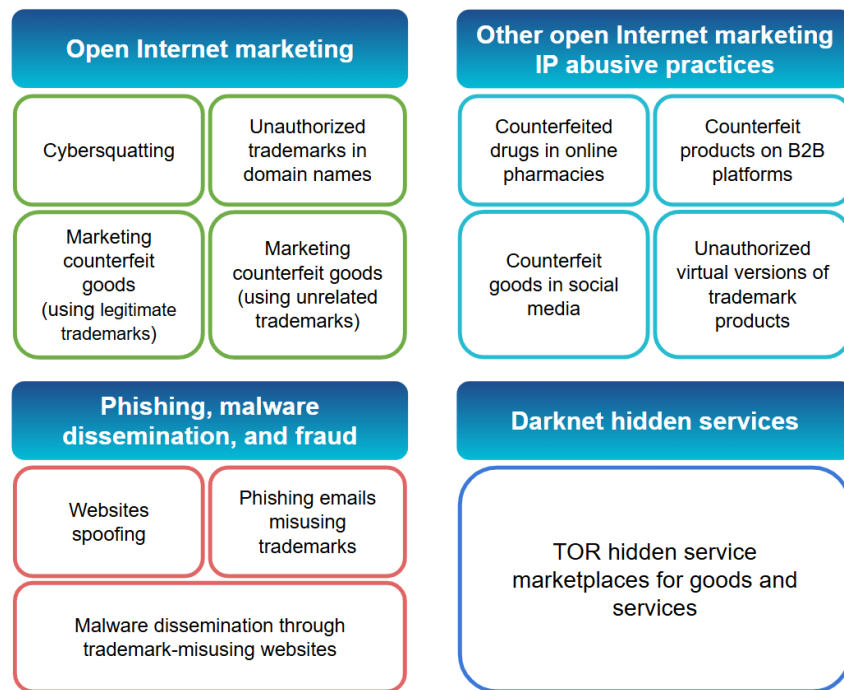
The aforementioned report shows that—in a sample of four economies which included Germany, Spain, Sweden and the United Kingdom— 27,870 e-shops were identified as likely sellers of infringing products. Of these, 75.4% (or 21,000 sites) operated under domain names that had previously redirected users to unrelated web content, suggesting a likely trend in other European markets with established e-commerce sectors. These findings highlight the potential of innovative enforcement policies, such as the “follow the money” approach, which aims to disrupt infringers' revenue streams through restrictions on advertising and payment processing, thus targeting the financial backbone of these illegal activities (EUIPO, 2019, p. 14).

Through this study, EUIPO developed a theoretical framework that allowed it to identify 25 different business models related to IP rights infringement. This classification provided a comprehensive overview of the various infringement models and a more detailed explanation of how they operate in digital markets (EUIPO, 2016, p. 25).

Among the categories identified in the EUIPO report, those relevant to a better understanding of the business models involved in "trademark counterfeiting in digital environments" are grouped into the following four groups:

Image N° 1

*Trademark counterfeiting business models based in digital environments, according to
EUIPO's report*



A. Open Internet marketing

Abuse of IP rights in domain names or digital identifiers, including (EUIPO, 2016):

- *Cybersquatting:*

It is described as the registration, trafficking, or use of a domain name with the goal of benefiting from the goodwill associated with a trademark owned by a third person. Cybersquatters generally register domain names that are identical or confusingly similar to recognized businesses' trademarks. Their major purpose is to sell these domain names to legitimate trademark owners at a high price.

This conduct not only exploits the trademark's prestige but also misleads consumers and may harm the reputation of the trademark owner. Locating and suing cybersquatters can be a time-consuming and expensive process. Furthermore, the worldwide nature of the internet makes the enforcement something challenging, as they can operate from places with permissive regulations.

- *Affiliate marketing using unauthorized trademarks in domain names*

This business model entails leveraging registered and/or well-known trademarks in domain names without permission to drive traffic to affiliate marketing websites. These websites create revenue by promoting third-party items or services and earning a percentage on sales made through their links. By including registered and/or well-known trademarks in their domain names, these sites might attract more users who wrongly feel they are accessing an official or approved site. Therefore, even if the product or service being sold is genuine, the use of a registered and/or well-known trademark to register a domain name is not an authorized use.

Such technique not only infringes trademark rights, but also deceives customers. The challenge for trademark owners is to monitor and enforce their rights across numerous affiliate marketing platforms and domain registrars, especially given the fast proliferation of such websites.

- *Selling counterfeit goods using legitimate trademarks in domain names*

In this model, counterfeiters create websites using domain names that include legitimate trademarks to sell counterfeit products. These websites often mimic the look and feel of official providers' sites to trick consumers into believing they are purchasing genuine goods.

This practice not only results in financial loss to the trademark owner, but also poses significant risks to consumers who may receive inferior or unsafe products. The main problem for trademark owners is to detect and shut down these sites quickly, as counterfeiters often change domain names and hosting providers to avoid detection. Coordination with Internet Services Providers (ISPs), domain registrars, and law enforcement is critical but can be resource intensive.

- *Marketing counterfeit goods using unrelated trademarks in domain names*

This type of operation involves the use of unrelated but well-known trademarks in domain names to attract traffic to websites selling counterfeit goods. For example, a counterfeiter may use a domain name containing a well-known trademark that is unrelated to the products being sold, simply to capitalize on the popularity of the well-known trademark and drive traffic.

Such deceptive practice confuses consumers and dilutes the value of the unrelated well-known trademark. The key for trademark owners is to monitor and enforce their rights against such misuse, which often involves complex litigation to prove intent to deceive and resulting consumer confusion. In addition, the widespread nature of the practice requires constant attention and significant resources to combat it effectively.

B. Other open Internet marketing IP abusive practices

- *Online pharmacies selling prescription drugs*

This business model involves the unauthorized sale of prescription drugs through online platforms, often resulting in the distribution of counterfeit drugs. These online pharmacies typically operate without proper licenses and sell medicines that may be substandard or even dangerous. They attract customers by offering lower prices and the convenience of online shopping.

However, the lack of regulation and oversight presents significant risks to the health and safety of consumers. Identifying and shutting down these illegal operations is challenging due to their ability to quickly change domain names and hosting services.

- *Sale of counterfeit products on B2B or B2C platforms*

This model involves selling counterfeit goods on legitimate B2B or B2C platforms, which include marketplaces. Counterfeiters use these platforms to reach a wide audience of potential buyers, often posing as legitimate suppliers. They use misleading listings and false certifications to convince buyers of the authenticity of their products.

Such practice not only undermines trust in B2B and B2C platforms but also causes significant financial loss to legitimate businesses. Monitoring and removing counterfeit listings is an ongoing challenge for platform operators, who must balance enforcement with maintaining a user-friendly experience. In addition, the sheer volume of transactions and listings makes it difficult to detect and prevent all instances of counterfeiting.

- *Selling counterfeit goods through social media*

In this business model, counterfeiters use social media networks to market and distribute counterfeit products. They harness the vast reach and influence of platforms (e.g., Facebook, Instagram or TikTok) to attract customers through targeted advertising and influencer partnerships. These counterfeit goods are often advertised as genuine, leading to consumer deception and potential harm.

The dynamic and fast-paced nature of social media makes it difficult for IP owners to monitor and remove infringing content in a timely manner. In addition, the anonymity afforded by social media accounts allows counterfeiters to easily reappear under different identities, complicating enforcement efforts.

- *Virtual product marketing in virtual worlds*

This model involves the sale of unauthorized virtual versions of trademarked products in digital environments such as virtual worlds and online games. These virtual goods often mimic real-world trademarked products and are sold to users for use within the virtual environment. This practice infringes the IP rights of trademark owners and can dilute the value of its companies.

In this rapidly evolving digital space, the challenge for IP owners is to monitor and enforce their rights. In addition, the decentralized and often anonymous nature of virtual worlds makes it difficult to identify and act against infringers. Collaboration with platform operators and the development of new enforcement strategies are essential to address this issue effectively.

C. Darknet hidden services

- *The Onion Router (TOR) hidden service marketplaces for goods and services*

These are anonymous platforms on the Dark Web using the TOR network to facilitate the sale of counterfeit goods and other illegal services. Such marketplaces operate clandestinely, making it difficult for law enforcement to track and shut them down. Sellers on these platforms often use cryptocurrencies to maintain anonymity and avoid detection.

The sale of counterfeit goods on these marketplaces not only infringes trademark rights but also presents significant risks to consumers, who may receive substandard or dangerous products. The anonymity provided by TOR networks creates a significant challenge to trademark owners and authorities, complicating efforts to identify and prosecute the individuals behind these illegal activities.

D. *Phishing, malware dissemination, and fraud*

- *Spoof websites misusing trademarks*

Spoof websites are fake websites that imitate legitimate trademarks in order to deceive consumers. These sites often replicate the design, logos and content of legitimate companies' sites to create a convincing facade. The primary goal is to trick consumers into believing they are interacting with the official trademark, leading to the purchase of counterfeit products or the theft of personal information.

This practice not only damages the companies' reputation, but also undermines consumer trust. Detecting and shutting down counterfeit sites is a constant battle for trademark owners, as these sites can quickly reappear under different domain names. Collaboration with ISPs and domain registrars is essential to effectively combat this problem.

- *Phishing emails misusing trademarks*

These emails are fraudulent messages that use familiar trademarks to steal personal information from recipients. These emails often appear to be from legitimate companies and use familiar trademarks to gain the recipient's trust. The emails typically contain links to fraudulent websites or attachments that prompt the recipient to enter sensitive information, such as passwords or credit card details.

This deceptive practice not only puts personal information at risk, but also tarnishes the reputation of the misused trademark. The challenge for trademark owners is to educate consumers about phishing tactics and to work with email service providers to filter and block such fraudulent messages.

- *Malware dissemination through trademark-misusing websites*

This business model involves the distribution of malicious software via websites that use established trademarks without authorization. These sites often appear legitimate and use familiar trademarks to entice visitors to download malware. Once installed, the malware can steal personal information, disrupt computer operations or provide unauthorized access to the user's system.

This practice not only infringes trademark rights, but also introduces significant cybersecurity threats. The challenge for trademark owners is to identify and shut down these malicious websites quickly. In addition, educating consumers about the risks of downloading software from unverified sources is critical to preventing malware infections.

E. SEO and SEM techniques as trademark counterfeiting tools

In addition to the digital-based trademark counterfeiting business models identified by EUIPO within its theoretical framework, we consider it relevant to mention the case of two additional techniques. Search Engine Optimization (SEO) and Search Engine Marketing (SEM) are common and legitimate digital marketing strategies used to improve search engine visibility (EUIPO, 2016, p. 38).

SEO focuses on improving a website's position in organic, or unpaid, search results through techniques such as keyword optimization, meta tags, and high-quality content creation. These strategies rely on various signals, including titles, domain names, and backlinks, to boost a site's search ranking. Conversely, SEM involves paid advertising campaigns where search engines like Google, Yahoo!, or Bing display ads based on users' search terms. Through tools like Google Ads, advertisers bid on keywords to display their content as sponsored results (EUIPO, 2016, p. 39).

However, SEO and SEM techniques can be also exploited in trademark counterfeiting practices to increase visibility. Websites using counterfeit trademarks misuse SEO techniques by optimizing keywords, links and even using trademarks as terms in unauthorized ways to obtain high rankings in organic search results, tricking consumers into believing they are authentic sources. For example, selling products in similar categories but unrelated to the trademark. Similarly, the use of SEM techniques allows counterfeiters to run paid ads that deceptively use trademarked terms, promoting products with counterfeit trademarks directly to consumers. These practices not only

broaden the exposure of counterfeit products but also undermine brand owners' efforts to protect the integrity of their brand.

This taxonomy provides a more nuanced understanding of the implications of the type of trademark counterfeiting under study. It is imperative to acknowledge that this Guidebook will present a series of recommendations that will be applicable to address the modalities of trademark counterfeiting involving intermediaries, such as digital platforms, including marketplaces, social networks, and online shops.

This means that business models based on trademark counterfeiting, such as online pharmacies selling prescription drugs, the sale of counterfeit goods on B2B or B2C platforms, the marketing of counterfeit goods through social networks, and the virtual product marketing in virtual worlds, can be mitigated through the implementation of multiple recommendations, which will be outlined in later sections.

Likewise, we can anticipate that those business models based on trademark counterfeiting that abuse mainly the use of domain names, including cases of cybersquatting, selling counterfeit products using legitimate trademarks in domain names, marketing counterfeit products with unrelated trademarks in domain names, and affiliate marketing practices involving the unauthorized use of trademarks in domain names, may also be confronted thanks to the knowledge of this Guidebook.

Notwithstanding the aforementioned, we believe it is crucial to highlight the selection of online counterfeiting modalities presented here, as it serves as a vital first step in understanding the complexity of the issue, increasing public awareness, and formulating effective solutions that can be implemented with optimal results.

Several IP rights infringing online business models mimic legitimate structures, such as B2B and B2C websites, listings on third-party marketplaces, streaming services, and affiliate marketing. These infringing models typically generate revenue through similar means as legitimate businesses, including direct sales or indirect sources such as pay-per-click fees and advertising revenue. What distinguishes these infringing models is their deceptive nature, which misleads consumers by presenting counterfeit products as authentic. This deception may be accompanied by fraudulent practices such as phishing or malware distribution, further exacerbating the risks to consumers (EUIPO, 2016, p. 45).

Certain online business models are deliberately designed to exploit IP rights infringements, generating revenue from activities such as phishing emails, ransomware distribution and various fraudulent schemes. In addition, the registration and use of domain names with third party trademarks is common and serves multiple purposes, such as generating pay-per-click revenue or redirecting traffic to the registrant's own sites. When IP rights infringements occur on websites directly controlled by the infringers, right holders can, in theory, take enforcement action, whether through litigation, criminal prosecution, or non-judicial methods. However, these efforts are often hampered by infringers' use of privacy services or false contact information to hide their identity, making enforcement difficult or impossible and highlighting their difference from legitimate operators (EUIPO, 2019, p. 45).

A growing number of IP rights infringers are moving their operations to the darknet or maintaining a presence in both the visible and hidden parts of the Internet. This trend complicates law enforcement because these providers take advantage of greater anonymity, making them harder to identify. In addition, the line between IP rights infringements and traditional cybercrime is becoming increasingly blurred. Activities such as website spoofing and phishing emails not only infringe IP rights but also trick recipients into revealing sensitive information such as bank account details or passwords —methods that were previously mainly associated with illegal hacking (EUIPO, 2016, p. 46).

Some online business models are specifically structured to profit from IP rights infringements, such as cybersquatting, the sale of counterfeit goods and phishing emails. These methods often take advantage of the ease and low cost of registering domain names similar to existing trademarks, which reinforces their deceptive nature (EUIPO, 2019, p. 28). Of the 25 business models examined, 12 potentially infringe multiple IP rights. Examples include the sale of counterfeit goods on self-managed websites, third-party marketplaces, or through social media platforms (EUIPO, 2019, p. 30).

The main methods of generating indirect revenue in the digital space include "pay per impression", where revenue depends on page views, "pay per click", which is based on the number of clicks, and "pay per action" (PPA), where revenue is generated from user actions on the advertiser's landing page. Variations of PPA include "pay per download" and "pay per install", which are triggered when a user downloads a file or installs software (EUIPO, 2016, p. 33).

While these revenue models are used by legitimate businesses, IP rights infringing activities often generate illicit or fraudulent profits. Phishing scams are a prominent example, in which individuals and businesses are tricked into paying for non-existent services, revealing banking details, disclosing trade secrets, or updating accounts, resulting in the installation of malware (EUIPO, 2016, p. 35).

As can be seen, several of these business models involve the participation, usually involuntarily, of actors that operate as intermediary platforms. This occurs, for example, in the sale of counterfeit goods through B2B or B2C platforms, through social networks, virtual worlds or even using companies that sell domain names for cybersquatting operations or similar modalities.

A concise examination of the role and liability of intermediaries in trademark counterfeiting is essential. As the digital economy has evolved, intermediaries have evolved from passive facilitators to active participants in shaping the online ecosystem. In the attention-driven economy, their services and content are tailored to support advertising-based business models and foster trust in digital transactions (Buiten, 2021, p. 361).

As a result, determining an intermediary's liability for infringement is often more complicated than it may appear at first glance. First of all, it should be noted that intermediaries provide a service typically characterized by the storage of information from different users (e.g. social networks), sometimes simply referred to as intermediary services. This allows them to be a central point where parties with compatible interests can come together, such as those users who want to sell something with those users who want to buy (e.g. marketplace) (OECD, 2019, 16).

To this end, intermediary service providers usually offer tools that facilitate the storage and display of information (e.g. offers of goods or services), communication between users or even mechanisms that enable commercial transactions, such as payment gateways. In this sense, intermediary platforms hold a pivotal position in the digital economy, which underscores their important role in promoting responsible practices and addressing activities occurring within their ecosystems. For example, an intermediary platform that facilitates trade in counterfeit goods would undoubtedly be directly responsible for facilitating this type of IP rights infringement (Buiten, 2021, p. 362).

However, there are also cases where intermediary platforms designed to facilitate legitimate transactions find that some users are using these tools to trade in products or services with counterfeit trademarks or other forms of IP rights infringement. In these scenarios, there is still a lot of room for discussion, thanks to which different economies have come up with solutions (Frosio, 2017, p. 22).

The main discussions on the attribution and exemption of liability of these actors therefore revolve around the intermediary role, in other words, whether their service is purely technical, automatic and passive, with no knowledge or control over the information stored, or whether, on the contrary, they have sufficient knowledge and capacity to prevent trademark infringements.

Notwithstanding the fact that this is still an open discussion, the first part of the recommendations section of this document will look at this aspect in more detail, in order to suggest ways of addressing this issue in a useful and constructive manner.

Having explored some of the trademark counterfeiting modalities in the digital ecosystem, and the additional complexity when an intermediary is involved, the subsequent section will focus on the examination of some of the main obstacles that may pose challenges to efforts aimed at combating digital counterfeiting of trademarks in the online environment.

2. Main barriers and challenges to combat the digital counterfeiting of trademarks in e-commerce platforms

E-commerce originated as a means of streamlining recurring transactions between large companies and relies heavily on specialized networks for electronic data exchange. However, with the advent of open networks such as the Internet, e-commerce has become more accessible to smaller businesses and is increasingly focused on B2C transactions. Although B2B exchanges still dominate in terms of volume, the highest growth rates are in consumer-facing sectors such as accommodation and retail. This shift is supported by widespread access to the internet via mobile devices and the emergence of innovative payment methods, which are driving an unprecedented expansion of e-commerce across a range of sectors (OECD, 2019, p. 32).

Despite this rapid growth, legal frameworks are struggling to keep pace with the evolving digital landscape. Courts and legislatures around the world face challenges in addressing the

actions of bad actors in online spaces, where traditional enforcement measures often fall short. In the digital environment, the following obstacles exacerbate these enforcement difficulties (Mostert and Lambert, 2019, p. 2):

A. Anonymity of counterfeiters

The digital environment provides counterfeiters with tools to remain anonymous, making them difficult to trace and identify. Many operate through pseudonyms, disposable email accounts, and temporary servers, evading detection by enforcement authorities.

B. The whack-a-mole effect

A pervasive issue in e-commerce enforcement is the "whack-a-mole" phenomenon, where infringing listings reappear shortly after removal under new Uniform Resource Locators (URLs) or accounts. This cyclical nature of counterfeiting creates a constant and resource-intensive battle for enforcement agencies and right holders.

C. Ephemeral nature of counterfeit listings

Counterfeit goods are often marketed through listings that exist only briefly —sometimes just for hours or days— further complicating efforts to track and act against infringers in real time.

D. Jurisdictional and cross-border enforcement issues

The global nature of e-commerce means counterfeiters frequently operate across multiple jurisdictions, using websites hosted in different economies. This makes it challenging to enforce judgments or coordinate cross-border legal actions effectively.

E. Lack of a unified global framework

Enforcement efforts are hindered by the absence of a centralized, globally recognized framework for information sharing among enforcement authorities. This gap in international cooperation limits the ability to track offenders and coordinate actions against them.

At the heart of these challenges is the issue of anonymity, which protects malicious actors from detection and accountability. Without mechanisms to systematically track and trace these offenders from the digital realm back to a physical source, law enforcement efforts remain largely ineffective. Significant progress can only be made by bridging the gap between digital activity and identifiable real-world actors (Mostert and Lambert, 2019, p. 3).

The anonymity challenge in the online environment is a divisive topic, far from being solved, due to its inherent complexity. For enforcement agencies to act effectively, they often require access to detailed information about sellers suspected of engaging in counterfeit activities. However, this need for transparency can clash with privacy principles and data protection laws, particularly when third parties, such as online marketplaces, are asked to share sensitive information about suspected infringers.

One of the recent regulations that decided to face this challenge should be mentioned in this context. The Integrity, Notification, and Fairness in Online Retail Marketplaces for Consumers Act (INFORM Consumers Act), went into effect in the US since June of 2023, aims to increase transparency in online transactions by requiring platforms to verify the identities of high volume sellers and collect sensitive data, such as tax identification numbers and bank account details.

While the INFORM Consumers Act seeks to reduce counterfeit activities by holding sellers accountable, it also raises concerns about the potential misuse of the data collected. The INFORM Consumers Act mandates that online marketplaces implement "reasonable security procedures and practices" to protect this information, but the lack of specific definitions for these standards has left room for varied interpretations, potentially leading to legal disputes.

While regulations like the INFORM Consumers Act represent one path in addressing the anonymity of counterfeiters, it is still too early to fully assess their effectiveness, and to clearly determine if they will represent a desired step toward greater beneficial transparency.

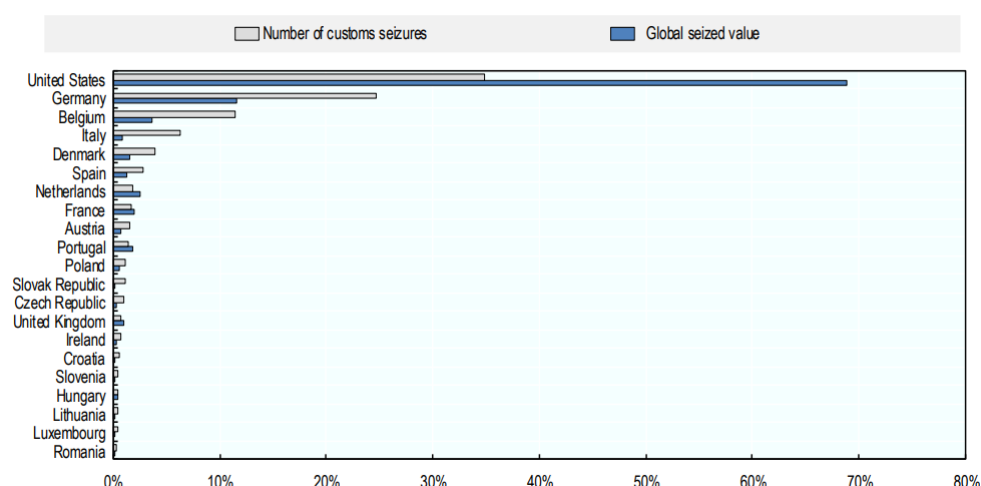
However, notwithstanding the importance of consumers' privacy and even anonymity in some cases, it is also true that the impact of counterfeiting goes beyond the damage it does to the profits of the companies concerned and to the economy as a whole. Counterfeited goods can also pose significant risks to public welfare and safety. This issue is even more critical in sectors that are considered high risk, such as illegal pharmaceuticals, food or alcohol. In these sectors, the availability of counterfeit products represents a serious threat to the health and

safety of consumers, which can have serious consequences for public welfare (OECD/EUIPO, 2023, p. 10).

Looking at the data on global customs seizures of counterfeit products sent in small parcels, importers of counterfeit small packages can be found in various economies, where affordable small parcels services and e-commerce are widely available. Additionally, the data may include seized goods not only destined for the specific market where the seizure took place but also transshipped further. Overall, these counterfeit imports were mainly directed to economies which, in absolute terms, are significant participants in world trade (OECD/EUIPO, 2023, p. 11, 15 and 21).

Figure N° 5

Top destination economies of counterfeit goods shipped in small parcels (In terms of number and value of customs seizures, 2017-2019)



Source: OECD/EUIPO (2023), Why Do Countries Import Fakes?

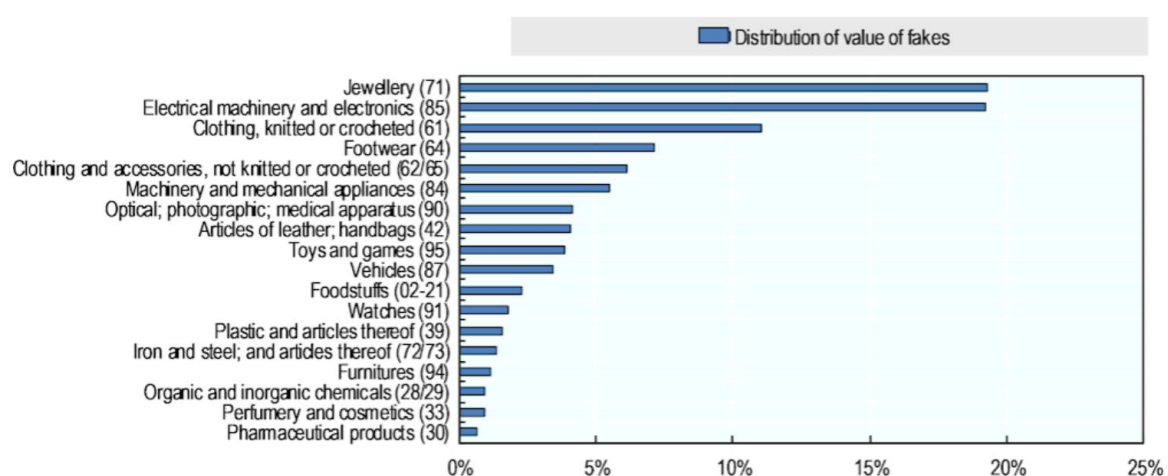
The analysis of the distribution of counterfeit imports by product category underscores the vast diversity in the types of fake goods circulating through global trade. This assortment includes everyday items such as footwear and ready-to-wear clothing, alongside luxury goods designed to mimic high-end trademarks. More concerning is the infiltration of counterfeit products that pose serious risks to consumers' safety, including toys and games, spare parts for machinery and vehicles, cosmetics, and pharmaceuticals (OECD/EUIPO, 2023, p. 23).

Among these, jewelry and electronics emerged as the product categories with the highest

value of counterfeit imports in 2019. Clothing and footwear are closely followed as major contributors to the overall value of fake goods in international trade. The breadth of these counterfeit categories highlights the complexity of enforcement efforts needed to address not only economic damage but also potential dangers to public health and safety (OECD/EUIPO, 2023, p. 23).

Figure N° 6

Distribution of the value of fake imports, by product categories, 2019



Source: OECD/EUIPO (2023), Why Do Countries Import Fakes?

One of the main obstacles to adapting trademark law to the digital ecosystem is the complexity of jurisdictional boundaries. The inherently cross-border nature of the Internet makes it difficult to determine where trademark infringement is occurring and to take appropriate legal action. This challenge is further complicated by the degree of anonymity often associated with online platforms, which can make it more difficult to identify and address those responsible for infringing trademark rights. The rapid proliferation of infringing content across multiple jurisdictions adds another layer of difficulty, making trademark enforcement a daunting task (Thio, Christiawan and Wagiman, p. 713).

Counterfeiters have the ability to replicate trademarked goods with relative ease and market them through digital platforms, significantly undermining the value and credibility of established trademarks. This threat is multi-faceted, not only undermining consumer confidence, but also leading to economic losses and potential risks to shoppers' safety. The

challenge for IP owners is immense; the high volume and rapid pace of online transactions makes monitoring and detecting infringement a continuous and resource-intensive effort (Thio, Christiawan and Wagiman, p. 714).

The presence of counterfeit products on the Internet also dilutes trademark identity, making it difficult for legitimate products to stand out and maintain market share. In addition, counterfeit products often evade regulatory controls, putting consumers at risk of purchasing items that do not meet safety or quality standards, further exacerbating the negative impact for both companies and the public (Thio, Christiawan and Wagiman, p. 714).

The jurisdictional complexity of online trademark protection creates significant obstacles to enforcement. The borderless nature of the Internet allows infringing activities to occur simultaneously in many jurisdictions, making it difficult to identify the appropriate legal framework for effective action. This problem is compounded by differences in legal standards and enforcement practices between economies, which may lead infringers to seek the most advantageous forum in jurisdictions with weak regulation or inadequate enforcement (Thio, Christiawan and Wagiman, p. 715).

Domestically, trademark owners face their own challenges in securing their online presence and protecting their IP. A lack of resources and expertise often hampers their ability to establish and maintain effective trademark protection strategies. This lack can leave them vulnerable to continued infringement and exploitation, making it difficult to respond quickly and comprehensively to emerging threats in the digital landscape (Thio, Christiawan and Wagiman, p. 715).

To conclude the section on challenges, it is appropriate to address insights from surveys conducted to APEC policymakers during the preparation of this Guidebook. Such answers shed light on key challenges in enforcing IP rights, particularly in the context of cross-border trademark infringement. Several APEC economies identified cross-border implementation as a significant obstacle, emphasizing the inherent difficulties of addressing online violations originating outside their jurisdiction.

3. *Highlights from surveys results*

Some notable results can be drawn from the aforementioned surveys, with cross-border enforcement emerging as a main challenge for several economies. This issue, highlighted by

Australia; Hong Kong, China; the Republic of Korea; and Peru, reflects the complexity of enforcing IP rights across borders.

Each of these economies noted that online trademark infringements often involve enforcement across various jurisdictions, making enforcement efforts and coordination with international bodies more difficult. This difficulty underscores the need for multinational cooperation and policy coordination to address the cross-border nature of online trademark infringement.

In addition to jurisdictional challenges, technological limitations are another major obstacle affecting a number of economies. The economies of Chile; Mexico; Papua New Guinea; Peru, the Republic of the Philippines; and the United States report limitations in technological capabilities that may hinder effective monitoring and enforcement against counterfeiting activities.

These limitations range from inadequate monitoring tools to disparate technological infrastructures between law enforcement agencies, creating loopholes that counterfeiters exploit. This disparity highlights the urgent need to invest in advanced surveillance tools and common technology solutions that can adapt to the evolving tactics of online criminals.

A third major challenge is the lack of effective information-sharing mechanisms, which affects almost all economies surveyed, including Australia; Chile; the Republic of Korea; Mexico; Peru; the Republic of the Philippines; Chinese Taipei; and the United States. The lack of robust data-sharing frameworks among these economies limits timely and comprehensive enforcement actions, as critical information about infringers often remains in silos.

In the context of regulatory frameworks, this lack of transparency not only limits real-time responses to IP rights violations but also constrains long-term policy development. Improving cross-industry information-sharing platforms could strengthen responses to counterfeiting across jurisdictions and support coordinated efforts globally.

Gaps in legal frameworks and policies, which are closely linked to inconsistencies in enforcement, were another common concern raised in the survey by economies such as Mexico; Papua New Guinea; Peru; the Republic of the Philippines; Chinese Taipei; and the United States.

These economies report a lack of uniform IP laws, which create enforcement challenges,

especially when infringers take advantage of regulatory differences. For example, counterfeiters may exploit jurisdictions with lenient penalties or vague trademark protection standards to host e-commerce websites or operate digital marketplaces that distribute counterfeit goods. Similarly, differences regarding rules for intermediary liability across economies can enable infringers to use platforms in one jurisdiction to sell counterfeit products to consumers in another, bypassing stricter regulations. Harmonizing IP laws on digital enforcement and establishing consistent enforcement priorities would reduce these inconsistencies and make it more difficult for counterfeiters to exploit legal loopholes.

Finally, some economies face knowledge and awareness issues that undermine IP enforcement efforts. Mexico and Papua New Guinea reported a shortage of IP professionals and limited IP training for government officials, which may limit their ability to effectively combat online trademark counterfeiting.

This lack of expertise not only limits direct law enforcement, but also reduces the potential for proactive awareness campaigns. To fill these gaps, law enforcement agencies should acquire IP knowledge and expertise, which could foster a more resilient response to the adaptation tactics used in trademark counterfeiting through digital platforms.

Critical barriers to combat digital trademark counterfeiting, such as jurisdictional complexity, the cross-border nature of e-commerce, and the anonymity of offenders, complicate enforcement efforts. In addition, the lack of a single global framework for international cooperation exacerbates these challenges, making it difficult for enforcement authorities to track and act against cross-border infringements.

In the same vein, the perspectives shared by APEC economies highlight the need for enhanced multinational cooperation and policy coordination to address the cross-border nature of IP rights infringements. A unified approach, supported by technological innovation and stronger legal frameworks, is essential to combat the growing problem of online counterfeiting and to ensure the integrity of e-commerce platforms across the region.

As a result, the following section will present voluntary recommendations that APEC member economies could adopt, taking into account the roles of both public actors (e.g., policymakers and law enforcement agencies) and private actors (e.g., e-commerce platforms and IP right holders). Similarly, the case studies offered below will highlight some of the best practices and major accomplishments in resolving some of the challenges identified thus far.

RECOMMENDATIONS

1. *Assessing the liability of online intermediaries*

The first recommendation proposes the creation of a typology of online intermediary platforms, in the form of a database, to classify these stakeholders and outline their levels of responsibility recognized by APEC or non-APEC economies. While IPEG's agenda already includes discussions on trademark counterfeiting, enforcement, and emerging technologies, this initiative would enhance its scope by providing economies with a practical tool to shape effective strategies for addressing platform liability. The database would promote regional consistency, alignment with global best practices, and support the development of tailored approaches by considering distinct regulatory environments, market conditions, and the complexities of the digital ecosystem in each economy.

To illustrate which aspects of the current liability standards for online intermediary platforms could be examined, we will reference three regulations that have either been enacted or are still under discussion: the European Digital Services Act (DSA), the Amended Provider Liability Limitation Act under consideration in Japan, and the Stopping Harmful Offers on Platforms by Screening Against Fakes in E-Commerce Act (SHOP SAFE Act) currently being advanced in the United States.

A. The DSA

The first example to consider is the Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022, commonly known as the DSA. This framework introduces, among several other changes, three aspects relevant to the topic of this recommendation: 1) wider diversity in the classification of intermediaries; 2) differentiated levels of responsibility for various types of intermediaries; and 3) tailored enforcement mechanisms for intermediaries in different categories. For the European case, these regulatory elements aim to enhance the detection and removal of harmful online content, including those infringing on IP owners' rights.

It is important to note, however, that the DSA is a relatively new regulatory framework, with its full implementation beginning in February 2024 and specific obligations for very large online platforms (VLOPs) and search engines taking effect in August 2023. As of December 2024, it is still too early to comprehensively assess its effectiveness through statistical data. While the groundwork for a safer and more transparent online environment

has been established, detailed evaluations and concrete statistical evidence are expected in upcoming reports and data analysis from the European Commission and relevant authorities.

A key aspect highlighted in the DSA is the approach of embracing diversity in the classification of intermediaries. The DSA introduces distinctions among intermediary services, designed to address illegal online content more effectively. The broadest category includes online search engines, followed by hosting services. A narrower category is online platforms, with a specific subcategory for VLOPs and very large online search engines (VLOSEs). This legal taxonomy acknowledges the distinct role each type of intermediary plays in shaping digital ecosystems (Buiten, 2021, p. 363).

Following the classification of intermediaries proposed by the DSA framework is the shift towards differentiated levels of responsibility for different types of intermediaries. This normative change aims to align tiered liability exemption scenarios with the type of role played by different categories of intermediaries. For example, all digital platforms dedicated to or used for e-commerce, including marketplaces, social networks, or online stores, are considered by the DSA to be hosting services that may be relieved of liability to the extent that they are unaware of illegal content (e.g., counterfeit goods) or that, upon becoming aware of such content, they act promptly to remove it⁵. In this way, depending on the level of influence of each intermediary, the DSA outlines some obligations to address illegal online content, which can include implementing notice-and-action procedures⁶ and establishing internal complaints systems that allow users to contest content moderation decisions (Buiten, 2021, p. 372; Frosio, 2017, p. 22).

According to this framework, the assumption that online platforms merely provide neutral, technical services is challenged. It suggests that their operations are significantly more complex, particularly when it comes to defining the permissible scope of moderation and

⁵ Article 6.- Hosting:

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider:

- (a) does not have actual knowledge of illegal activity or illegal content and as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or
- (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

⁶ Article 16.- Notice and action mechanisms

1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access and user-friendly and shall allow for the submission of notices exclusively by electronic means.

identifying the point at which such actions might be deemed "active" in terms of liability (Buiten, 2021, p. 372).

For example, in the specific subcategory of VLOPs, the DSA outlines even stricter requirements. These include robust risk management protocols, transparent data access provisions, adherence to compliance measures, and periodic independent audits. By tailoring responsibilities to align with the scale and societal impact of VLOPs, this framework aims to balance the need for regulatory oversight with the operational realities of platforms, promoting accountability while minimizing excessive burdens on smaller entities (Buiten, 2021, p. 369)

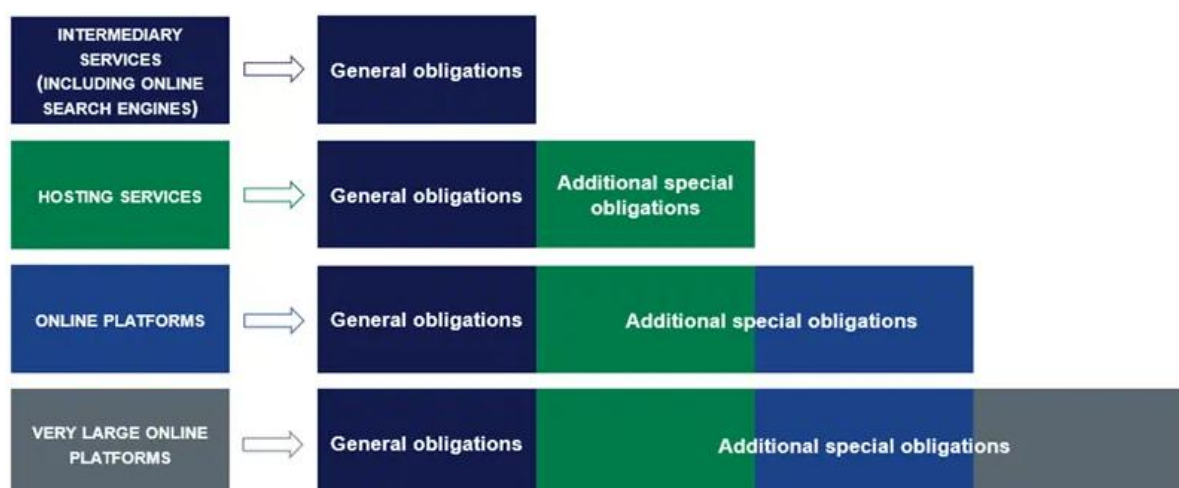
The introduction of differentiated enforcement mechanisms for intermediaries is another shift present in the DSA. General due diligence obligations apply across all intermediary services, requiring measures such as establishing a single point of contact, integrating specific provisions into terms and conditions, and fulfilling transparency reporting requirements. Hosting services, in particular, must implement accessible and user-friendly notice-and-action procedures that enable third parties to report illegal content. For online platforms, the DSA tightens complaint management standards and imposes stricter reporting duties to supervisory authorities, enhancing accountability and compliance across the digital ecosystem (Buiten, 2021, p. 368).

Specific provisions emphasize the need for a uniform, transparent, and clear notice-and-action procedure. This approach ensures timely, thorough, and impartial responses to illegal content while safeguarding the rights and legitimate interests of all parties, particularly their fundamental rights (Buiten, 2021, p. 374). Complementing this, the DSA mandates that providers expeditiously remove flagged content upon awareness of its illegality⁷. However, this heightened vigilance may inadvertently lead to excessive content moderation, potentially stifling freedom of expression as platforms err on the side of caution to avoid liability (Turillazzi et al., 2023, p. 95).

Image N°2

Classification of intermediary services and liability levels according to the DSA

⁷ See the reference in footnote 5, regarding literal (b) numeral 1), of Article 6 of the DSA.



Source: “Digital Services Act – an overview”, (2022) Taylor Wessing.

B. Information Distribution Platform Act (Partial Amendment of the Provider Liability Limitation Act)

Information Distribution Platform Act (Partial Amendment of the Provider Liability Limitation Act) in Japan establishes a framework for addressing the liability of online intermediary platforms. This legislation aims to balance the protection of individual rights with the operational realities of online service providers.

Under the Act, online intermediary platforms are required to disclose the identifying information of users who post content that infringes the rights of others. This includes the name and address of the sender, which can be requested by victims of defamatory or harmful postings. The law introduces a streamlined court procedure to facilitate the disclosure of such information, ensuring that victims can more easily seek redress (Ishikawa and Takiguchi, 2024).

The law does not explicitly introduce greater diversity in the classification of intermediaries. Instead, it applies uniformly to all specified telecommunications service providers.

However, in terms of differentiated levels of responsibility, the Act imposes stricter requirements and more extensive disclosure obligations on platforms that operate login-based services, such as social media networks. These platforms must disclose not only IP addresses associated with specific posts, but also login event information, which can

help identify users even when direct post-related data is not available. This nuanced approach reflects an understanding of the different capabilities and data retention practices of different types of intermediaries (Ishikawa and Takiguchi, 2024).

The Act's enforcement mechanisms are also tailored to address the unique challenges posed by different categories of intermediaries. For example, large platform operators, defined by the size of their user base, are subject to stricter requirements for responding to removal requests and ensuring transparency in their operations. These operators must establish clear procedures for handling takedown requests, conduct timely investigations, and provide detailed notifications to both takedown requesters and senders. This approach ensures that larger platforms, which have greater resources and a more significant impact on the online environment, are held to higher standards of accountability (Kobayashi, 2022).

This regulation shows that it is part of a regulatory trend that implements a new differentiation of liability and enforcement mechanisms based on the specific roles and capacities of intermediaries. This ensures a balanced and effective regulatory framework that takes into account the complexities of the online environment.

C. The SHOP SAFE Act

The SHOP SAFE Act, introduced in 2023 since its last amendment, is a legislative initiative pending approval in the United States' Congress aimed at addressing the growing problem of counterfeit goods on online marketplaces. The SHOP SAFE Act focuses on increasing the accountability of online intermediary platforms, particularly those involved in the sale of counterfeit products that could pose significant health and safety risks to consumers. Its core objective is to establish stricter liability standards for these platforms, requiring them to take proactive measures to prevent the sale of counterfeit goods⁸.

Under the SHOP SAFE Act, online platforms are required to implement preventative measures to avoid liability for counterfeit products. These measures include enhanced screening processes to detect counterfeit listings, verification protocols for third-party sellers, and procedures to quickly remove counterfeit products from the marketplace. By

⁸ SHOP SAFE Act of 2023, S. 2934, 118th Cong. (2023). <https://www.congress.gov/bill/118th-congress/senate-bill/2934/text>

enforcing these measures, the SHOP SAFE Act aims to ensure that platforms take responsibility for monitoring and controlling the sale of potentially harmful counterfeit products, thereby protecting consumer welfare.

The proposed regulation also includes specific requirements for online platforms to enhance the verification and monitoring of sellers. Platforms are required to verify the identity and contact information of sellers, including ensuring that they have a registered agent or verified address for service of process in the United States. In addition, sellers must agree not to use counterfeit trademarks on the goods they sell, reinforcing the platform's responsibility to ensure that only legitimate products are offered to consumers. To further combat trademark counterfeiting, platforms are required to implement technical measures to pre-screen listings, using technology to detect and remove products bearing counterfeit trademarks before they are made available to the public.

In addition to these preventative measures, the SHOP SAFE Act emphasizes the importance of responding quickly to counterfeit listings. Platforms must act quickly to remove such listings and take appropriate action against repeat offenders, including banning them from the platform. The SHOP SAFE Act also introduces a "safe harbor" provision, which protects platforms from liability for contributory trademark infringement as long as they can demonstrate compliance with preventive measures. This means that if a platform can demonstrate that it has properly screened sellers, removed counterfeit listings, and banned habitual offenders, it will not be held liable for the actions of third-party sellers. This legal framework encourages platforms to take a more proactive role in policing their marketplaces.

After analyzing strategies adopted by economies such as Japan and the United States, as well as regions like the EU, the value of this recommendation becomes clearer the proposed initiative for IPEG to create a typology expressed in the form of a reference database would provide a practical tool for categorizing online intermediary platforms and their levels of responsibility recognized by APEC and non-APEC economies. This recommendation is not intended to identify the names of individual or corporate identities of intermediaries, but to create general categories that can be useful and applied by APEC economies to their different realities.

This resource would serve as a foundation for shaping effective strategies to address platform liability, particularly in combating trademark counterfeiting. It would also promote regional consistency and alignment with global best practices. Complementing this effort, IPEG could

expand its discussions to include input from non-APEC economies or organizations, facilitating a broader exchange of innovative practices and perspectives.

To ensure the success of this initiative, it is essential to take into account the distinct regulatory environments, market conditions, and complexities of the digital ecosystem in each economy. Such an approach would ensure that the reference database remains relevant, adaptable, and valuable across the diverse contexts of APEC economies.

To advance the understanding and alignment of the liability framework for online intermediary platforms, IPEG, aided by APEC economies, could develop a reference database that maps the various categories of intermediaries and their levels of responsibility as recognized by APEC and non-APEC economies. This initiative would prioritize the exchange of regulatory trends, best practices, and innovative strategies, offering economies a comprehensive resource to shape effective responses to platform liability challenges.

The reference database would serve as a dynamic tool, fostering collaboration and knowledge sharing among APEC economies. It could be enriched with insights from expert presentations, case studies, and contributions from private stakeholders and non-APEC organizations, ensuring that members remain informed of global developments.

This information would enable economies to make informed decisions on adapting their regulatory frameworks, tailored to their domestic priorities while addressing shared challenges. By supporting regional consistency and alignment with global standards, this initiative would help mitigate jurisdictional gaps and strengthen enforcement efforts in the digital ecosystem.

Through this collaborative approach, IPEG would promote sustained attention to platform liability issues, encouraging economies to leverage shared tools while respecting the diversity of regulatory environments across the region.

2. *Guidelines and voluntary documents for digital platforms*

The second recommendation emphasizes the importance of adopting guidelines for digital platforms to enhance the ability of APEC economies to combat trademark counterfeiting in online environments.

A. Importance and application of guidelines to combat trademark counterfeiting in the digital environment

For any government involved in policy making, it is crucial to assess the effectiveness of measures in achieving their stated objectives, the associated costs and trade-offs, and the potential for alternative approaches that might better balance competing goals to maximize overall benefits for the population. The primary focus should be on ensuring that policies are implemented in a way that minimizes restrictive impacts on trade (Casalini and González, p.13).

Soft law, in the form of guidelines or voluntary documents, offers several advantages over traditional regulations. Its instruments can be adopted and revised relatively quickly, by bypassing the lengthy bureaucratic rulemaking process typically required by governments. It also allows for the simultaneous testing of different approaches, though this can sometimes lead to inconsistencies among private standards and other soft law instruments. Additionally, soft law fosters a cooperative rather than adversarial relationship among stakeholders. Unlike formal regulations, it is not limited by delegations of authority and can address concerns arising from emerging technologies. Moreover, since it is not adopted by a formal legal authority, soft law is not restricted to specific legal jurisdictions, enabling it to have broader international applicability. (Marchant, 2019, pp. 4-5).

When implementing soft law approaches, compliance is driven not by adherence to a pre-established norm but by its demonstrated effectiveness and efficiency. Legal frameworks adapt to the realities of the situation, rather than imposing rigid standards onto them. In this sense, soft law embodies a lesson in humility regarding legality and legitimacy, recognizing that these concepts are always subject to the evolving dynamics of society. (Sorel, 2021).

B. Guidance documents as complementary tools to regulation

Taking into consideration the fast-paced growth of the commercial transactions –including the provision of services– in digital spaces, such as online marketplaces, the spread of new forms of trademark counterfeiting in such environments is not a surprise. During our research for drafting this Guidebook, we found a significant gap in the availability of guidance documents for digital platforms in this area, underscoring the need for complementary tools to support traditional hard law regulations.

The application of soft law presents an effective and flexible alternative for addressing gaps in regulatory frameworks that exacerbate trademark counterfeiting in the digital environment. Technology companies like Facebook, Microsoft, Twitter, and YouTube, which are active participants in initiatives like the EU Internet Forum, have embraced their shared responsibility to balance the promotion of freedom of expression with the mitigation of illegal activities online (European Commission, 2016, p. 1). By leveraging voluntary commitments and collaborative guidelines, these platforms can play a pivotal role in reducing trademark counterfeiting while fostering a safer digital ecosystem.

The EU's experience in addressing illegal online hate speech offers valuable insights into how soft law measures can complement traditional enforcement mechanisms. For instance, major technology companies in the social media and online services sectors have voluntarily implemented a *Code of Conduct on Countering Illegal Hate Speech Online*. This code not only provides internal guidelines for addressing hate speech but also encourages the sharing of best practices among industry players. The approach combines self-regulation with public accountability, as regular assessments of its implementation are reported to key stakeholders, such as the *High Level Group on Combating Racism, Xenophobia, and Intolerance* (European Commission, 2016, p. 3)

In this way, while there is a robust system of enforcement of criminal law sanctions against the individual perpetrators of hate speech, this effort is supposed to be complemented with concrete actions aimed at ensuring that illegal hate speech online is expeditiously acted upon by online intermediaries and social media platforms, upon receipt of a valid notification, in an appropriate time-frame; so notifications should be precise and adequately substantiated to be considered valid (European Commission, 2016, p.1).

Another prominent example is the EU's *Communication on Tackling Illegal Content Online*. This document provides non-binding guidance to online platforms, aiming to establish a unified approach to tackling illegal content. This includes encouraging platforms to adopt good procedural practices and fostering collaboration with law enforcement while safeguarding free speech. This guidance complements sector-specific dialogues, striking a balance between fast content removal, crime prevention, and the protection of fundamental rights (European Commission, 2017, p. 20).

Recent initiatives outside the EU, such as the agreement signed in 2022 under the auspices of Russia's Federal Antimonopoly Service, further underscore the role of self-

regulation in addressing digital marketplace challenges. The *Principles of Interaction of Digital Market Participants* and subsequent *Standards of Interaction between Marketplaces and Suppliers* represent a voluntary commitment by information technology companies and private market participants to prevent unfair practices and the sale of counterfeit goods (Federal Antimonopoly Service, 2024, p. 4).

These guiding documents developed a set of good practices for marketplaces and right holders/sellers' interaction, to prevent the sale of counterfeit goods. The application of the aforementioned intends to increase self-regulation of the industry, therefore fighting against trademark counterfeiting. The immediate results are showing: since July 2023, more than 4.5 million publications of unoriginal goods have been blocked (Federal Antimonopoly Service, 2024, p. 4).

Overall, we can see how the existing regulatory frameworks for the digital environment in several economies have been complemented by a number of non-legislative measures. To give some examples in addition to those already mentioned, we find guidance documents such as the *Memorandum of Understanding on the sale of Counterfeit Goods*, the EU Commission *Notice on the market surveillance of products sold online*, and the *European Strategy for a Better Internet for Children*. All these examples complement aspects that regulation, in this case European regulation, does not directly cover (European Commission, 2017, pp. 3-4).

Another reason why this approach makes sense for the digital ecosystem is that online platforms need the resources to navigate the legal frameworks in which they operate. In many cases, hard law regulations are general and do not always provide mechanisms for close cooperation with competent authorities. This is highly desirable, for example, to ensure that takedown requests for illegal content are communicated in a timely and effective manner. (European Commission, 2017, p. 7).

Considering the absence of specific regulations on trademark counterfeiting for digital platforms in APEC economies, as well as the potential of guidance documents as an effective tool in the absence of mandatory regulations, it is recommended that the APEC economies come together to initiate a conversation aimed at the elaboration of a voluntary document of good practices to combat trademark counterfeiting for online platforms.

This document of good practices would provide a non-binding yet influential framework for aligning the efforts of digital platforms and relevant stakeholders in tackling online trademark

counterfeiting. Authorities related to IP enforcement in the digital environment from each APEC economy, as well as representatives of the platforms operating in these economies, could be invited to contribute to the creation and implementation of these good practices.

Drawing inspiration from initiatives like the EU's Memorandum of Understanding on Counterfeit Goods, this voluntary document could serve as a practical benchmark, encouraging platforms to adopt consistent anti-counterfeiting practices tailored to local and regional contexts.

The implementation of such a document could be supported by local initiatives from APEC economies to encourage adherence. For instance, economies could establish programs for the recognition of platforms that effectively adopt and implement the good practices outlined in the document, promoting visibility of these efforts and fostering peer emulation within the industry.

3. *Digital forensics for IP rights enforcement*

This recommendation focuses on integrating digital forensics into the strategies of law enforcement agencies to enhance the protection of IP rights in the digital ecosystem. By encouraging each APEC economy to assess its specific needs, develop tailored training programs, and collaborate on technical assistance, this approach aims to strengthen the enforcement capabilities of law enforcement agencies, ensuring more effective responses to IP infringements in the digital environment.

A. Definition of digital forensics

Although processes like digital forensics have long been discussed in computer science literature, the field was not well defined until the 1980s when it began to attract interest. The first personal computers made access to this technology more widely available, which increased interest in digital evidence. As a result, a large group of people formed a digital forensics community, which became more official in 1993 when the US Federal Bureau of Investigation hosted the First International Conference on Computer Evidence. Initially, the focus was on examining stand-alone computers to recover deleted or damaged material from the hard drives. But since the early 2000s, the field of digital forensics has gradually grown and evolved alongside legislation. Today, users tend to use multiple digital devices and access tens of digital services every day. The digital footprint of our daily lives has become enormous, and the likelihood of illegal activities leaving digital evidence is correspondingly high (Casino et al., 2022).

In terms of definition, the National Institute of Standards and Technology Glossary (NIST) 2021 describes digital forensics as “the application of computer science and investigative techniques to the examination of digital evidence - following proper search authority, chain of custody, mathematical validation, use of validated tools, repeatability, reporting, and possibly expert testimony”. These techniques are used in criminal investigations as a means of identifying the perpetrator or accomplice of a crime and their associated actions. They are sometimes used in IP cases to establish the rightful ownership of a variety of objects, both written and graphic, and in cases of fraud and counterfeiting (Johnson, Davies and Reddy, 2022).

Forensic science can be defined as the application of scientific or technical approaches to the identification, collection, analysis and interpretation of evidence in legal proceedings

and encompasses a number of disciplines, each providing techniques and procedures. In particular, digital forensics is one of the primary fields, as all forensic sciences use valid principles and methods in the evaluation of evidence that is referred to as scientific evidence. Furthermore, the evidence must be empirical as it provides support to either accept or refute a hypothesis and conclude on the guilty or innocent outcome. It is essential for actual evidence that it can be explained and justified by systematic and experimental methods (Arshad, Jantan and Abiodun, 2018, p. 348).

B. Application of digital forensics in IP infringements

When IP rights infringements occur in the digital space, digital forensics helps to preserve evidence, conduct forensic analysis, and present findings of fact in legal proceedings. It also helps to determine the extent of the infringement, identify the responsible parties and prove the intent behind the illegal activities. Digital forensic techniques such as data carving, deleted file retrieval, chat history analysis, metadata analysis, network forensics and file identification help to identify counterfeit products, pirated software, unauthorized distribution of copyrighted material and other IP rights infringements. The results of digital forensic investigations are of great value in court, providing irrefutable evidence and assisting in the successful prosecution of offenders (Hegde, Naik and Kumar, 2024. p. 501).

Digital forensics plays an important role in protecting IP rights. For example, if a company suspects software theft or infringement, digital forensics experts will image the hard drive of the suspected infringer's computer, taking a complete snapshot of its contents, and then analyze the data to identify any signs of software theft or infringement. This may include examining files, metadata, logs, and other digital artefacts. Based on the forensic findings, appropriate remedial actions can be taken, such as removing unauthorized copies, securing IP, and initiating legal proceedings against the infringing party (Hegde, Naik and Kumar, 2024, p. 501).

C. Digital forensics application in law enforcement

Today's protection structure must actively seek out new approaches and tools such as encryption, biometrics, and artificial intelligence (AI). This is not only to provide an anti-fragile digital infrastructure, but also to provide the ability to detect and counter risks to the organization's IP assets (Mavani, et al, 2024, p. 530).

Identifying whether the threat to the organization is external, internal or both is an excellent first step in applying digital forensics. As with any digital investigation, examiners need to fully understand the scope of the case by identifying key custodians involved in the development of IP, including creators, inventors, or other stakeholders. All of the custodians involved are potential sources of information that can help guide the case and best prepare an examiner for the next step of identifying data sources. It is common to find multiple data sources for each custodian involved (Magnet Forensics, 2023).

D. The Philippines' National Bureau of Investigation (NBI) case:

In a case that illustrates this point well, the NBI in the Philippines used digital monitoring and intelligence gathering to track down an online seller who was allegedly selling overpriced counterfeit designer bags. NBI agents closely monitored the seller's activities on social media platforms, particularly during live sales sessions, which have become increasingly popular for showcasing and selling goods online. Through a combination of cyber and physical intelligence, they were able to gather the necessary information to apply for a search warrant, which was promptly approved by the court.

Once the warrant was granted, NBI agents raided the online seller's boutique while the counterfeit bags were being marketed during a live sales event. This operation highlights the critical role that digital forensic tools, such as online monitoring and data collection from social media platforms, can play in combating online counterfeiting. By using digital evidence such as posts, videos and online sales data, the authorities were able to gather the evidence they needed to act quickly and legally. The success of the operation was largely due to timely and efficient intelligence gathering, proper coordination between law enforcement agencies and cooperation with private complainants, demonstrating the vital role of digital forensics in modern IP enforcement efforts.

This recommendation aims to promote the effective adoption of digital forensics in APEC economies by focusing on individual actions that each economy can undertake to strengthen IP enforcement in digital environments.

Identify resource needs and gaps:

- Each economy should assess its current capabilities and determine the resources needed for effective implementation of digital forensics, such as personnel, infrastructure, and tools.

- This includes defining the minimum trained personnel required and identifying specific technological resources necessary for monitoring and enforcement activities.

Development of specialized training programs:

- Economies should design and implement capacities building initiatives for enforcement personnel, focusing on technical expertise in forensic analysis, data interpretation, and investigative methods.
- These programs can be developed locally or in collaboration with economies that already have robust digital forensics frameworks.

Seek technical cooperation and assistance:

- Economies with limited experience in digital forensics are encouraged to seek cooperation or technical assistance from economies with advanced capabilities, whether within or outside APEC.
- This could involve sharing best practices, providing training support, or facilitating access to digital tools and platforms.

Promote simulation exercises locally:

- Economies are encouraged to organize local simulation exercises to test and refine their digital forensics processes.
- These exercises should mimic real-world scenarios to identify operational gaps and improve enforcement strategies.

In this way, by focusing on individual actions and fostering technical cooperation, this recommendation ensures that economies can take concrete steps to leverage digital forensics effectively. This decentralized approach provides flexibility while encouraging knowledge sharing and capacity building across APEC economies.

4. *IP owners and digital platforms collaboration*

This advice underlines the critical importance of cooperation between IP owners and digital platforms to effectively combat trademark counterfeiting in the online environment. IP owners and digital platforms can benefit from working together as the first ones know their trademarks and products, while digital platforms have the technological capability to monitor, detect, and remove counterfeit listings.

A. Collaborating to combat the trademark counterfeiting

Collaborative platforms and industry initiatives play a crucial role in combating online trademark abuse (such as trademark counterfeiting in the digital environment) through collective action and information sharing; while some of its direct actions are to develop best practices, share intelligence, and coordinate enforcement efforts. Organizations such as the Anti-Counterfeiting Group (ACG) and the International Trademark Association (INTA) facilitate collaboration between trademark owners, law enforcement agencies, and online marketplaces (Thio, 2024, p. 716).

Even more, collaborative approaches involving cooperation between stakeholders, including trademark owners and online platforms, are essential for effective trademark protection. Industry best practices, such as the establishment of voluntary anti-counterfeiting programs and the adoption of enforcement procedures, facilitate proactive enforcement and mitigate the risk of online trademark abuse (Thio, 2024, p. 718).

These efforts often involve the establishment of industry-wide initiatives and partnerships aimed at addressing common challenges and sharing insights and resources. For example, industry associations and trade groups can facilitate knowledge exchange and capacity-building activities, such as workshops, training sessions, and information-sharing platforms (Thio, 2024, p. 719).

B. Successful examples of collaboration

Among examples of this kind of initiatives, most of the efforts led by the International AntiCounterfeiting Coalition (IACC) can be considered. It must be noted that the IACC is a non-profit organization dedicated to combating counterfeiting and piracy since its foundation in 1979. It is predominantly constituted by IP right owners, as well as IP

consulting and/or enforcement companies. This organization aims to deter counterfeiters, protect legitimate businesses, and safeguard consumers from potentially harmful and substandard products, through the articulation of IP owners and encouraging the participation of enforcement agencies and the international community. In order to achieve these objectives, the IACC has launched a number of programs and initiatives designed to address trademark counterfeiting through the cooperation of interested private stakeholders, including:

- The IACC-Amazon Program, initiated by a Memorandum of Understanding (MoU) in April 2018, is a unique voluntary collaboration supported by senior management and specialized teams within Amazon and the IACC. The Program focuses on streamlining, accountability and meaningful engagement – providing an expedited resolution path for enforcement issues as well as a real-time feedback mechanism to drive long-term solutions. It is a collaboration designed to continuously evolve and bolster IP enforcement on Amazon, not only to the benefit of Program participants but also the entire right-holders community (International AntiCounterfeiting Coalition, 2024).
- The IACC MarketSafe is the result of a long-standing strategic collaboration between the IACC and Alibaba Group. This one-of-a-kind program provides right-holders with a streamlined mechanism for expedited take-down actions against infringing listings and sellers, complex issue resolution and special policies to address counterfeiters' evasive tactics, and the hands-on support of dedicated Chinese-speaking analysts. It also facilitates dialogue between companies and Alibaba to strengthen preventative measures and address policy concerns. Thanks to the strong commitment from the IACC and Alibaba's senior management, right-holders can address emerging trends and issues on the platform effectively through the program. Since 2014, the IACC MarketSafe Program has served more than 190 brands across 40 industries, large and small, members and non-members. Over 760,000 infringing product listings and 16,100 sellers have been permanently removed from the platforms, making the program the most successful industry association collaboration with Alibaba.

With an expedited registration process, take-down procedures, and an easy-to-use submission portal, the IACC MarketSafe Program provides all the necessary tools for right-holders, large and small, to achieve effective enforcement on Alibaba

platforms. Each right holder is assigned to a dedicated IACC analyst who assists in resolving communication/language issues and provides additional assistance throughout their participation (International AntiCounterfeiting Coalition, 2024).

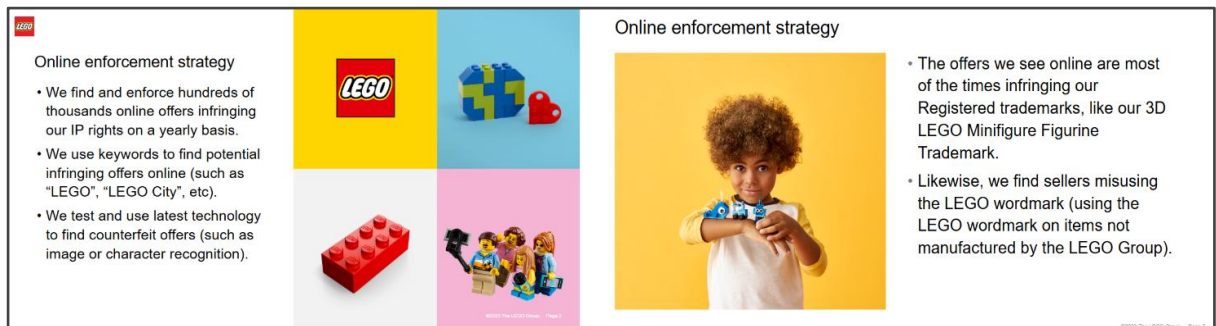
Another successful case of collaboration can be found in LEGO's partnership with Mercado Libre, as this illustrates how cooperation between private actors, such as IP owners and digital platforms, can enhance efforts to combat trademark counterfeiting in the e-commerce space. In particular, this collaboration targets the Latin American market, with a focus on key economies such as Mexico and Brazil, where LEGO's sales are significant.

As LEGO's largest market in the region, Mexico has become a key focus for the company's anti-counterfeiting efforts. Through its partnership with Mercado Libre, LEGO has integrated its trademark protection initiatives into the platform's operations, using advanced technologies such as image and character recognition tools to detect counterfeit products. This proactive collaboration has been instrumental in identifying and quickly removing infringing items from Mercado Libre's listings, significantly reducing the risks posed by infringing goods.

One of the key strengths of this partnership is the use of AI-powered systems that automate the process of detecting counterfeit listings. LEGO uses technology that compares images of products posted on the platform against a database of its registered IP rights, enabling it to quickly identify infringements.

Image N° 3

LEGO Online enforcement strategy



The infographic is titled "LEGO Online enforcement strategy" and is divided into two main sections. The left section, titled "Online enforcement strategy", lists three bullet points: "We find and enforce hundreds of thousands online offers infringing our IP rights on a yearly basis.", "We use keywords to find potential infringing offers online (such as 'LEGO', 'LEGO City', etc).", and "We test and use latest technology to find counterfeit offers (such as image or character recognition).". The right section, also titled "Online enforcement strategy", features a large photo of a young child with curly hair holding a LEGO minifigure, and two smaller photos of LEGO products: a red brick and a blue and red minifigure. To the right of the child photo, there are two bullet points: "The offers we see online are most of the times infringing our Registered trademarks, like our 3D LEGO Minifigure Figurine Trademark." and "Likewise, we find sellers misusing the LEGO wordmark (using the LEGO wordmark on items not manufactured by the LEGO Group).". The infographic includes the LEGO logo in the top left corner and a small copyright notice "©2023 The LEGO Group" in the bottom right corner.

Online enforcement strategy

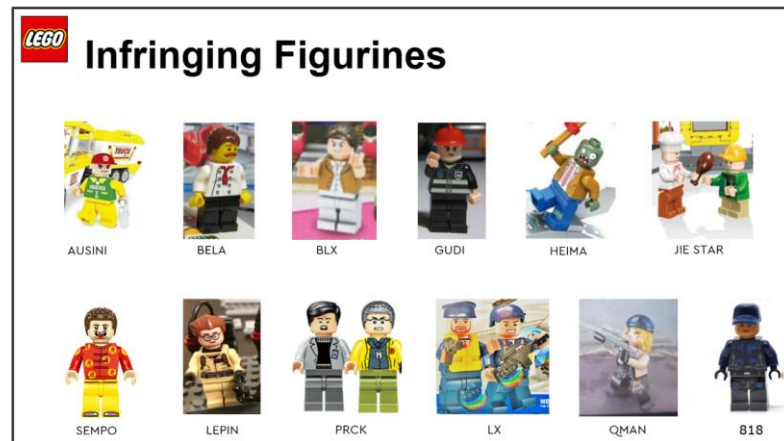
- We find and enforce hundreds of thousands online offers infringing our IP rights on a yearly basis.
- We use keywords to find potential infringing offers online (such as "LEGO", "LEGO City", etc).
- We test and use latest technology to find counterfeit offers (such as image or character recognition).

Online enforcement strategy

- The offers we see online are most of the times infringing our Registered trademarks, like our 3D LEGO Minifigure Figurine Trademark.
- Likewise, we find sellers misusing the LEGO wordmark (using the LEGO wordmark on items not manufactured by the LEGO Group).

Source: Ishbak, A. (2024). LEGO: Digital enforcement to improve fight trademark counterfeiting | APEC

Image N° 4



Source: Ishbak, A. (2024). LEGO: Digital enforcement to improve fight trademark counterfeiting | APEC

This has not only increased the efficiency of trademark protection, but also enabled a more systematic and scalable approach to combating counterfeiting in digital marketplaces. The success of this initiative in Mexico has set a strong precedent, and LEGO is now using it as a model to expand its efforts in other Latin American markets.

The collaboration between LEGO and Mercado Libre also highlights the importance of adapting anti-counterfeiting strategies to the unique legal and regulatory contexts of each economy. By engaging with local partners and platforms, LEGO has been able to navigate the complexities of the regional market while strengthening its trademark protection efforts.

Image N° 5

Mercado Libre Anti-counterfeit Alliance Collaboration Agreement



Source: Ishbak, A. (2024). LEGO: Digital enforcement to improve fight trademark counterfeiting | APEC

Another case worth mentioning is the approach taken by INTA, a global non-profit organization dedicated to trademark owners and professionals. INTA is a strong example of collaboration between IP owners and digital platforms because it brings together the expertise of trademark owners, legal professionals, and digital tools to address the challenges of trademark protection in the evolving online environment.

As the representative organization for IP owners, INTA understands the complexities of digital platforms and the growing problem of online infringement, such as counterfeiting and unauthorized use of trademarks. Through this collaboration, INTA creates educational tools, such as INTA To Go, that help trademark owners leverage digital resources and strategies to protect their IP in an increasingly digital marketplace.

The impact of this collaboration is particularly evident in the INTA To Go platform. The initiative provides a centralized digital space where trademark owners can access a variety of resources that address current challenges in the digital world, such as e-commerce counterfeiting and enforcement on online platforms.

By partnering with digital platforms and experts, INTA To Go provides practical, real-world knowledge and strategies that IP owners can apply directly to protect their trademarks. The platform's comprehensive approach, which includes live and on-demand webcasts featuring discussions with policy experts and industry leaders, ensures that trademark owners are equipped with the most up-to-date information.

Collaboration involving IP owners and digital platforms has proven to be both possible and effective. The long-term benefits of these projects are clear but they additionally improve the industry as a whole by allowing it to adapt and enhance its operations. This form of collaboration should be encouraged by APEC economies to yield positive outcomes and to assist law enforcement authorities in combating trademark counterfeiting in online environments.

Strengthening collaboration between IP owners and digital platforms is essential to effectively address trademark counterfeiting in digital environments. This recommendation outlines practical approaches for IP owners to actively engage in these efforts.

A practical and efficient way to achieve this would be for trademark owners to join existing initiatives, such as the IACC, INTA, or any other organization dedicated to combating trademark counterfeiting, especially those focused in digital or e-commerce environments. Membership in these initiatives can provide concrete benefits, such as access to capacity-building programs designed to strengthen enforcement capabilities, digital tools to support trademark protection efforts, and opportunities for direct engagement with digital platforms to address trademark misuse. By leveraging these resources, trademark owners can enhance their ability to combat counterfeiting effectively while fostering collaboration with key stakeholders in the digital ecosystem.

However, it is important for each IP owner to consider the specifics of the economy in which they operate, including their commercial interests and the real risks they face. These factors may vary depending on the relevance of their trademark in the market, the type of product or service they offer, and the digital channels they use for distribution.

Another alternative is for trademark owners to directly approach digital platforms, particularly if such trademarks have a wide reputation and sufficient market presence (e.g. most well-known trademarks), in order to formalize cooperation agreements, as was seen in the case of the collaboration between LEGO and Mercado Libre. These agreements could coordinate joint efforts to combat trademark counterfeiting more effectively. This approach requires strong negotiation capabilities from trademark owners and a voluntary interest from digital platforms in aligning their efforts.

Collaborative efforts among IP owners could also be directed towards capacity building. Examples such as INTA's training initiative for private IP rights enforcers, INTA to go (discussed in more detail later in this document), can be considered for this purpose. Similarly,

APEC economies' own IP owners can work with the most relevant digital platforms in their economies, first to identify the capabilities that need to be developed to combat trademark counterfeiting on those platforms, and second to promote strategies to strengthen those capabilities, such as the creation of IP enforcement strengthening programs offered in cooperation with digital platforms.

Promoting these strategies will enable IP owners to better protect their trademarks and contribute to a safer digital ecosystem.

5. *Cooperation between private stakeholders and government authorities*

Several economies often struggle with limited capacities and resources to deal with the issue of trademark counterfeiting in the digital environment. Therefore, in the absence of adequate regulatory frameworks or funds for the implementation of technologies, cooperation between private (e.g., digital platforms and trademark owners) and public actors is a viable alternative.

In this sense, one of the strategies most widely adopted by various economies is the development of cooperation strategies between public institutions in charge of the fight against trademark counterfeiting and private actors. This strategy is recommended as a first step towards strengthening the institutional capacity of economies to combat the crimes analyzed here.

A. Importance of cooperation strategies

Such collaborations are particularly valuable in contexts where organizational partnerships with dispersed stakeholders —such as communities, advocacy groups or commercial enterprises— are essential to achieving common goals. These partnerships can help reduce operational costs, improve organizational efficiency and facilitate knowledge sharing. Close and sustained interactions among participants create opportunities for learning and innovation, increasing the overall effectiveness of anti-counterfeiting efforts (Desai, 2018, p. 222).

In addition, collaborative agreements allow organizations to gain direct access to critical information from both participants and third-party observers, fostering greater transparency and mutual trust. These arrangements encourage stakeholders to share relevant data and insights, enhancing the legitimacy of the organizations involved and improving their ability to address specific challenges, such as trademark counterfeiting, in a targeted and sustainable manner (Desai, 2018, p. 224).

Traditional remedies for trademark counterfeiting often rely on adversarial, litigation-based approaches that focus primarily on punishing offenders rather than implementing systemic changes. This model typically neglects opportunities for collaboration or institutional reform that could lead to sustainable improvements in enforcement mechanisms. In contrast, a multi-stakeholder approach allows different actors to work

together to identify challenges, implement institutional changes, and effectively monitor progress (Chavis, 2008, p. 497).

Collaboration among interested private stakeholders and enforcement authorities is key for combating online trademark abuse. Trademark owners can report instances of counterfeiting, piracy and trademark infringement, enabling authorities to act quickly to disrupt illegal operations. Given the transnational nature of the digital environment, cooperation between stakeholders—including government agencies, online platforms, international organizations and trademark owners—is essential. Voluntary anti-counterfeiting programs and standardized notice and takedown procedures exemplify industry best practices, facilitate rapid enforcement, and reduce the prevalence of online trademark infringement. In addition, knowledge-sharing initiatives and capacity-building efforts raise awareness and promote a culture of respect for IP rights within digital ecosystems (Thio, 2024, pp. 717 - 718).

Beyond traditional enforcement, working with e-commerce marketplaces and online platforms offers significant opportunities to combat trademark counterfeiting. By partnering with these platforms, IP enforcement authorities can increase their capabilities and promote robust anti-counterfeiting methods, such as proactive content monitoring, seller verification processes, and the implementation of takedown mechanisms for infringing content. These collaborative approaches not only improve enforcement, but also increase trust and transparency among public and private stakeholders in the digital marketplace, thereby strengthening efforts to protect IP rights (Thio, 2024, pp. 718 - 719).

B. Applied cases

Collaborative efforts to combat trademark counterfeiting have been successfully exemplified by several global initiatives that bring together public and private stakeholders. One notable example is the Interpol Intellectual Property Crime Action Group (IIPCAG), which was established as a public-private partnership (PPP) to support Interpol's programs against IP crime. Initially supported by the music industry, the group evolved into a network of collaborative sub-PPPs, organizing activities such as anti-crime operations, training seminars and conferences, and managing a database to facilitate information exchange. Private sector members not only provided strategic advice but also contributed significant resources to these initiatives. Notable participants included organizations such as the Coalition for Intellectual Property Rights, the Global Anti-

Counterfeiting Group and the International Chamber of Commerce Business Action to Stop Counterfeiting and Piracy (Paun, 2011, p. 11).

One of the IIPCAG's key initiatives is to conduct training seminars for law enforcement officials to enhance their understanding of the methods used by IP criminals and to improve their ability to distinguish counterfeit products from genuine ones. These educational efforts provide law enforcement with the practical tools needed to effectively combat IP crime in a globalized economy (Paun, 2011, p. 11).

Another important example of collaborative innovation is the Interpol Database on International Intellectual Property, which serves as a centralized repository of information on IP crimes. Launched in 2006, the database collects data from both public law enforcement agencies and affected industries, providing a comprehensive, cross-industry perspective on IP crime. By 2009, it had expanded to include data from 20 industry sectors, providing critical insights that enhance Interpol's ability to coordinate global responses to IP violations. This initiative underscores the value of sharing resources and information to strengthen the fight against trademark counterfeiting and other IP crimes (Paun, 2011, p. 12).

Also, an important example to be considered as well is the EU's Intellectual Property Enforcement Portal (IPEP). This initiative provides a compelling example of how technology and coordination can be used to combat counterfeiting in the e-commerce era. With the growing flow of products entering the EU from third economies —often from clandestine markets or illegal channels— counterfeit goods have become more specialized and complex. Counterfeiters are increasingly using digital platforms, social media, and instant messaging to source components and distribute their products, challenging traditional enforcement methods. The IPEP, launched by the EUIPO in 2013, directly addresses these issues by providing law enforcement agencies in all EU member states with access to a secure database for monitoring and reporting IP rights infringements (EUIPO, 2023, pp. 12-13).

One of IPEP's key features is its statistical module, which collects data from customs via the anti-counterfeit and anti-piracy information system and records detentions of IP rights infringing goods. This centralized repository not only tracks the movement of counterfeit goods but also provides valuable insights for designing coordinated enforcement strategies. The platform also facilitates seamless two-way communication between right

holders and enforcement authorities, such as customs and market surveillance authorities. This enables swift action against infringers and increases transparency in enforcement activities (EUIPO, 2023, pp. 13 - 14).

IPEP has also extended its network to e-commerce marketplaces, allowing these platforms to become members and participate in data exchange with enforcement authorities. This collaboration fosters stronger relationships between marketplaces and law enforcement, creating opportunities for proactive interventions against counterfeiting activities in the digital domain. In addition, right holders can submit *applications for action* directly through IPEP, requesting customs to assist in the protection of their IP rights under Regulation (EU) 608/2013 (EUIPO, 2023, p. 14).

Another notable example of collaborative efforts in the fight against trademark counterfeiting is Mercado Libre's proactive approach to partnering with public institutions and industry organizations. While the COVID-19 pandemic caused delays in the implementation of some partnerships, Mercado Libre still remains committed to resuming these efforts once procedural normalcy returns (Rodríguez, 2021).

In this order of ideas, the company has signed a cooperation agreement with Indecopi. This agreement aims to protect the IP rights registered in Peru. As part of this collaboration, Mercado Libre provided Indecopi with a monitoring and reporting tool to enhance its enforcement capabilities.

Between 2020 and 2024, collaborative efforts between Indecopi and Mercado Libre platform achieved notable progress in combating trademark infringement in digital environments. During this period, a significant number of virtual stores engaged in illicit activities —such as selling products that violate trademark rights— were shut down, with closures rising from 151 in 2020 to 223 in 2023.

Although the number of takedowns might appear modest in isolation, each action was accompanied by the initiation of infringement proceedings by Indecopi. This comprehensive approach not only reduces the presence of illegal listings but also strengthens enforcement by holding infringers accountable through formal legal measures.

These interventions were made possible by the authority granted under Peruvian legislation, specifically Article 115, paragraph (e) of Legislative Decree 1075, as amended by Legislative Decree 1397. This provision empowers Indecopi to impose corrective measures aimed at mitigating or preventing the continuation of actions that violate trademark rights.

In addition to the agreement with Indecopi, Mercado Libre has signed similar cooperation agreements across Latin America, reflecting a broad commitment to IP rights protection. These partnerships include stakeholders such as the Argentine Chamber of Books, the Colombian Chamber of Books, the Argentine Chamber of Producers of Phonograms and Videograms, the Brazilian Film Agency, the National Association of Uruguayan Broadcasters, and the Mexican Institute of Industrial Property (IMPI). Each of these agreements covers specific aspects of IP protection, ranging from books and music to audiovisual content, thereby addressing different areas of counterfeiting. Mercado Libre is also actively negotiating additional agreements, further strengthening its network of partnerships to maintain IP standards throughout the region (Rodríguez, 2021).

C. Highlights from surveys results

The survey of policymakers reveals a range of activities undertaken by some economies to improve enforcement and information sharing with major e-commerce platforms. Information sharing as a key measure is a common practice in several economies, including Japan; the Republic of Korea; Mexico; Peru; the Philippines; Chinese Taipei; and the United States. This information sharing allows economies to track infringing activity and respond quickly to infringements. Information sharing with e-commerce platforms highlights a proactive approach as economies work to stay on top of trends and anticipate new counterfeiting tactics.

Beyond information sharing, some economies have taken additional steps by participating in joint enforcement actions. Economies such as the Republic of Korea; Mexico; Peru; the Philippines; Chinese Taipei; and the United States not only share information with these platforms, but also cooperate in active enforcement initiatives. Joint enforcement initiatives have a more immediate impact, allowing IP authorities to work with e-commerce platforms to identify and remove counterfeit listings in real time. These operations are particularly valuable in disrupting large-scale counterfeiting networks and reducing the availability of counterfeit products online.

The Republic of Korea; the Philippines; Chinese Taipei; and the United States are also engaged in training and capacity-building activities with e-commerce platforms. These efforts reflect a broader commitment to enhancing the capabilities of law enforcement teams and ensuring that personnel are equipped with the skills necessary to combat sophisticated counterfeiting methods. In addition, the economies of the Republic of Korea; the Philippines; and the United States are engaged in the development of best practices, contributing to the creation of standardized guidelines that inform effective strategies for both platforms and regulators. These best practices serve as a reference for systematically addressing trademark counterfeiting, providing consistent protocols that can be adopted across different regions.

Through these diverse partnerships, economies such as the Republic of Korea; the Philippines; Chinese Taipei; and the United States are demonstrating a comprehensive approach to counterfeiting that goes beyond law enforcement, fostering stronger relationships and establishing common standards with key stakeholders in e-commerce. The diversity of cooperative efforts, from information sharing to the development of best practices, underscores the commitment to building a resilient defense against online counterfeiting on multiple fronts.

As can be seen from both the case studies and the survey results, many APEC economies have succeeded in developing forms of cooperation between IP enforcement authorities and key private stakeholders.

This recommendation builds on this model and suggests using APEC's regional convening power to enable relevant IP enforcement authorities from member economies to improve their negotiating capabilities to develop agreements with marketplaces, social networks, among other digital platforms, or guilds and associations representing trademark rights holders.

The recommendation recognizes that it may be challenging for government authorities of certain APEC economies to engage in negotiations with some of the major players in the global digital marketplace. In this sense, it is proposed to use the convening power of APEC to negotiate cooperation agreements on anti-counterfeiting measures in the digital environment with key private stakeholders.

In this way, representatives from APEC economies could group together, especially in the negotiation phase, based on the similarity of the reality of their digital markets (e.g.,

marketplaces with greater presence, common trademarks in all these markets, etc.) and from there promote the development of public-private cooperation agreements. However, the execution and monitoring of the implementation of each agreement would be an individual task between each participating economy and the respective private actors.

Another modality of cooperation among these stakeholders can be achieved if each economy or groups of related economies set up anti-counterfeiting working groups or committees. These teams would integrate relevant public and private players for the analysis and design of strategies to combat trademark counterfeiting practices in the most important digital spaces of their respective economies.

For example, the public-private partnership approach promoted by the Korean Intellectual Property Office (KIPO), through its Anti-Counterfeiting Council, allows us to better understand this modality of cooperation. This organization is the result of a multi-stakeholder cooperation initiative, which brings together both government agencies and key private stakeholders to facilitate communication and decision-making on concrete actions to combat trademark counterfeiting in online space (e.g. removal of counterfeit listings, blocking of counterfeit sites). This example will be better explained in the case study section of this Guidebook.

As with KIPO's Anti-Counterfeiting Council, the aim of the committees proposed by this recommendation would be to combine the resources, experience and regulatory authority of both sectors. In this way, by combining public regulatory authority with private sector expertise in technology and market dynamics, each committee can significantly enhance their enforcement capabilities.

6. *Coordination between private stakeholders and Top-Level Domains operators to combat trademark counterfeiting*

This recommendation advocates for an enhanced coordination between trademark owners, digital platforms, and top-level domain operators to combat trademark counterfeiting. Currently, the lack of a unified approach between these stakeholders often results in ineffective enforcement against infringing websites, as domain names—whether generic Top-Level Domains (gTLDs) or country code Top-Level domains (ccTLDs)—serve as key entry points for counterfeit activities.

A. *Domain names' role in IP enforcement*

The Domain Name System (DNS) is the backbone of online navigation, and its management plays a key role in combating IP infringement on the Internet. At the heart of DNS management is the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organization that oversees the technical administration of gTLDs and ccTLDs (Marks and Nordeman, 2022, p. 7).

When websites infringe IP rights, their domain names—whether gTLDs or ccTLDs—often serve as critical entry points for infringing activities. A common enforcement strategy is to suspend or freeze domain names. Suspension completely disables the associated website, preventing users from accessing its content. This method is effective in removing the visibility of infringing content but is limited because the underlying website remains accessible via its IP address unless removed by the hosting provider. Domain name blocking, on the other hand, prohibits the transfer or modification of registrant information but does not disable the website, making it a complementary but incomplete remedy in the fight against IP infringement (Marks and Nordeman, 2022, p. 21).

Despite their usefulness, these measures are often criticized as "blunt instruments" that do not address more nuanced issues, such as the removal of specific content or URLs. Their success depends on effective cooperation between registries, registrars, and law enforcement, and the establishment of policies that balance the efficiency of enforcement with broader considerations such as due process and freedom of expression (Marks and Nordeman, 2022, p. 21). In this context, targeted policy refinement and stakeholder engagement are essential to maximize the effectiveness of domain name enforcement mechanisms.

While ICANN coordinates gTLD policies and accredits registrars and registry operators, the administration of ccTLDs is largely the responsibility of individual local authorities. For example, Korea's .kr domain is administered by the Korea Internet & Security Agency, a government agency, while Germany's .de domain is administered by the German Network Information Center (DENIC), a non-profit cooperative on behalf of the government (Marks and Nordeman, 2022, p. 7).

There is evidence that the ccTLD operators' control over the domain name space can effectively enforce policies against trademark infringement. Therefore, collaborating with ccTLD operators offers significant advantages for IP owners in protecting their trademarks against counterfeiting.

Some ccTLD operators have access to advanced detection technologies, such as automated systems for monitoring domain registrations and identifying patterns of abuse (EUIPO, 2021, p. 21). For example, the Internet Domain Registration Netherlands Foundation (SIDN), the operator of the .nl ccTLD, uses tools such as BrandCounter and FaDe to identify and suspend thousands of suspicious domains, including over 6,000 counterfeit webshops in a single registrar operation. These measures significantly reduce counterfeit activity on the .nl domain (EUIPO, 2021, p. 27).

Other ccTLD operators, such as the European Registry for Internet Domains (EURid) (.eu) and Domain Name Server Belgium (.be), enhance their control by verifying the identity of domain registrants and restricting proxy services. Automated systems proactively detect and suspend abusive domain registrations, while notice-and-takedown procedures ensure swift action against illegal activity. These initiatives demonstrate the critical role of ccTLD operators in combating trademark counterfeiting through localized and proactive measures (EUIPO, 2021, p. 24).

B. Domain names dispute-resolution mechanisms towards trademark protections

ICANN oversees compliance with obligations established by the global multistakeholder community, particularly for ICANN-accredited registrars. These registrars must address abusive domain name registrations, including reports of IP infringement. Policies require registrars to maintain a permanent abuse point of contact to receive and act upon abuse reports, including those from law enforcement and consumer protection authorities.

Reports of illegal activity must be reviewed within 24 hours by a qualified individual authorized to take appropriate action (ICANN, 2022, p. 3).

Such institutions provide dispute-resolution and rights-protection mechanisms, such as the Uniform Domain Name Dispute Resolution Policy (UDRP), which allows trademark holders to resolve domain disputes through expedited administrative proceedings instead of court litigation. The UDRP applies across all gTLDs (ICANN, 2022, p. 4). Additional protections for trademarks in new gTLDs include the Uniform Rapid Suspension system and the ICANN's Trademark Clearinghouse (TMCH), which offers priority registrations for validated trademarks and maintains a centralized database for registries and registrars, as will be explained in more detail in this recommendation (ICANN, 2022, p. 5).

In the ccTLD context, dispute resolution procedures vary by jurisdiction. Some ccTLD registries adopt the UDRP or modified versions of it, while others create unique procedures. For instance, the .eu registry uses an alternative dispute resolution framework aligned with EU regulations and managed independently by appointed providers (ICANN, 2022, p. 5).

C. Highlights from surveys results

Surveys conducted as part of this project, addressed to policymakers, indicate that some economies are already adopting the collaborative approach. For example, Australia; the Republic of Korea; and the United States reported active cooperation between their respective ccTLD operators and trademark owners.

This cooperation is an important line of defense, as ccTLD operators play a central role in managing domain names within their jurisdictions and can significantly intervene in cases where counterfeit domain names are used. By fostering these partnerships, economies are better equipped to identify and suspend domain names involved in IP infringements, thereby reducing counterfeiting activity at its online source.

This recommendation specifically addresses trademark infringements occurring in domain names. It suggests that trademark owners can register their trademarks in the ICANN TMCH system as a preventive action, reducing the need to rely on dispute-resolution and rights-protection mechanisms such as the UDRP.

The TMCH is a mechanism developed by ICANN that acts as a central database for the protection of trademarks in the domain name system. Trademark owners submit their trademarks to the TMCH for verification to ensure their authenticity. Once validated, the TMCH allows trademark owners priority access to register domain names during the initial launch of new gTLDs.

It also provides a complaint notification system that alerts registrants when they attempt to register a domain name that matches a trademark registered in the TMCH, thus preventing cybersquatting. The TMCH maintains a secure data center of verified trademarks, accessible to accredited registrars and registries, and periodically revalidates trademarks to ensure their continued accuracy and protection.

It should be noted that this mechanism is functional for gTLD domain names, but does not cover ccTLD domain names, which are also quite common in the e-commerce landscape.

Therefore, additionally, it can be suggested that trademark owners could join together within their respective economies and initiate a conversation with the ccTLD operators present in their economies, in order to create a similar trademark registry, useful to prevent trademark counterfeit cases when registering a new ccTLD domain name. As evidenced by previously mentioned surveys, the economies where this collaborative approach has been applied have reported benefits in their fight against trademark counterfeiting in domain names.

7. Common frameworks alignment to combat trademark counterfeiting

Another key recommendation is to align common frameworks to combat trademark counterfeiting, following examples such as the APEC Privacy Framework and the APEC Online dispute resolution Collaborative Framework. Currently, there is a lack of harmonization and clear protocols between these frameworks regarding cross-border enforcement of IP.

A. International cooperation in IP law enforcement

International law enforcement cooperation against transnational organized crime often contrasts the adaptability of global criminals with the constraints faced by law enforcement agencies due to jurisdictional and procedural limitations. Despite these challenges, PPPs in law enforcement demonstrate a shift in traditional state control over the legitimate use of force, creating opportunities for cooperative action (Paun, 2013, p. 13).

Such cooperation can be analyzed through normative, procedural and organizational dimensions, with the normative framework focusing on the criminalization of activities under international and local law. For IP crimes, international harmonization of laws began with foundational treaties such as the Paris Convention for the Protection of Industrial Property (1883) and the Berne Convention for the Protection of Literary and Artistic Works (1886), and progressed with the establishment of the World Intellectual Property Organization (WIPO) in 1967, which oversees treaties securing IP rights (Paun, 2011, p. 5).

The TRIPS Agreement under the WTO was an important step in setting minimum global standards for IP, followed by ongoing negotiations on contentious issues such as public health, digital fair use, and penalties for IP crimes. Initiatives such as the Doha Declaration reflect ongoing debates on how to balance rights and obligations (Paun, 2011, p. 5).

Challenges remain in international cooperation against IP infringement, including adapting to Internet-related infringements, cross-border trade on e-commerce platforms, and inconsistencies in IP law enforcement across jurisdictions (Paun, 2011, p. 5).

B. Collaboration through APEC frameworks

Aligning legal frameworks across APEC economies is critical to effectively addressing digital infringements, which often span multiple jurisdictions. The aim is to harmonize laws on digital enforcement and establish a consistent approach to digital crimes and IP rights infringements. Key aspects of this alignment include standardizing definitions of these crimes, adapting legal frameworks to deal with extraterritorial jurisdiction (which allows prosecution of infringements that originate in one economy but affect another), and facilitating cross-border cooperation. These efforts will help law enforcement agencies to work together more effectively and improve the investigation and prosecution of trademark infringements in APEC economies (APEC Economic Committee, 2024).

APEC has made significant progress on the APEC Privacy Framework, which seeks to balance the protection of personal information with the promotion of the free flow of data to support the growth of e-commerce. This framework aims to prevent regulatory regimes that unnecessarily restrict the flow of information, which could harm global businesses and economies (Tan, 2008, p. 16). In contrast to the EU's more top-down regulatory approach, APEC is adopting a market-oriented strategy, focusing on industry self-regulation and co-regulatory models. Even in economies with existing privacy laws, such as Australia; Japan; and the United States, APEC emphasizes a less prescriptive approach (Tan, 2008, p. 17).

Despite its success, the APEC Privacy Framework faces challenges related to enforceability. The Framework provides a range of options for implementing its principles, including legislative, administrative or self-regulatory, but does not require a central enforcement body (Tan, 2008, p. 18). Member economies are encouraged to establish access points for redress and infringement prevention, but there is no mandate for specific legislative remedies. The focus remains on preventing the misuse of personal information to support international commerce, rather than protecting privacy rights more broadly (Tan, 2008, p. 20).

In 2019, APEC launched a pilot program to support the development of a collaborative framework for online dispute resolution (ODR) to help micro, small and medium-sized enterprises (MSMEs) efficiently resolve cross-border B2B disputes. The initiative works with regional arbitration and mediation centers that adhere to the Model Procedural Rules for the APEC Collaborative Framework for ODR of Cross-Border B2B Disputes (APEC Procedure Rules). These rules, based on the United Nations Commission on International Trade Law (UNCITRAL) Arbitration Rules and the UNCITRAL Technical Notes on ODR,

provide a structure for resolving disputes with fairness, transparency and confidentiality (Calliess and Heetkamp, 2019, p. 18).

The APEC Rules of Procedure outline a three-stage dispute resolution process. First, the parties engage in online negotiations. If the dispute is not resolved, it proceeds to online mediation and, if necessary, to online arbitration. Arbitration awards are enforceable under the New York Convention, ensuring that the results of the ODR process are internationally recognized. This framework provides an efficient, accessible and legally backed method of resolving commercial disputes, helping to streamline cross-border B2B transactions, particularly for MSMEs (Calliess and Heetkamp, 2019, p. 18).

The APEC ODR Collaborative Framework emphasizes that legal frameworks within APEC economies do not need to be identical but must effectively support the implementation of ODR mechanisms (APEC Economic Committee, 20/24, p. 7). Most economies participating in the Framework already have legal structures in place that are consistent with the UNCITRAL instruments referenced in the Framework, enabling them to implement ODR without the need for specific ODR legislation (APEC Economic Committee, 2024, p. 10).

In addition, the Framework includes a Model ODR Clause for Contracts to guide parties in agreeing to use ODR under the Collaborative Framework. This clause simplifies the process of incorporating ODR into contracts and ensures a smoother transition to resolving cross-border disputes through the APEC ODR system (APEC Economic Committee, 2024, p. 11).

This recommendation proposes the development of a comprehensive common framework to APEC member economies for aligning minimum standards aimed at detecting, addressing, and preventing trademark counterfeiting in the digital environment.

Unlike the second recommendation, which targets digital platforms, this initiative focuses on empowering IP enforcement authorities across APEC economies. The framework would go beyond gathering good practices by encouraging enforcement authorities, on a voluntary basis, to advocate for necessary regulatory adaptations or enhancements within their economies. This would help foster a unified understanding of digital counterfeiting challenges and establish shared tools to combat them effectively.

The proposed framework should prioritize adaptability, enabling APEC economies to customize its standards to suit their distinct legal and regulatory environments. This ensures that the framework remains applicable across diverse jurisdictions, enhancing its utility and relevance.

Key elements of the framework should include robust dispute resolution mechanisms and cross-border enforcement protocols to address jurisdictional challenges. Together, these components would provide a solid foundation for collective action against trademark counterfeiting in the digital environment.

To implement this initiative, APEC economies could establish a collaborative process by appointing representatives of IP enforcement authorities to draft the common framework, drawing on input from legal experts, trademark owners and interested digital platforms from different economies. Once drafted, the framework could be presented as a voluntary standard, accompanied by a toolkit with adaptable templates and practical examples of implementation.

8. *Enforcement mechanisms across jurisdictions for cross-border measures in the digital environment*

Cross-border enforcement mechanisms are essential to address the extraterritorial nature of IP rights infringements in the digital environment. These tools provide right holders with the means to protect their IP rights across local borders and ensure a coordinated approach to tackling online infringements (Rosati, 2023, p. 13). APEC economies can enhance their trademark enforcement capabilities by establishing and strengthening enforcement tools tailored to address digital counterfeiting.

A. Cross-border measures and applications

Key aspects include the extraterritorial application of enforcement mechanisms that extend the reach of local laws beyond territorial boundaries to combat the global scope of digital infringements. Judicial cooperation plays a crucial role through agreements and protocols that facilitate the mutual recognition and enforcement of judgments relating to IP infringements. In addition, administrative measures empower authorities in some jurisdictions to issue cross-border takedown notices or blocking orders for infringing content, further strengthening enforcement efforts (Rosati, 2023, p. 13).

Harmonization of IP enforcement rules has largely been achieved through the adoption of adequate standards, such as those established under the TRIPS Agreement. Part III of the TRIPS Agreement introduced detailed standards for the enforcement of IP rights, setting a baseline for Members to follow. However, many jurisdictions have adopted more extensive requirements than are established by the TRIPS Agreement to further strengthen enforcement measures. At a regional level, instruments such as the EU Directive 2004/48 (Enforcement Directive) provide minimum standards for the enforcement of all IP rights, allowing EU member states to implement more protective measures if they wish (Van Greunen and Gobac, 2021, p. 13).

Judicial jurisdiction in cross-border infringement cases poses significant challenges, despite efforts to harmonize rules. Under EU law, jurisdiction often depends on the localization of the infringing activities, with protection typically being governed by the law of the economy where the IP rights are registered (Van Greunen and Gobac, 2021, p. 16). Courts in different jurisdictions use three key criteria to determine jurisdiction: (i) accessibility, where jurisdiction is granted on the basis of the accessibility of the infringing

content within the economy; (ii) causation, where jurisdiction lies in the territory where the infringing act originates; and (iii) targeting, where courts consider jurisdiction on the basis of whether the infringing content is targeted at their territory (Van Greunen and Gobac, 2021, p. 19).

B. Specific enforcement mechanisms

Several enforcement tools target cross-border IP infringements, focusing on cooperation and harmonized procedures to overcome jurisdictional boundaries (Bulayenko et al., 2022):

- International injunctions: Some courts can issue extraterritorial injunctions requiring online platforms to remove infringing content worldwide. These injunctions extend the reach of judicial decisions and enhance the ability of right holders to address infringements beyond their domestic territory.
- Notice and takedown systems: Streamlined and harmonized procedures allow right holders to submit multijurisdictional takedown requests, ensuring more efficient removal of infringing content.
- Domain name seizures: Cross-border cooperation between local authorities and domain registrars allows the seizure of domains used for IP-infringing activities, regardless of their locality of registration.
- Information sharing: Law enforcement and IP offices share information on cross-border infringements, promoting coordinated enforcement strategies and reducing enforcement gaps.

C. Judicial cooperation in the EU

The EU has made considerable progress in improving judicial cooperation to facilitate cross-border enforcement, particularly in civil and commercial matters. Regulations on private international law issues such as choice of court, choice of law, and mutual legal assistance provide a basis for the effective handling of cross-border cases. However, these measures often lack specific provisions tailored to IP rights, in particular for online copyright infringement. To fill these gaps, expert groups such as the European Max

Planck Group on Conflict of Laws in Intellectual Property Principles have drafted proposals for rules targeted at such scenarios (Bulayenko et al., 2022, p. 22).

In addition, the EU has developed four "European procedures" aimed at speeding up the recovery of outstanding debts. Although not originally intended for IP-related claims, these mechanisms could be adapted to deal with IP enforcement disputes and provide a template for quick and efficient solutions in cross-border contexts (Bulayenko et al., 2022, p. 23).

As can be seen, combating trademark counterfeiting requires robust cross-border cooperation, particularly in combating the misuse of domain names. These domain names often serve as critical access points for counterfeiters to reach consumers in multiple jurisdictions, complicating enforcement efforts.

It is recommended that a cooperative initiative be established among IP enforcement authorities of APEC economies to address trademark counterfeiting through domain names. This initiative would enable enforcement authorities to work together, particularly in cases where action is required against a domain name provider or registrar located in another economy. Such cooperation would facilitate timely and effective responses to domain-related trademark infringement and ensure that enforcement mechanisms can operate seamlessly across jurisdictions.

The initiative could be implemented through a structured, voluntary network of IP enforcement authorities within APEC economies that would act as a conduit for cross-border cooperation. This network would allow authorities to request mutual assistance in domain name infringement cases. For example, an enforcement authority encountering a counterfeiting operation associated with a domain name hosted in another economy could request its counterpart to contact local domain registrars directly, gather jurisdiction-specific evidence, or take steps to suspend or seize the domain name.

A critical component of this initiative would be the targeted seizure of domain names as a strategic measure to disrupt counterfeiting operations. Enforcement authorities could work with domain registrars and organizations such as ICANN to establish streamlined procedures for identifying and taking action against domain names involved in IP-infringing activities. This would include developing criteria for domain names seizures to ensure that actions are based

on clear, consistent standards that respect the diverse legal and procedural norms of APEC economies.

9. *Detection and monitoring tools*

This recommendation focuses on leveraging detection and monitoring tools, including AI-based solutions, as an effective strategy to combat trademark counterfeiting in online environments. These tools enable all interested stakeholders within any APEC economy, including IP enforcement authorities and private actors (e.g. digital platforms), early detection of IP rights infringements and real-time monitoring, allowing them to act immediately.

A. Monitoring technologies to combat trademark counterfeiting

One of the most effective technological tools in this regard is trademark monitoring software, which uses advanced algorithms and web crawling techniques to scan the internet for instances of trademark infringement, counterfeiting and unauthorized use of trademark assets. These tools enable trademark owners to proactively identify and address potential threats, minimizing the impact of online trademark abuse on their reputation and revenue (Thio, 2024, p. 715).

It is undeniable that a company's trademarks can be among its most valuable assets, and trademark owners must be proactive in protecting them. Trademark registration is an important first step. However, trademark protection should not end there, as it is recommended that trademark owners implement a protection strategy that includes a plan to continuously monitor the marketplace for trademark infringement or misuse (Love and Lange, 2024).

Among some relevant examples of the benefits resulting from monitoring software we can point out the following. Trademark monitoring keeps a constant pulse on the trademark reputation, allowing the IP owner to identify shifts regarding trademark sentiment and act quickly. If trademark monitoring tools indicate that consumers are having negative perceptions about a specific trademark, the IP owner can address the situation in real time rather than reacting when it is too late (Quantilope, 2024).

B. AI tools to enhance the digital trademark monitoring

The integration of advanced detection and monitoring tools powered by AI is a transformative step in the fight against trademark counterfeiting in the digital environment. By harnessing AI's ability to process and analyze large amounts of data, APEC economies can strengthen their ability to detect and respond to IP rights infringements in real time.

Automated systems can flag suspicious activity, such as counterfeit product listings or phishing attempts, with greater efficiency than manual processes. This proactive approach enables stakeholders to act quickly, reducing the risk of reputational damage and protecting consumer confidence (Thio, 2024, p. 716).

To address the double-edged nature of AI, which can be used for both IP protection and infringement, the recommendation emphasizes the promotion of AI development with built-in ethical guidelines and controls to minimize misuse. Governments must prioritize updating their legal frameworks to address sophisticated forms of AI-enabled infringement, including technologies such as deepfakes, while encouraging innovation. Balancing enforcement with technological advancement will ensure that AI remains a force for good, enhancing IP protection without stifling creativity (Arampatzis, 2023).

By embedding AI tools into domestic and regional enforcement strategies, APEC economies can create a unified response to digital counterfeiting. Collaboration, supported by shared AI-enabled detection platforms, will ensure consistent standards of protection and make it harder for counterfeiters to exploit jurisdictional gaps. This holistic approach will ensure that AI does not just serve as a reactive tool but becomes a cornerstone of proactive IP defense strategies in the digital ecosystem (Arampatzis, 2023).

C. Some application examples

Several cutting-edge tools exemplify the application of AI-powered detection and monitoring systems in the fight against trademark counterfeiting. One prominent solution is Clarivate's suite of monitoring software, which offers a range of specialized services to protect trademarks and trademark integrity across digital platforms:

- Trademark Watch enables businesses to proactively safeguard their trademarks by monitoring potential infringements of both word and design marks. Timely reports empower trademark owners to take swift legal or administrative actions against unauthorized usage, ensuring trademark protection remains robust on a global scale (Clarivate, 2022).
- Domain Name Watch focuses on identifying "copycat" domains that mimic established trademarks, including ccTLDs and misspelled variants (domain typosquatting). This tool ensures that counterfeiters cannot exploit similar domain names

to mislead consumers or harm company reputation (Clarivate, 2022).

- Web Watch offers actionable insights into instances of online trademark misuse, including unauthorized mentions or derogatory content. By highlighting potential risks and providing comprehensive data on abuse, this tool allows businesses to mitigate threats and uphold their brand image effectively (Clarivate, 2022).

Monitoring software and AI are both part of the technological innovation wave that digital spaces offer, in which, to combat the trademark counterfeiting in online environments, should both be used. They offer a very much better overall performance when compared with human resources, thus being the alternative for automating many processes and systems still being controlled and monitored by people. Its use (and application in law enforcement as well) should be considered and recommended by APEC economies.

Another case to review is Alibaba's use of their advanced AI and machine learning technologies to enhance digital enforcement against trademark counterfeiting on its platform. These tools include image recognition, text analysis, and behavioral monitoring to detect counterfeit products and suspicious seller activities. Real-time monitoring systems enable swift removal of infringing listings, preventing harm to consumers and trademark owners while increasing the efficiency and scalability of anti-counterfeiting efforts.

Additionally, Alibaba's Automated Content Recognition (ACR) technology proactively filters suspected counterfeit listings by analyzing seller details, item presentation, and payment data in real time. The platform collaborates with trademark owners to customize ACR detection models, targeting trademark infringements and unauthorized trademark use. This partnership ensures precise and adaptable filtering, withholding flagged items from publication until their authenticity is confirmed.

D. Japan Patent Office experience and challenges for implementation

The Japan Patent Office's (JPO) study on the use of AI in anti-counterfeiting, completed in FY2023, sheds light on both the potential and current challenges of using AI technology to combat the growing problem of counterfeit goods in the digital marketplace. AI-based anti-counterfeiting tools have become increasingly prevalent, particularly among major e-commerce platforms, which use these services to monitor and combat the proliferation of counterfeit goods. However, the widespread adoption of this kind of tool has been delayed

in some cases by some important challenges (Japan Patent Office, 2024).

The study conducted by the JPO aimed to address these barriers by providing updated insights into the state of AI in anti-counterfeiting, as well as the specific needs of companies, particularly Japanese companies, when it comes to AI-based solutions. One of the key objectives was to identify the main barriers to implementing effective anti-counterfeiting measures using AI, and how these could be mitigated. Among the key challenges outlined in the study were the technical and non-technical issues preventing the widespread use of AI. For example, the difficulty of collecting clean, reliable data from infringing websites remains a significant hurdle. As counterfeiting is often carried out using sophisticated and evolving methods, some AI tools may struggle to detect these infringing products without access to high-quality data that can accurately represent counterfeiting activity.

In addition, the cost of AI-based services is another barrier to their adoption, particularly for smaller businesses or economies with limited resources. These advanced anti-counterfeiting tools can be expensive to implement, making them less accessible to small and medium-sized enterprises, which are often the most vulnerable to counterfeiting. In many cases, these companies may also lack the necessary awareness of the importance of investing in anti-counterfeiting technologies, which is essential for creating a market-wide commitment to combating digital trademark counterfeiting (Japan Patent Office, 2024).

Despite these challenges, the study highlights the enormous potential of AI-based anti-counterfeiting solutions. This technology is particularly effective at analyzing product images to assess their authenticity and identifying counterfeiting risks by examining the characteristics and behaviors of sellers. This capability enables AI tools to detect patterns of infringement and prevent counterfeit goods from entering the market.

The JPO study highlighted that with advances in AI technology and improvements in data quality, these tools could become significantly more effective in the fight against digital trademark counterfeiting. Therefore, according to the JPO, by supporting the development and adoption of AI tools, APEC economies could improve their ability to combat trademark counterfeiting and ensure a safer and more trustworthy digital marketplace for consumers and businesses alike (Japan Patent Office, 2024).

E. Highlights from surveys results

Regarding the tools used by different economies to detect and monitor online trademark counterfeiting, the survey of policymakers reveals a range of technological strategies, each ranked according to its perceived effectiveness. Economies such as Hong Kong, China; the Republic of Korea; and the Philippines place a high value on automated web crawlers⁹ and Internet Protocol address trackers¹⁰, which they consider to be highly effective in identifying lists of counterfeits and tracking infringements in real time. In addition, Hong Kong, China uses big data analytics for digital enforcement and its Big Data Analytics System is operated for 24-hour automatic cross-platform cyber patrol and information analysis to combat online IPR infringement. The Republic of Korea, in particular, uses a wide range of highly effective tools such as AI image recognition, blockchain for traceability, big data analytics and automated web crawlers. This integrated approach enables a robust and multi-dimensional detection system, demonstrating an advanced technological framework for counterfeit prevention.

In economies such as Japan and the Philippines, AI image recognition and blockchain technology for traceability also play an important role in monitoring, as they are considered highly effective tools. These technologies improve traceability and help distinguish between authentic and counterfeit products through advanced imaging and data tracking capabilities. Japan's use of automated web crawlers and blockchain technology demonstrates its commitment to adopting innovative tools to strengthen IP protection. Similarly, the Philippines has adopted big data analytics alongside these technologies to enable a more comprehensive approach to tracking and analyzing patterns of counterfeiting activity across all platforms.

Economies such as Chile and Peru use more selective approaches. Chile uses moderately effective case-by-case social analysis with a focus on manual monitoring, while Peru relies on direct monitoring of listings on platforms by its Digital Enforcement Team within the Technical Secretariat of the Distinctive Signs Commission. These methods reflect a more focused and practical approach to counterfeit detection, although they may lack the scalability offered by automated technologies. Chinese Taipei uses AI

⁹ A web crawler is a program that automatically navigates the internet, systematically indexing web pages for search engines by following links and parsing HTML to extract relevant data while adhering to rules specified by website owners.

¹⁰ An IP tracker is a digital tool designed to identify and trace the geographic location and other attributes of an IP address. This technology is employed for various purposes, such as enhancing online security, optimizing content delivery, and analyzing web traffic patterns.

image recognition and IP trackers with moderate effectiveness as part of its detection toolkit, highlighting its commitment to using data-driven tools despite having fewer resources compared to other economies.

To enhance the ability of APEC economies to combat trademark counterfeiting in the digital environment, it is recommended to create a shared AI-ready database. This centralized resource would serve as both an informational and operational tool to facilitate the adoption and use of AI-based technologies for detecting and monitoring counterfeiting activities. The key objectives of this initiative are as follows:

Informational Resource:

- Provide access to a source with comprehensive and up-to-date information about existing AI-based tools and technologies for combating counterfeiting.
- Include details such as the tool's name, description, functionalities, implementation case studies, and the economy or stakeholder utilizing the tool.

Supporting Technology Adoption:

- Act as a repository of data to enhance the development and improvement of AI-based systems, including information on trademarks, known cases of counterfeiting, and infringement patterns.
- Provide tiered access to the database, with baseline data available to all economies and additional features accessible through partnerships or technical assistance programs.

The database would include:

- *Technology profiles:*
 - Comprehensive information on AI-based tools, such as detection and monitoring software, blockchain applications, and watermarking technologies.
 - Descriptions of how these tools function and examples of their successful implementation in different economies.
- *Data for AI development:*
 - Aggregated data on known cases of counterfeiting, trademarks, and patterns of infringement contributed by trademark owners, enforcement authorities, and digital platforms.
 - This data would support the customization and improvement of AI systems.

Regarding the implementation of a shared database:

- *Design and Development:*
 - The relevant stakeholders (e.g. IP enforcement authorities, digital platforms, etc.) interested in using AI tools to leverage detection and monitoring capabilities could establish work together to define the database's structure, scope, and governance model.
 - Ensure the database complies with data protection regulations and respects the confidentiality of sensitive information.
- *Launch and Pilot Phase:*
 - Begin with a pilot version of the database, including a limited number of tools and data sets, to test its usability and relevance.
 - Invite economies selected by their expertise and experience with these tools to participate in the pilot and provide feedback for refinement.
- *Regional Rollout and Maintenance:*
 - Expand the database to include contributions from all APEC economies interested including public as well as private stakeholders.
 - Regularly update the database to incorporate new tools, technologies, and training opportunities.

Finally, the expected benefits of this recommendation will be the following:

- *Enhanced Awareness:* keep APEC economies informed of cutting-edge technologies and practices for combating counterfeiting.
- *Improved Enforcement Capabilities:* support economies in adopting and tailoring AI-based tools to meet their specific enforcement needs, leading to more effective IP protection across the region.
- *Capacity Building:* offer opportunities for economies with limited resources to access training and technical support, reducing disparities in enforcement capabilities.

10. *Tracking and IP protection technologies*

Technological advances have revolutionized the tools available to track and protect IP online, providing trademark owners with innovative solutions to combat infringement and counterfeiting in the digital environment. These technologies not only enhance the ability to alert any unauthorized uses but also increase the possibilities of strengthening the enforcement efforts against infringers. It must be noted that even if the main users of these tools are the trademark owners, its extended application would imply positive effects for all interested stakeholders within any APEC economy in the combat against trademark counterfeiting in online environments (e.g. IP enforcement authorities or digital platforms).

A. Protection through watermarking tools

One such tool is digital watermarking and fingerprinting technology, which embeds unique identifiers into digital assets such as images, videos and documents. These identifiers allow trademark owners to track unauthorized distribution and use of their content on the Internet. In addition to deterring potential infringers, these technologies generate valuable evidence that can be used in legal proceedings against infringers, supporting IP enforcement efforts in a highly efficient manner (Thio, 2024, p. 716).

Digital watermarking plays a critical role in protecting IP in the digital ecosystem. Similar to traditional paper watermarks, which were historically used to certify the composition of paper or to record a manufacturer's trademark (Shaw, 1999, p. 4), digital watermarks are embedded in digital assets—such as images, videos, text or sound—and enable content creators and trademark owners to assert ownership and protect their IP rights in the digital domain.

The process of digital watermarking involves combining clear input data (the cover object) with the watermark or fingerprint (the embedded object) to create a “stego” object that carries the hidden information.¹¹ This process can be secured with a secret key known only to the data owner or shared with an agent (e.g. a detector function) and is critical to the recovery of the watermark or fingerprint (Shaw, 1999, p. 5). The key feature of digital

¹¹A “stego” object is the result of embedding hidden information, such as a watermark or fingerprint, into a clear input data, known as the cover object. This integrated object, called the stego object, carries the concealed data in a manner that is typically imperceptible to users.

watermarking is that it enables unique identification of content ownership and protection of IP across digital platforms.

Unlike general watermarking, fingerprinting embeds a unique identifier for each customer who purchases the content. This function acts as a hidden serial number, allowing the content owner to trace and identify the specific customer responsible for distributing the content to unauthorized third parties. This technique is extremely valuable in the detection and prosecution of IP infringement (Shaw, 1999, p. 5).

A notable innovation in the field of digital watermarking is the "patchwork" algorithm developed by researchers at the Massachusetts Institute of Technology Media Lab. This algorithm increases the variance in luminance of selected pixel pairs within an image, creating a watermark that is difficult to remove without the proper key. While this method has certain vulnerabilities —such as susceptibility to transformations such as cropping— it provides a robust approach to asserting content ownership without easy removal, making it an important tool for protecting online content (Shaw, 1999, p. 6).

For trademark owners, watermarking tools also play a critical role in combating counterfeiting. By embedding invisible but detectable watermarks in product images and digital versions of their trademarks used in digital advertisements or e-commerce listings, trademark owners can identify unauthorized sellers using these images to promote counterfeit goods. This approach not only helps in tracing the origin of counterfeit content but also facilitates swift takedown actions on online platforms.

B. Protection through blockchain tools

Another innovative solution, and more contemporary, is blockchain technology, which provides a decentralized and tamper-proof system for recording transactions and verifying the authenticity of digital and physical products. For online trademark protection, blockchain can create immutable records of ownership and ensure product authenticity, making it a powerful tool in the fight against counterfeiting. Blockchain platforms enable transparent supply chain management and provide consumers with verifiable proof of a product's origin, building trust and strengthening trademark reputation in the marketplace (Thio, 2024, p. 716).

Blockchain is rapidly gaining attention for its potential to protect IP rights and address

challenges related to traceability and verification in the online environment. This emerging technology provides a secure, transparent and tamper-proof system for recording transactions, ensuring that data and IP-related activities can be tracked, audited, and verified without the possibility of manipulation. Its decentralized nature enhances trust, making it an invaluable tool for establishing the authenticity and ownership of digital assets, particularly in online environments where counterfeiting and IP theft are prevalent (Lin et al., 2020, p. 283).

In conjunction with other emerging technologies, such as the Internet of things (IoT) systems and devices, it enables the automatic exchange of data without the need for human intervention, creating an interconnected ecosystem that is particularly useful for tracking the movement of physical and digital assets. In this way, blockchain-based solutions can provide real-time protection and authentication of product trademarks, ensuring their traceability from origin to end user and preventing counterfeit goods from entering the market (Lin et al., 2020, p. 283).

A notable example of the application of these technologies is the "Maker-IP" platform developed in China by the Intellectual Property Publishing House in collaboration with various government agencies. This platform provides a unique method of IP protection through a combination of real-time evidence preservation and digital certification. "Maker-IP" platform allows users to upload unregistered trademarks and trade names and certify their use prior to official registration. The platform records and authenticates these trademarks and trade names, providing irrefutable evidence of ownership and use, which can be crucial in the event of infringement (Lin et al., 2020, p. 284).

By combining blockchain with IoT, "Maker-IP" platform increases the credibility of the data stored. The tamper-proof nature of blockchain ensures that all records are secure and cannot be altered after certification, while IoT capabilities can facilitate automated processes for verifying and inspecting the authenticity of goods. This system reduces human error and the potential for deliberate tampering, allowing businesses to verify the provenance of their products and IP, and differentiate between genuine and counterfeit goods. This integration of blockchain and IoT could significantly improve IP enforcement and create a more transparent, efficient, and reliable system for tracking digital and physical assets throughout their lifecycle (Lin et al., 2020, p. 286).

This recommendation seeks to empower trademark owners to lead the adoption of blockchain

and digital watermarking technologies, improving traceability, authentication, and enforcement against trademark counterfeiting in online and offline environments.

Identifying Vulnerabilities: trademark owners should first assess which products or trademarks are most at risk of counterfeiting within the APEC economies where they operate.

Engaging Digital Platforms: once vulnerabilities are identified, trademark owners can independently engage with relevant digital platforms (e.g., e-commerce marketplaces, social media networks) to explore integrating these technologies into their systems.

Defining Technical Criteria: trademark owners should establish working groups to define minimum technical standards for blockchain or digital watermarking infrastructure, tailored to improve traceability and authentication throughout the supply chain.

This recommendation encourages trademark owners to lead the adoption of blockchain and digital watermarking technologies to enhance traceability, authentication, and enforcement against counterfeiting in both online and offline environments.

CASES OF STUDY

1. *Aura Blockchain*

A. Challenge

The primary challenge addressed in this case study revolves around emerging technologies and technological barriers to IP protection in the luxury goods market. The global rise of e-commerce and digital platforms has significantly increased the risk of trademark counterfeiting, as counterfeiters exploit the anonymity and vast reach of the digital environment to distribute counterfeit goods. This problem is compounded by the complexity of monitoring and enforcing IP rights in a fragmented and decentralized online marketplace, where traditional methods of verification and enforcement struggle to keep pace. Companies face significant hurdles in tracing the origin of counterfeit goods and ensuring the authenticity of their products throughout the supply chain, undermining consumer confidence and causing significant economic loss.

A secondary but related challenge is the interaction between public authorities and private stakeholders. Fighting counterfeiting in the digital environment requires cooperation between stakeholders, including luxury companies, e-commerce platforms, consumers, and regulators. However, different legal frameworks and enforcement standards across jurisdictions often hinder coordinated action, leaving gaps that counterfeiters exploit. Luxury companies also face the burden of developing private mechanisms to protect their IP in the absence of comprehensive public sector solutions, creating a need for innovative, scalable, and collaborative approaches that bridge the gap between private initiatives and public enforcement efforts.

B. Problem under study

The traditional IP framework, designed to protect innovation and creative works, is based on a system of patents, trademarks, copyrights and trade secrets. Each element serves different purposes, such as protecting inventions, identifying the origin of goods or services, securing creative output, and preserving valuable business data. While this system is robust in theory, it presents significant challenges when applied to the modern, borderless environment of e-commerce (Potluri et al., 2023, p. 2).

The decentralized and expansive nature of e-commerce platforms exacerbates these difficulties, as counterfeit goods can be distributed across multiple jurisdictions, rendering traditional IP protections less effective (Potluri et al., 2023, p. 2).

Enforcement mechanisms within the current system also have significant drawbacks. Detecting and dealing with IP rights infringements, particularly in the digital sphere, is often time-consuming and resource-intensive. Litigation remains the primary enforcement tool, but the time-consuming nature of legal proceedings and the lack of short-term solutions often discourage proactive measures. These challenges are compounded by the reliance on centralized authorities to maintain records and resolve disputes, which can lead to a lack of transparency and, in some cases, manipulation of the process. Taken together, these factors hinder the effectiveness of the traditional IP system in combating trademark counterfeiting in e-commerce (Potluri et al., 2023, p. 2).

Despite the potential of technological solutions such as blockchain to improve IP management, they are not stand-alone remedies. Blockchain-based tools can provide additional layers of transparency and traceability, but they need to work in tandem with existing legal frameworks. Their integration faces regulatory challenges and requires further development to meet the nuanced needs of IP enforcement. As such, the limitations of the traditional IP system remain a critical obstacle, particularly for the e-commerce sector, which continues to grapple with the pervasive problem of trademark counterfeiting (Potluri et al., 2023, p. 2).

C. Main actors involved

The issue of trademark counterfeiting in e-commerce involves a complex network of actors, each playing distinct roles that contribute to the problem's persistence and complexity. Public authorities, such as IP offices, customs agencies, and law enforcement bodies, are tasked with monitoring, regulating, and enforcing IP rights. However, their efforts are often hampered by resource limitations, jurisdictional constraints, and the fast-paced nature of online transactions. On the private side, e-commerce platforms serve as intermediaries that facilitate the sale of goods, but their varying levels of commitment to IP enforcement can either mitigate or exacerbate counterfeiting issues.

These platforms often rely on automated systems to detect counterfeit listings, yet such measures are not always effective without active collaboration with IP right holders. They themselves are central to this ecosystem, bearing the burden of identifying infringements and

initiating enforcement actions, a task that can be both resource-intensive and technically demanding. Finally, consumers, though often unwitting participants, play a crucial role as their demand for lower-cost alternatives fuels counterfeit markets. The interplay among these actors underscores the necessity for coordinated efforts and shared responsibility to address the challenges posed by trademark counterfeiting in the digital realm.

D. Solution studied

To address the challenges of trademark counterfeiting in e-commerce, blockchain technology offers an innovative and effective solution through its unique attributes of transparency, immutability and decentralized data management. Blockchain's decentralized ledger enables the creation of tamper-proof records that ensure the integrity of IP ownership, transaction data and authentication processes. By embedding digital watermarks with owner information into blockchain records, it becomes possible to establish verifiable ownership while preserving the original state of the asset. This combined approach minimizes reliance on centralized authorities and reduces vulnerabilities associated with single points of failure (Bhadauria, Kumar, and Mohanty, 2021, p. 1).

Smart contracts, a key feature of blockchain, automate IP management by embedding predefined rules that enforce ownership, track asset transactions and ensure fair compensation for creators. These contracts eliminate intermediaries, making the enforcement process more efficient and reducing the cost and complexity associated with traditional IP enforcement. In addition, blockchain's ability to maintain a complete, immutable history of asset ownership allows stakeholders to verify the provenance and authenticity of products, significantly curbing counterfeiting activity. This is particularly impactful in the e-commerce sector, where the digital environment enables the rapid and widespread distribution of counterfeit goods (Potluri et al., 2023, p. 1).

The efficiency of blockchain solutions is further enhanced by consensus algorithms, such as Proof-of-Authority (PoA), which facilitate the rapid validation of transactions with minimal computational resources. PoA relies on a set of trusted validators to ensure fast and reliable operations within private or consortium blockchains tailored for e-commerce applications. This approach not only reduces operational costs but also ensures scalability, making it suitable for high-volume digital marketplaces (Islam, Merlec, and Hoh, 2022, p. 328).

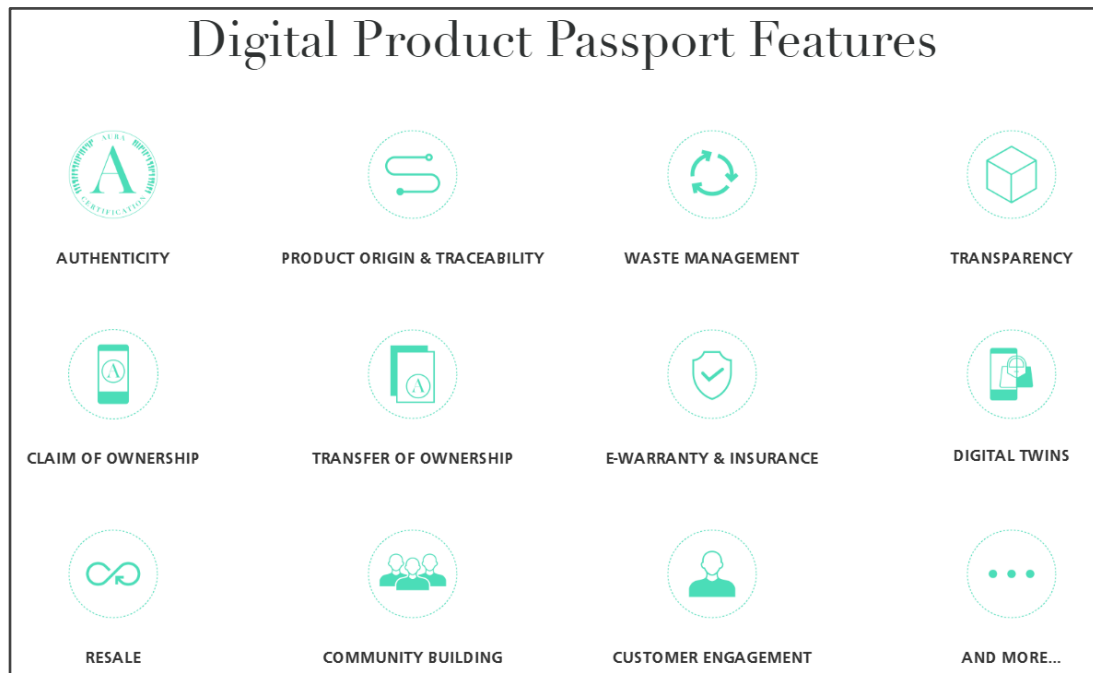
The integration of blockchain and digital watermarking creates a robust anti-counterfeiting system by combining traceability with cryptographic security. This dual approach allows IP owners to securely embed and track ownership data, while preventing unauthorized changes. The immutability of blockchain records also supports the transfer of ownership by providing a transparent, verifiable history of transactions. As a result, IP owners gain a reliable mechanism to protect their assets, while e-commerce consumers benefit from increased confidence in the authenticity of purchased goods (Bhadauria, Kumar, and Mohanty, 2021, p. 2).

- *Aura Blockchain as a solution:*

The Aura Blockchain Consortium is an example of how blockchain technology can be used strategically to combat trademark counterfeiting and improve the authenticity and traceability of goods in the luxury market. Founded in 2021 by leading luxury trademarks Prada, Louis Vuitton and Richemont, Aura operates as a not-for-profit platform offering a secure and transparent blockchain solution. Its main objective is to protect trademark value, prevent counterfeiting and increase consumer trust by certifying the authenticity, origin and sustainability of luxury products. The Consortium's blockchain platform uses a multinodal private blockchain technology, protected by ConsenSys and Microsoft, to ensure the integrity of product data. Each recorded transaction generates a certificate that verifies the authenticity of the product to the end consumer (Cedrola, Kulaga, and Pomi, 2024, pp. 41-42).

By providing transparency throughout the product lifecycle, Aura addresses critical challenges in the luxury sector. The platform helps verify the authenticity of products, ensures responsible sourcing of raw materials and supports sustainability initiatives. These capabilities not only enhance the customer experience, but also deter counterfeiting by guaranteeing the originality and provenance of goods. Aura's blockchain technology also enables trademark owners to monitor distribution channels and ensure that only authorized sellers handle their products, increasing the likelihood of identifying counterfeit items. Trademarks such as Bulgari, Cartier, Hublot, Louis Vuitton, and Prada are already using the system, with more names expected to join (Cedrola, Kulaga and Pomi, 2024, p. 42).

Image N° 6



Source: Aura Blockchain Consortium, Solutions

The Digital Product Passport is one of the main services offered by Aura. This service aims to provide a full lifecycle traceability system, ensuring transparency and authenticity from origin to end-of-life, as illustrated in the previous image. With this service, Aura creates comprehensive digital identities for products, enriching customer loyalty through e-warranty or loyalty programs.

- *Implemented tools*

Such technology provides a decentralized ledger system designed to enhance the authenticity, transparency, and traceability of luxury goods throughout their lifecycle. By assigning a unique digital identifier to each product, which is securely stored on the blockchain, the system allows providers and consumers to verify authenticity at every stage of the product's journey. The platform also tracks the entire supply chain, documenting every step from manufacture to sale, increasing accountability and providing valuable insights into sourcing and production practices. Aura Software as a Service (SaaS) further simplifies adoption by offering Application Programming Interface (API) integrations, allowing companies to seamlessly connect blockchain to their existing information technology (IT) systems (World Law Group, 2023).

In addition to its technological capabilities, the Aura Blockchain Consortium has prioritized the protection of its own IP to ensure the integrity of its system. This has included filing trademark applications for the "Aura" trademark in various categories, such as software and advertising services, to prevent unauthorized use of its platform and name. By securing these trademarks early, the Consortium is strengthening its strategic position in the luxury goods market and setting a precedent for proactive IP management in the digital realm (World Law Group, 2023).

The blockchain system offers significant IP enforcement benefits in the fight against trademark counterfeiting and unauthorized use of luxury trademarks. For example, the platform's authentication capabilities allow for the rapid identification of counterfeit goods, while its transparent and immutable records increase consumer trust by providing verifiable information on product provenance. In addition, the detailed data recorded on the blockchain can serve as solid legal evidence in cases of trademark infringement or counterfeiting disputes, helping companies to protect their rights. The collaborative structure of the Consortium also enables participating companies to work together, creating a unified approach to IP protection and raising industry standards for anti-counterfeiting (World Law Group, 2023).

- *Aura SaaS*

Aura has advanced its technological offerings with the development of a SaaS tool in 2022. This innovation simplifies the implementation of blockchain functions, making it easier for companies to use authenticity assurance, ownership tracking and transparency tools. The SaaS tool expands accessibility for new entrants, reinforcing the platform's position as a comprehensive solution to the challenges of trademark counterfeiting in the digital ecosystem (Cedrola, Kulaga, and Pomi, 2024, p. 43).

According to Aura, the introduction of this service marks a significant step in the application of blockchain technology to the operational needs of luxury companies, addressing issues such as trademark counterfeiting and supply chain traceability. The platform facilitates the integration of blockchain into areas such as supply chain management, customer service, sustainability and legal processes. By providing tools for both upstream applications (e.g. raw material sourcing) and downstream applications (e.g. digital certificates of authenticity) it offers companies a mechanism to increase

transparency and ensure traceability throughout the product lifecycle (Aura Blockchain Consortium, 2022, p. 1).

Aura SaaS is designed as a no-code solution to simplify implementation and reduce costs. Firms can connect directly to the Aura blockchain via APIs and integrate it with their existing IT systems and applications. The system includes features such as smart contract generation, blockchain-based product registration, and tools for managing product history and ownership changes. These capabilities enable companies to document and verify product authenticity and ownership, while streamlining processes such as warranty management and ownership transfers. These tools address the challenges of counterfeiting and increase trust in the supply chain (Aura Blockchain Consortium, 2022, p. 1).

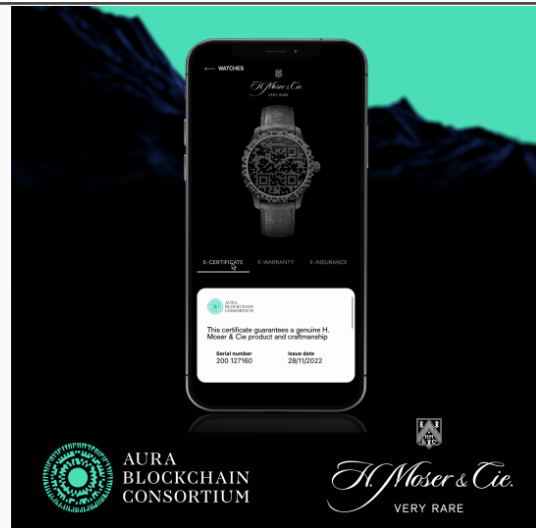
In addition, Aura SaaS includes customizable interfaces that align with each company's visual identity and user experience. These interfaces make blockchain functionality accessible without requiring specialized technical knowledge, allowing end consumers to access information such as product authentication certificates, ownership history and sourcing details. This approach supports transparency and strengthens the connection between producers and consumers by providing verifiable product information in an accessible format (Aura Blockchain Consortium, 2022, p. 1).

By focusing on key aspects such as authenticity, ownership verification and traceability, Aura SaaS provides a practical framework for addressing systemic issues in the luxury sector. At the same time, its design lowers barriers to entry for companies and expands the capacity for blockchain adoption globally (Aura Blockchain Consortium, 2022, p. 1).

Image N° 7

H.Moser & Cie. Project Genesis

Through Aura SaaS, this project offers blockchain watch authentication for enhanced multi-level security and transparency, which includes an e-warranty and e-insurance services. As the watch is logged on to our permission-based blockchain, customers can then use the H. Moser & Cie. app to access the enriched details, such as the technology used, the warranty expiry date and full traceability on the watch's insurance that has been embedded to the products in this collection.



Source: Aura Blockchain Consortium, Solutions

As the previous image illustrates, the SaaS offered by Aura provides blockchain-based authentication for enhanced multi-level security and transparency. This includes integrated e-certification and e-traceability services. Once a product is registered on the permission-based blockchain, users can access its enriched details through a dedicated app.

Through these initiatives, Aura Blockchain demonstrates how collaboration among stakeholders and the integration of advanced technologies can drive significant progress in protecting IP rights and fostering consumer trust in e-commerce markets.

2. Collaboration through INTA To Go

A. Challenge

The challenge in this case study is primarily related to emerging technologies and technological barriers, as well as the cooperation among private actors. The digital transformation of commerce has created a vast and interconnected ecosystem in which counterfeiters use e-commerce platforms and social media to misuse trademarks, often bypassing traditional enforcement mechanisms.

Trademark owners often lack the specialized training and technical expertise to identify and address these unauthorized uses, leaving them vulnerable to the proliferation of counterfeit goods and unauthorized product listings. The speed and scale with which counterfeit products can spread online exacerbates this problem, making it difficult for trademark owners to respond effectively and protect their IP rights (Tursunov, 2024, p. 41).

This case also addresses the limited collaboration among the parties interested in dealing with this growing problem. While some digital platforms have implemented measures to combat trademark counterfeiting, the enforcement landscape remains fragmented, with inconsistent policies and inadequate resources allocated for oversight. This lack of coordination undermines the ability to implement comprehensive strategies, forcing trademark owners to navigate a complex web of platform-specific procedures without robust support from regulatory frameworks or public enforcement mechanisms. As a result, the responsibility for monitoring and protecting IP often falls primarily on private actors. While this reflects the private nature of IP rights, it also highlights the challenges these actors face, as they may lack the tools or capacity to address the issue independently. Cooperation by the public sector, although sometimes limited by resource constraints or lack of expertise, remains an essential complement to private efforts to achieve effective enforcement (Tursunov, 2024, p. 41).

B. Problem under study

A major issue is the territorial nature of trademark rights, which complicates efforts to secure protection across multiple jurisdictions. Navigating these complexities becomes even more burdensome in the digital environment, where trademarks can be easily abused across multiple platforms such as marketplaces, social networks, and search engines. For IP owners without adequate training in these digital landscapes, the situation can be overwhelming,

increasing the likelihood of undetected infringement and weakening trademark protection (Tursunov, 2024, p. 41).

Consumers also face significant consequences from trademark counterfeiting in digital environments. Online platforms often blur the distinction between genuine and counterfeit products, leading to consumer confusion and reduced trust in trademark authenticity. The increasing reliance on digital influencers, online reviews and marketplace endorsements has further shaped consumer behavior, making them vulnerable to deceptive practices. Counterfeit goods and unauthorized listings can mislead consumers into purchasing inferior or even harmful products, damaging the companies' reputation and eroding consumer trust in legitimate businesses. This highlights the wider implications of trademark counterfeiting, not only for businesses seeking to protect their IP, but also for the trust and safety of consumers navigating the digital marketplace (Tursunov, 2024, pp. 41-42).

C. Main actors involved

Key stakeholders include trademark owners, digital platforms (such as marketplaces and social networks), regulators, and consumers. Trademark owners play a critical role in monitoring and combating infringements, but their efforts are often hampered by limited resources and expertise. Digital platforms act as both enablers and regulators of counterfeiting activities, as they provide the space in which counterfeiting takes place, but also have the power to enforce anti-counterfeiting measures. Regulators face the challenge of bridging gaps in enforcement, while consumers inadvertently become participants in the counterfeiting ecosystem by purchasing counterfeit goods. The following interactions across key stakeholders underscore the interconnected nature of the problem and the need for collaborative solutions (Tursunov, 2024, p. 43):

- Trademark owners: Are subjects at the forefront of the fight against trademark counterfeiting and its unauthorized use. However, many of these owners lack the training and resources to effectively monitor and protect their trademarks across multiple digital platforms. Nevertheless, trademark owners do not always respond to notifications of suspected online infringement issued by IP enforcement authorities, which often results in a lack of action based on such notifications. This inaction further complicates efforts to combat counterfeiting in the digital space.
- Digital platforms: Marketplaces, social media networks, and search engines play a

crucial role in the contention or spread of counterfeit goods and trademark infringements. Therefore, they usually implement robust measures to detect and prevent the sale of counterfeit products. Social media networks implement policies to monitor and regulate content to prevent trademark misuse. Search engines operate in a similar way to avoid the inadvertent promotion of counterfeit goods and services.

- Consumers: They are significantly affected by the proliferation of counterfeit goods and unauthorized product listings online. The seamless integration of digital content on platforms such as marketplaces and social media makes it increasingly difficult for consumers to distinguish between genuine and counterfeit products.
- IP enforcement agencies: Serve as key regulators and enforcers in the fight against trademark counterfeiting infringement. In addition to developing and implementing policies, they can play a critical role in coordinating enforcement efforts across jurisdictions. These authorities must also invest resources in public education to reduce the demand for counterfeit goods and services. By raising awareness and educating citizens on these issues, IP enforcement authorities can help discourage demand by addressing the root causes of trademark counterfeiting in the digital environment.

C. Solution studied

This issue was identified and studied by INTA, a global non-profit association of trademark owners and professionals. In line with its mission to support trademarks and IP, INTA responded to the growing complexities of trademark protection in the digital ecosystem by developing *INTA To Go*. This is a comprehensive e-learning platform aimed at equipping trademark owners with the skills and knowledge they need to effectively navigate the digital landscape.

This initiative represents a specific measure of collaboration among private actors and digital tools, providing a robust solution to the challenges faced by trademark owners. With an extensive selection of live and on-demand webcasts, INTA To Go serves as a one-stop shop for quality trademark and IP education.

The platform offers a range of learning opportunities, from quick refreshers on the basics to in-depth explorations of current hot topics, featuring insightful conversations with experts and policymakers from around the world. Most webcasts also offer Continuing Legal Education

and Continuing Professional Development credits, adding further value to the learning experience.

For IP right holders, the introduction of INTA To Go has yielded noteworthy advantages. This proactive strategy lessens the frequency of illegal product listings and counterfeit goods while preserving the exclusivity and integrity of their trademarks.

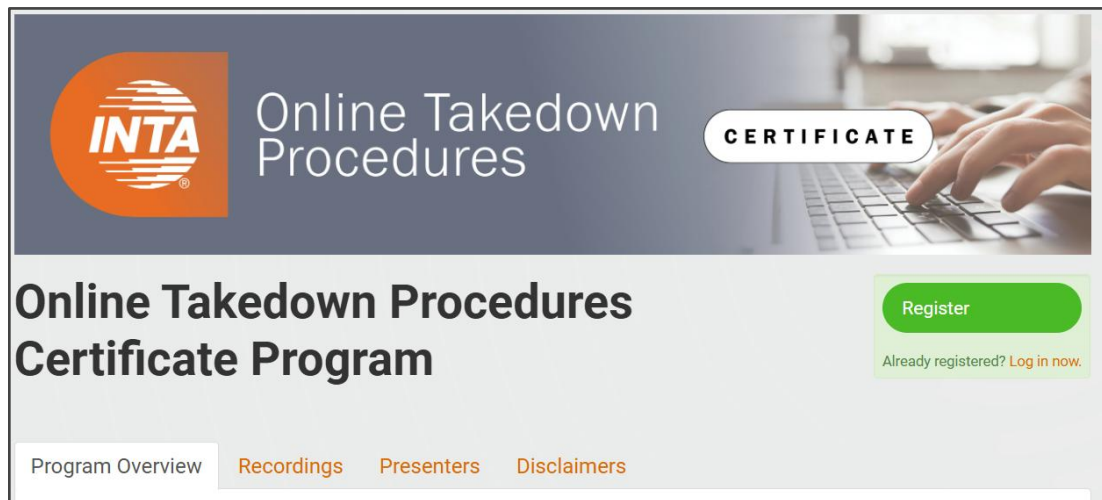
The advantages for e-commerce customers are just as significant. There are fewer fake goods on the Internet as a result of trademark owners' improved capacity to defend their names. Businesses and customers alike gain from the general increase in consumer confidence and trademark legitimacy, which supports a more robust e-commerce environment.

D. INTA e-learning programs

The solution to trademark counterfeiting in the digital environment is a combination of education, training, and strategic online enforcement. INTA's e-learning platform, INTA To Go, offers a wide range of resources, including live and on-demand webcasts, to equip trademark owners with the knowledge they need to effectively protect their IP in the digital ecosystem.

A key initiative is the Online Takedown Procedures Certificate Program, which provides trademark owners and professionals with practical knowledge on how to manage and enforce their rights on major online platforms such as Amazon, Mercado Libre, TikTok, Meta, and Temu. This program helps participants understand the procedures for identifying, reporting and removing counterfeit goods online, thereby improving the digital enforcement of trademark rights.

Image N° 8



Source: INTA, Certificate Programs

- *Understanding Platform-Specific Enforcement Requirements:*

Each online platform has its own set of policies and procedures for enforcing trademarks and removing infringing content. This section details the enforcement requirements for Amazon, Mercado Libre, TikTok Shop, Meta, and Temu. Participants learn how to read and follow these guidelines in order to maximize the success of their takedown requests.

- *Navigating the Notice and Takedown Process:*

The notice and takedown process is an important tool for protecting trademarks and content online. This section of the curriculum walks participants through the step-by-step process of submitting takedown notifications on each platform. It discusses best practices for writing clear and compelling notices, the sorts of evidence required, and the timescales for taking action. Mastering these processes enables participants to respond quickly and effectively to instances of infringement.

- *Identifying Solutions and Resolving Reporting barriers:*

Trademark owners frequently face obstacles and barriers when attempting to protect their rights online. This section discusses frequent challenges such as unresponsive platforms, serial infringers, and jurisdictional difficulties. Participants learn solutions for overcoming these problems, such as how to escalate concerns inside the platform, interact with platform support staff, and use legal remedies as needed.

- *Case studies and practical exercises:*

To reinforce learning, the program includes case studies and practical exercises based on real life scenarios. Participants apply their knowledge to hypothetical situations, analyze the effectiveness of different enforcement strategies, and receive feedback from instructors. These hands-on activities help participants build confidence and competence in managing online takedown procedures.

- *Opportunities for networking and collaboration:*

The program offers participants the opportunity to network with peers and industry experts. Through interactive sessions and group discussions, participants can share experiences, exchange best practices and make valuable connections to support their ongoing efforts in online trademark protection.

According to INTA, by the end of the program participants should be able to show a comprehensive understanding of the tools and techniques needed to protect their trademarks and content across multiple online platforms. Being prepared to tackle the challenges of online enforcement and ensure the integrity of their IP in the digital environment.

In addition, INTA offers the Trademark Administrators (TMA) Certificate Program, which is aimed at early career professionals and new practitioners in the field of IP. This program provides basic knowledge of IP rights, trademark administration, and the technologies used in digital trademark protection, as can be seen in the list of contents of the program described in the next page.

Image N° 9



Source: INTA, Certificate Programs

- *What is IP, the different types of IP and why it is important:*

This section delves into the concept of IP, exploring its various forms such as patents, trademarks, copyrights, and trade secrets. It emphasizes the importance of IP in fostering innovation, protecting creators' rights and promoting economic growth.

- *The role of the trademark administrator in different work environments:*

This chapter examines the diverse responsibilities of TMAs in various industries, including law firms, corporations, and government agencies. It highlights the critical functions that TMAs perform, such as managing trademark portfolios, conducting searches, and ensuring compliance with IP laws.

- *How to obtain IP rights and the benefits of protecting them:*

This section aims to show the processes involved in securing IP rights, including the application and registration procedures for patents, trademarks, and copyrights. The chapter also discusses the strategic benefits of IP protection, such as preventing unauthorized use, enhancing market position, and generating revenue through licensing.

- *The importance of monitoring IP rights, practical tools for monitoring and enforcement strategies:*

This section highlights the need for vigilant IP monitoring to detect and address infringements. It presents practical tools and techniques for effective monitoring, such as trademark watch services and online monitoring tools. It also covers enforcement strategies, including cease and desist letters, litigation, and alternative dispute resolution methods.

- *The main technological tools that TMAs should be familiar with:*

This chapter provides an overview of the key technologies and software that support trademark administration tasks. It includes discussions of trademark management systems, IP databases, and digital tools for conducting searches and managing filings.

- *Types of trademarks, advantages of registration, and how to access and review IP office records:*

Participants explore the various categories of trademarks, such as word marks, design marks, and collective marks. The chapter explains the benefits of trademark registration, including legal protection and trademark recognition. It also guides participants on how to access and analyze records from IP offices to ensure comprehensive trademark management.

- *The necessary skills to be a successful TMA:*

This final chapter focuses on the competencies required to excel in the role of a TMA. It covers essential skills such as attention to detail, legal knowledge, effective communication, and the ability to navigate complex regulatory environments.

Together, the Online Takedown Procedures Certificate Program and the TMA Certificate Program enable collaboration between public and private stakeholders by promoting a common understanding of IP management and enforcement and ensuring that trademark owners can navigate the complexities of the digital environment. These educational initiatives empower trademark owners and professionals to take proactive, informed action against trademark counterfeiting, facilitating effective IP protection in the online space.

Challenges as complex as those posed by trademark counterfeiting in the digital environment require a multi-pronged approach that includes education, digital enforcement, and

collaboration between stakeholders. INTA's INTA To Go platform addresses this need by offering specialized training programs.

Through these initiatives, INTA provides valuable resources to strengthen the capabilities of trademark owners and their respective economies, ensuring that they are well equipped to navigate the complexities of the digital landscape. In addition, by fostering collaboration among stakeholders, these efforts contribute to the broader goal of protecting trademarks and consumers from the negative impacts of counterfeiting. This is an example that APEC economies should not overlook.

This case illustrates how the collaborative approach would not only enhance the capability of trademark owners to protect their IP, but also provide government officials with the skills needed to effectively regulate and enforce IP laws in the digital environment.

3. *Alibaba Anti-Counterfeiting Alliance (AACA)*

A. Challenge

One of the main ways in which counterfeiting has become widespread is through digital e-commerce platforms, also known as marketplaces. Given the volume of transactions involved, these intermediaries need to implement solutions that address the problem on a large scale. Some of the proposed solutions include the implementation of automated tools for the detection and elimination of publications linked to counterfeit trademarks.

On the other hand, other strategies prefer to wait for trademark owners to make claims, which the platforms then process to remove the infringing content. The former has sometimes proven to be inaccurate, while the latter depends largely on the investment that IP owners are willing to make in monitoring and protecting their trademarks.

This example is particularly relevant because the Alibaba Group, through its AACA initiative, proposes to combine the best of both strategies. Thus, thanks to the power of AI, a system has been developed that allows the IP owner to detail the various ways in which counterfeiting may affect him, and to use resources such as image recognition, text analysis, and behavioral analysis, monitored in real time, to detect infringements of his trademark rights.

B. Problem under study

As explained in the background section of this Guidebook, the rise of globalization and the digital economy has dramatically expanded counterfeiting trade, transforming it into a global industry valued at approximately USD 464 billion in 2019, or 2.5% of global trade. Looking ahead, recent research projects that the global trade in counterfeit goods could reach USD 1.79 trillion by 2030, marking a 75% increase from 2023 and growing 3.6 times faster than the global economy over the same period. This underscores the urgent need for enhanced enforcement measures to combat this escalating issue (Cosearch, 2024).

This rampant counterfeiting has far-reaching consequences, including economic losses, reduced tax revenues, job displacement, exploitative labor practices, and the proliferation of dangerous counterfeit products that pose risks to public safety.

Beyond the economic and social toll, consumer behavior plays a key role in perpetuating this illegal industry. In a survey conducted in 17 economies, Alhabash et al. (2023)¹² found that nearly three-quarters of consumers surveyed had purchased counterfeit goods in previous years, more than half had been deceived into buying counterfeits at least once, 50% had purchased deliberately counterfeits over the same period, and 20% were chronic shoppers. These figures demonstrate how consumer demand supports the counterfeit business and exacerbates its detrimental effects (Shepherd, 2023, p. 6).

The rise of e-commerce has exacerbated the problem, allowing counterfeiters to reach a global audience through online marketplaces that connect illicit suppliers with consumers. The e-commerce sector, valued at more than USD 5.7 trillion in 2022 and estimated to grow to USD 8.1 trillion by 2026, provides counterfeiters with unprecedented access to consumers.

Studies suggest that approximately 40% of consumers worldwide have purchased counterfeit goods through online platforms, underscoring the inadequacy of current anti-counterfeiting measures in the digital marketplace. As e-commerce continues to grow, so too will the pressure on online platforms to adopt more effective anti-counterfeiting policies and practices. Without stronger controls, this growth risks further entrenching the counterfeiting industry and increasing its harmful impact on the global economy and society at large (Shepherd, 2023, p. 6).

Counterfeiting within the e-commerce ecosystem involves a wide range of actors, each playing a critical role in either enabling or combating the problem. A key group of actors are the online marketplaces themselves, whose business models, service offerings and target audiences significantly influence their ability to combat trademark counterfeiting.

These marketplaces range from generalist platforms such as Alibaba, Aliexpress, Amazon, and Walmart that offer a wide range of goods and services, to more specialized platforms that cater to niche markets or specific industries. The variability of their business models—whether B2C, B2B or Consumer-to-Consumer (C2C)—determines the scope and complexity of the anti-counterfeiting measures they can implement (Shepherd, 2023, p. 9).

¹² Alhabash, S., Kononova, A., Huddleston, P. Moldagaliyeva, M., and Lee, H. (2023). *Global anti-counterfeiting consumer survey 2023: a 17 economies study*. Center for Anti-Counterfeiting and Product Protection, Michigan State University., held such surveys in 17 economies including Argentina; Australia; Brazil; Canada; People's Republic of China; Egypt; India; Italy; Kenya; Republic of Korea; Mexico; Nigeria; Peru; Spain; United Arab Emirates; United Kingdom; and United States.

Generalist marketplaces face unique challenges because they serve as hubs for a wide range of sellers, from individual entrepreneurs to large corporations, creating a high-volume, high-traffic environment in which counterfeit goods can easily be listed and distributed. Platforms with hybrid structures can combine traditional retail operations with open marketplaces, adding another layer of complexity (Shepherd, 2023, p. 9).

Classified ad marketplaces provide platforms for C2C sales of both new and used goods and services. These platforms differ significantly from generalist marketplaces in that they often operate with limited buyer protection, relying on the "buyer beware" principle. Sellers on these platforms are often transient, making it difficult to establish accountability and implement long-term anti-counterfeiting controls (Shepherd, 2023, p. 10).

Similarly, social media and search engine platforms face similar challenges regarding counterfeit trade due to their massive reach and their own nature of user-generated content. These platforms often act as advertising intermediaries, connecting buyers and sellers either through direct messages or links to external websites. The highly volatile nature of listings, combined with relatively anonymous access for users or limited capabilities for transaction monitoring, makes these platforms a good environment for counterfeiters to exploit (Shepherd, 2023, p. 10).

In contrast, specialist marketplaces that focus on a narrow range of products demonstrate that robust anti-counterfeiting measures, such as product authentication checks and warranties, can be effective. Meanwhile, source integrator marketplaces that support the drop-shipping business model add another layer of complexity. These platforms, which integrate supply across multiple marketplaces, are not always able to verify the authenticity of trademarks or the origin of goods resold through their platforms, sometimes without ever physically handling them, complicating traceability and enforcement efforts (Shepherd, 2023, p. 11).

C. Solution studied

To combat trademark counterfeiting in the digital environment, a combination of collaborative initiatives between private stakeholders and digital enforcement tools has emerged as a practical and effective solution. The AACA demonstrates an effective blend of digital enforcement and collaborative measures to combat trademark counterfeiting in the e-commerce sector. This initiative highlights the role of advanced technology and cooperative action in addressing the pervasive issue of counterfeit products:

- *Digital enforcement through AI*

AACA leverages Alibaba's cutting-edge AI and machine learning capabilities to quickly detect and remove counterfeit listings. AI-powered tools such as image recognition and text analysis help identify subtle differences between genuine and counterfeit products, while behavioral analysis detects suspicious seller activity. Real-time monitoring systems enable proactive responses, ensuring that infringing listings are removed before they harm consumers or companies. This technology-driven approach increases the efficiency and scalability of anti-counterfeiting efforts, creating a safer online marketplace.

- *Digital tools for offline enforcement*

Alibaba's efforts to work with law enforcement and IP owners to protect IP rights and prevent trademark counterfeiting aim to hold all counterfeiters accountable to the fullest extent of the law. In 2022, Alibaba supported 2,123 offline investigations that led to law enforcement raids and arrests, resulting in the arrest of 2,737 criminal suspects. These statistics reflect Alibaba's commitment to fighting counterfeiting offline as vigorously as we do online.

Image N° 10



Source: Alibaba Group. (2022). Annual Report on Intellectual Property Protection

- *ACR in proactive filtering*

ACR technology enables Alibaba to analyze seller information, item presentation details, changes to listings, and payment data. This real-time analysis identifies suspected counterfeit listings and blocks them before they become available to consumers. The system ensures that flagged items are withheld from publication until authenticity is determined, an example of proactive content moderation (Gangjee, 2024, p. 4).

Alibaba enhances its anti-counterfeiting measures by offering trademark specific ACR capabilities. Using its intelligent algorithms, the platform works with trademark owners to customize detection models for individual trademarks. These models target counterfeit goods, trademark infringement and unauthorized use of trademark assets such as stolen images. By leveraging the expertise and insights of trademark owners, Alibaba ensures that ACR filtering is both accurate and adaptable to different management scenarios (Gangjee, 2024, p. 10).

- *Integration with the Queqiao Program*

Launched in 2018, the Queqiao program complements the ACR by using infringement characteristics and product samples provided by companies. Once Queqiao identifies suspected infringements, they are forwarded to right holders for validation. Confirmed infringing listings can then be quickly removed by the right holder with a single click, streamlining enforcement efforts and improving collaboration between Alibaba and trademark owners (Gangjee, 2024, p. 6).

This release allows members of the AACAA to actively adapt and refine algorithms, enabling real-time responses to the dynamic and evolving methods counterfeiters use to advertise and sell counterfeit goods.

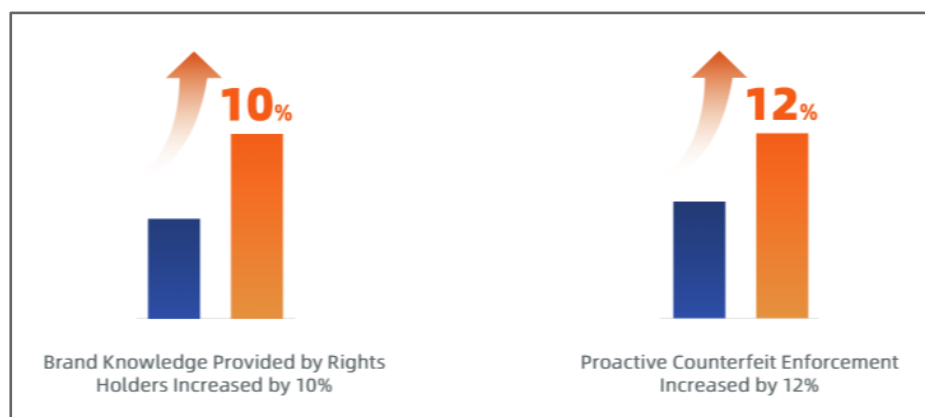
Queqiao 3.0 enables right holders to input infringement knowledge directly into Alibaba's system and interact with the platform in real time. This collaborative approach allows right holders to fine-tune machine learning algorithms specific to their company's needs, ensuring accurate identification of infringing content.

For example, IP right holders can register their trademarks on Alibaba's IP Protection Platform and submit detailed complaints about infringing products or listings. Supporting evidence, such as product descriptions, comparison photos, or other documentation, can also be provided to enhance the system's ability to identify and remove counterfeit

items. This functionality not only streamlines the reporting process but also allows right holders to continuously improve the detection accuracy of infringing content by tailoring machine learning algorithms to their specific needs.

Depending on the context, these algorithms either automatically block listings that are clearly counterfeit or flag them for manual review by right holders. The streamlined interface also allows flagged listings to be removed quickly with a single click, reducing the administrative burden on right holders (Gangjee, 2024, p. 10).

Image N° 11



Source: Alibaba Group. (2022). Annual Report on Intellectual Property Protection

As illustrated by the previous image, in 2022, the Queqiao 3.0 program enhanced collaborative enforcement efforts by enabling right holders to input infringement knowledge directly and interact with Alibaba in real-time. This upgrade led to a 10% increase in trademark infringements identification with the information provided by right holders and a 12% rise in proactive counterfeit enforcement, showcasing Alibaba's improved ability to detect and address infringements through multi-dimensional cooperation and advanced technologies.

- *Infringement categorization*

Registered right holders can define the nature of the IP infringement (e.g., trademark misuse, counterfeit goods) and specify broad categories of misuse that may go beyond formal legal definitions in certain jurisdictions. For example, infringements may be

categorized on the basis of prior judicial or administrative decisions, test purchases, obvious counterfeit features, or even admissions of counterfeiting by the seller.

To support these claims, right holders can upload evidence such as textual descriptions or image comparisons between genuine and counterfeit products. This evidentiary flexibility ensures robust and context-sensitive enforcement of IP rights (Gangjee, 2024, p. 8).

D. Benefits for the main actors of this digital ecosystem

The implementation of solutions, such as AACA, demonstrates how automated tools and collaborative frameworks can bring significant benefits to both IP owners and e-commerce consumers:

- *For IP right owners*

Automated tools such as Queqiao 3.0, combined with comprehensive databases of trademark images, greatly enhance the ability to detect counterfeiting practices. This level of monitoring and enforcement is beyond the ability of most individual IP owners, especially small and medium-sized enterprises, to effectively protect their trademarks. Such measures provide a proactive mechanism to address potential infringements before they cause significant damage, thereby preserving the reputation of the trademark and ensuring consumer confidence (Bumatay, 2015, p. 346).

The benefits also extend to reduced legal and operational burdens. In cases such as Tiffany vs. eBay, courts have reinforced that the primary responsibility for policing trademarks lies with the IP right holder, not the digital platform¹³.

However, platforms that implement robust measures such as "notice and take down" or "notice and action" protocols ensure that they meet the required legal standards. These tools not only enhance compliance, but also provide IP right owners with a streamlined

¹³ In the case of Tiffany (NJ) Inc. v. eBay Inc., No. 08-3947, Tiffany & Co, which was decided by the United States Court of Appeals for the Second Circuit in 2010, Tiffany & Co. accused eBay of facilitating the sale of counterfeit Tiffany goods on its platform. However, the court ruled in favor of eBay, stating that the primary responsibility for policing trademarks lies with the owner of the IP rights (Tiffany), not the digital platform (eBay). eBay was not held liable for trademark infringement as long as it did not have specific knowledge of the counterfeit goods and took reasonable steps to address reports of infringement. This case established that online marketplaces are not primarily responsible for monitoring and preventing trademark infringement on their platforms.

process to address infringements, reducing the need for costly and time-consuming litigation (Bumatay, 2015, p. 347).

- *For e-commerce consumers*

From a consumer perspective, these solutions contribute to a safer and more trusted marketplace. Real-time monitoring and proactive removal of counterfeit goods minimizes the risk of purchasing fake or potentially harmful products. By ensuring that only authentic goods are listed on their platforms, marketplaces like Alibaba foster an environment where consumers can shop with confidence, knowing that their purchases meet safety and quality standards.

- *For digital marketplaces*

Digital platforms also gain significant benefits from implementing these systems. Tools such as automated content detection allow platforms to comply with legal frameworks and invoke safe harbor provisions that protect them from liability as long as they act responsibly when notified of infringements. By enhancing their credibility and complying with legal obligations, platforms ensure their long-term viability and maintain consumer trust as a critical part of their business model (Bumatay, 2015, p. 346).

The AACA demonstrates a comprehensive and collaborative approach to addressing the challenges of trademark counterfeiting in the digital marketplace. By integrating advanced AI tools such as Queqiao 3.0 with customized algorithms and real-time monitoring, Alibaba has set a high standard for proactive and preventive measures against counterfeit listings.

This technological innovation, coupled with active collaboration with right holders, enables both IP owners and the platform to address infringements quickly and efficiently. The combination of automated detection, customized algorithms and streamlined reporting ensures a robust system that not only protects IP but also fosters consumer confidence.

The case also highlights the wider implications of these solutions for the e-commerce ecosystem. By implementing these measures, digital platforms such as Alibaba are not only complying with legal frameworks such as 'notice and action' requirements, but also reducing the operational burden on IP owners while maintaining a safer shopping environment for consumers. This collaborative model demonstrates that technology, coupled with partnerships

between private stakeholders, can create a balanced, effective, and scalable response to counterfeiting, and serves as a benchmark for other online marketplaces around the world.

4. KIPO's Anti-Counterfeit Council

A. Challenge

The challenge in this case revolves around the limitations of traditional public sector regulation and enforcement. The complexity of combating counterfeiting in the digital environment requires not only a robust legal framework, but also effective cooperation between public authorities and private sector actors.

Counterfeiting poses significant risks to consumer safety, undermines the reputation of legitimate businesses and erodes IP rights. The challenge is to create effective public policies and legal frameworks to address this problem, while fostering seamless cooperation between public authorities, private companies, and other stakeholders to maximize enforcement efforts.

Success in tackling this problem will depend on how well these actors can work together to ensure faster detection, enforcement, and consumer protection, bridging gaps in traditional regulatory approaches. In addition, the rise of online platforms and marketplaces creates a dynamic and rapidly evolving environment that adds a layer of complexity to regulatory and enforcement efforts.

B. Problem under study

The low effectiveness of traditional intergovernmental organizations in addressing complex global challenges has led to a shift in governance models, emphasizing the importance of involving private actors in the policy-making process. Often reliant on consensus-based decision-making, intergovernmental organizations have struggled to deliver effective and timely results. This inefficiency has led to a loss of trust and confidence from various sectors, undermining the ability of these organizations to address pressing issues such as trademark counterfeiting and IP protection in the digital landscape (Momen, 2021, p. 3).

In contrast, private actors—including global corporations, civil society organizations (CSOs) and non-governmental organizations (NGOs)—have proven to be more effective in addressing policy issues, contributing valuable resources, expertise and knowledge. These actors are increasingly seen as critical partners in policy design and implementation, particularly in areas where traditional government structures may fall short. By offering bottom-up, collaborative solutions, private organizations help set the agenda for policy discussions

and build consensus among a wide range of stakeholders. This model not only increases the effectiveness of policy solutions, but also supports more agile and responsive action, as seen in efforts to combat counterfeiting on e-commerce platforms (Momen, 2021, p. 3).

In contrast to the top-down approach typically used by intergovernmental organizations, a partnership governance structure encourages collaboration and consensus-building among different actors. This collaborative approach strengthens the capacity of all stakeholders to address societal problems and fosters ownership of the policy process, increasing the likelihood of achieving effective solutions (Momen, 2021, p. 3).

The concept of PPPs is a good example of this shift towards more inclusive governance. While there is no single definition of PPPs, these partnerships generally involve collaboration between public and private sector actors with the aim of achieving long-term, sustainable results. By pooling resources, expertise and skills, PPPs allow both sectors to build on each other's strengths and create solutions that are both innovative and practical.

The benefits of such partnerships are particularly evident in areas such as IP protection, where the combined efforts of government, private and civil society stakeholders can help address complex issues such as counterfeiting in global e-commerce markets (Paun, 2011, p. 8). PPPs can take several forms, each with its own dynamics and contributions to solving public problems.

Collaborative PPPs involve private partners who voluntarily invest significant resources, often without immediate payment, to support public service delivery or policy development. These partnerships can stimulate innovation and mobilize private sector expertise for the public good. Contractual PPPs, on the other hand, are based on formal contracts in which private partners are compensated for their investment in delivering public services or contributing to policy implementation. These contractual arrangements can ensure accountability and efficiency by setting clear terms for the delivery of services (Paun, 2011, p. 7).

Advisory and consulting PPPs focus on the role of private sector actors in providing guidance and expertise to public partners, with advisory PPPs involving unpaid advice, while consulting PPPs typically involve financial compensation for services provided. These models reflect the growing recognition of the critical role of the private sector in policy formulation and implementation, particularly in areas where specialized knowledge is required (Paun, 2011, p. 7).

The most important regarding this case study are PPP networks. This emerged as an extension of these individual partnerships, linking different types of PPPs under a common management structure or larger organizational umbrella. These networks facilitate collaboration across sectors and regions and promote the sharing of best practices and resources.

For example, the Global Alliance for Improved Nutrition and United Nations Development Program's (UNDP) Public-Private Partnership for the Urban Environment are examples of how multiple PPPs can be coordinated to address global challenges such as improving nutrition or managing urban environmental issues. These networks, often orchestrated by international organizations, promote a more integrated approach to solving global problems and demonstrate how different types of PPPs can complement each other in achieving sustainable development goals (Paun, 2011, p. 8).

C. Main actors involved

Looking at this issue, it can be seen that different stakeholders play a critical role in shaping the effectiveness of governance and policy outcomes. Stakeholders can be defined as "individuals or groups with an interest in the success of an organization in fulfilling its mission - delivering intended results and maintaining the viability of its products, services and outcomes over time" (Momen, 2021, p. 4). These actors may include, for example, government agencies, private sector actors and CSOs. Each of these actors brings unique perspectives and resources that influence how policies are designed, implemented, and monitored:

- *Government bodies:* Governments are key drivers in the establishment of PPPs, as they create the policy frameworks that allow these partnerships to flourish. They are responsible for setting the regulatory environment, ensuring that the public interest is protected and holding private partners accountable for their actions. Governments are typically involved in contractual and advisory PPPs, where they either engage private actors to deliver services or rely on external expertise for policy advice (Momen, 2021, p. 4).
- *Private sector actors:* The private sector, including global corporations and other private companies, is crucial in providing the resources, knowledge and expertise needed to address public sector challenges. Their involvement can be seen in contractual and collaborative PPPs, where they may be responsible for the delivery of public services,

contribute to policy development, or offer innovative solutions that improve the efficiency of public services (Momen, 2021, p. 5).

- CSOs: CSOs, including NGOs and community-based organizations, play an important role in advocating for public participation, accountability, and transparency in PPPs. CSOs are particularly influential in consultative PPPs, where they provide unpaid advice and raise awareness of potential policy failures or abuses of power. Their ability to build public opinion and advocate for fair policies makes them key actors in ensuring the long-term success of PPPs (Momen, 2021, p. 5).

The effectiveness of these different actors in shaping PPPs relies on how well they work together and share responsibilities. While it is crucial that stakeholders are adequately represented, it is equally important that the manner in which they are involved fosters cooperation and decision-making that reflects the needs and aspirations of all parties. A lack of balanced representation can lead to dissatisfaction, a lack of public trust, and opposition to PPPs, which can undermine their potential for success (Paun, 2011, p. 22).

D. Solution studied

The Anti-Counterfeiting Council of the KIPO is an example of a successful model of collaborative multi-stakeholder partnerships to combat trademark counterfeiting in the digital space, which is a typical collaboration strategy among public and private stakeholders.

This council, established in May 2014, brings together 96 members, including government agencies, KIPO, trademark owners, and major online platforms, with the aim of addressing the spread of counterfeit goods. The inclusion of international stakeholders, such as foreign trademark owners and service providers, further enhances the global reach and effectiveness of the initiative (KIPO Trademark Police, 2024, p. 1).

Multi-stakeholder participation is essential to address the growing challenges of counterfeiting. Multi-stakeholder refers to a diverse group of individuals, organizations and institutions, such as governments, NGOs, private companies, and local authorities, working together to solve common problems. When stakeholders work together, collective solutions are more effective in addressing complex issues such as counterfeiting (Wai, Nitivattananon, and Kim, 2018).

The primary objective of the Council is to protect consumers from the dangers of counterfeit products, to protect IP rights and to ensure fair competition in the marketplace. The Council fosters a collaborative environment where information about counterfeit goods can be shared quickly among its members.

By facilitating rapid communication and information exchange, stakeholders can take prompt action to remove counterfeit listings and prevent the sale of such goods on e-commerce platforms. This approach not only strengthens the enforcement of trademark rights but also creates a proactive system for detecting and combating counterfeiting across multiple sectors (KIPO Trademark Police, 2024, p. 1).

As explained by the KIPO Trademark Police, the Anti-Counterfeiting Council operates through several key mechanisms that foster collaboration between public and private stakeholders to effectively identify and reduce counterfeit goods in the marketplace. These include the following (KIPO Trademark Police, 2024, p. 1):

- *Information sharing:* One of the core activities of the Council is information sharing. Members, including government agencies, trademark owners, and online platforms, share data on the distribution of counterfeit goods. Collective efforts of this kind make it possible to identify counterfeit goods and take swift action against counterfeiters.
- *Identifying counterfeits:* Trademark owners play a crucial role in identifying counterfeit products. They provide detailed information and expertise that helps distinguish counterfeit goods from the real thing. This knowledge is essential for online platforms to accurately identify and remove counterfeit listings.
- *Blocking counterfeit websites:* When counterfeit products are identified, online platforms can take swift action to block the sites selling these goods. Such a proactive approach, based on information provided by trademark owners, ensures that counterfeit goods do not reach consumers.

It should be noted that the effectiveness of the Anti-Counterfeiting Council is demonstrated by its impressive achievements in 2023. The Council successfully prevented the sale of 238,000 counterfeit goods in various sectors, including fashion, cosmetics, and technology. This resulted in an estimated saving of approximately USD 7.5 billion in potential consumer losses. These results underscore the significant impact of well-coordinated public-private partnerships

in combating counterfeiting and highlight the potential benefits of collaborative efforts in addressing complex global challenges (KIPO Trademark Police, 2024, p. 1).

The Anti-Counterfeit Council's ongoing initiatives are crucial in enhancing its efforts to combat counterfeit goods. One such initiative is the creation of sector-specific working groups, which focus on developing tailored anti-counterfeiting strategies for different industries. This ensures that measures are adapted to each sector's unique challenges. Another initiative is the unified reporting center, a centralized platform that streamlines the process for businesses to report counterfeit-related issues. This allows for faster responses and more efficient coordination among Council members (KIPO Trademark Police, 2024, p. 2).

The Council also holds performance sharing sessions and training workshops to keep members informed about new counterfeiting tactics, enforcement technologies, and best practices. These sessions promote knowledge sharing and enhance the Council's collective ability to combat counterfeit goods. Furthermore, the expansion of membership demonstrates the Council's growing influence. In May 2024, AliExpress joined the Council, along with platforms like Temu and Shein, strengthening its global efforts to address counterfeiting in digital marketplaces (KIPO Trademark Police, 2024, p. 2).

Image N° 12



Source: KIPO Trademark Police, Anti-Counterfeit Council 2023 Wrap-up Meeting

Image N° 13



Source: KIPO Trademark Police, Anti-Counterfeit Council 2023 Wrap-up Meeting

E. Benefits on collaboration with government authorities

The KIPO Trademark Police illustrates the benefits of public-private cooperation through the Anti-Counterfeiting Council as significant. First, the partnership has greatly enhanced enforcement capabilities by combining public regulatory authority with private technological expertise and market knowledge, enabling the Council to act swiftly against counterfeiting activities. This collaboration also ensures a real-time response to counterfeiting threats, enabling rapid detection and removal of counterfeit goods, minimizing consumer exposure and market disruption. The initiative also provides strong consumer protection by blocking the sale of harmful counterfeit products and maintaining consumer confidence in the marketplace.

In addition, the Council's efforts help support legitimate businesses by preventing unfair competition from counterfeit goods that could damage brands and undermine market prices. The involvement of international trademarks and organizations strengthens global cooperation and ensures that IP rights are respected across borders. This enhanced cooperation facilitates the sharing of best practices and the creation of a united front against the proliferation of counterfeit products, benefiting both businesses and consumers worldwide (KIPO Trademark Police, 2024, p. 1).

To summarize, the success of the Anti-Counterfeit Council demonstrates the value of public-private cooperation in dealing with the difficult issue of counterfeit goods. By combining the

resources, experience, and regulatory authority of both sectors, the Council has dramatically decreased the proliferation of counterfeit items, protected consumers, and maintained the integrity of real enterprises.

The addition of large platforms such as AliExpress, as well as the ongoing increase of membership, illustrate the model's effectiveness and expanding importance. This collaborative strategy provides a significant model that other economies can follow, opening the path for better, more coordinated anti-counterfeiting operations around the world.

Through this partnership, the Anti-Counterfeiting Council, exemplifies the benefits of a successful cooperation with government authorities, a strategy highlighted in the Recommendations of this document. By combining public regulatory authority with private sector expertise in technology and market dynamics, the Council has significantly enhanced enforcement capabilities.

5. *Indecopi - Mercado Libre Cooperation Agreement*

A. Challenge

This case allows us to examine the importance of closer cooperation between public and private actors in order to mutually improve their ability to combat counterfeiting in the digital ecosystem. Existing IP rights protection frameworks, often designed for traditional trade, are not always efficient to keep pace with these developments.

As a result, many economies are struggling to deal effectively with digital counterfeiting. This problem is not isolated to a single platform or trademark owner; rather, it has become a systemic issue that is growing in tandem with the expansion of online platforms (EUIPO, 2021 B, p. 21). The lack of an adequate, dynamic regulatory framework makes it difficult to ensure that enforcement remains relevant and effective.

In addition, the growing reliance on online platforms for business transactions has increased the need for cooperation between public authorities and private actors, such as digital platforms. This interaction is crucial to ensure effective solutions, as public authorities often lack the technological tools and market access that private platforms have. The challenge is therefore not only to enforce the law but also to foster collaborative efforts that can bridge the gaps between public regulation and private sector capabilities.

B. Problem under study

As explained, the challenges arising from the proliferation of trademark counterfeiting in the digital environment demonstrate to be particularly difficult for those economies with limited resources and insufficient capacity to deal with the problem effectively. Without robust legal frameworks or adequate funding for technological advances anti-counterfeiting efforts are often fragmented and inefficient. This resource gap underlines the urgency of alternative approaches to tackle the problem comprehensively.

One widely adopted strategy is to foster collaboration between public institutions tasked with combating trademark counterfeiting and digital platform operators. These partnerships, which include entities such as marketplaces and social networks, are seen as a crucial first step in strengthening institutional capacity. By leveraging the strengths and expertise of both sectors,

this collaborative approach aims to create a more coordinated and effective response to trademark counterfeiting in the digital environment.

This kind of collaboration has emerged as a powerful approach to addressing shared challenges. They can be a useful way to strengthen the institutional capacity of all the parties by leveraging the technological capabilities and data-driven insights of digital platforms. Furthermore, public authorities can gain access to tools for detecting and removing counterfeit content more effectively, while digital platforms benefit from clear regulatory guidance and support in enforcement efforts. (Desai, 2018, p. 222).

By working hand to hand with digital platforms, these efforts create an environment where both public authorities and platform operators can work in real-time to address counterfeiting activities. For example, platforms can share detailed analytics, suspicious activity reports, and automated detection mechanisms with authorities, facilitating rapid responses to trademark counterfeiting. Additionally, these collaborations allow public institutions to fine-tune their enforcement strategies to align with the unique operational landscapes of these platforms (Desai, 2018, p. 222).

This form of engagement also increases transparency, allowing external stakeholders and third parties to observe the organization's practices more closely. This transparency builds trust and encourages other stakeholders to share critical information that can help address specific challenges. Furthermore, these interactions allow digital platforms and authorities to evaluate and refine their approaches, ensuring the legitimacy and effectiveness of their actions, which is essential for maintaining stakeholder trust and ensuring long-term collaborative success (Desai, 2018, p. 224).

C. Solution studied

The case of Peru's Indecopi Distinctive Signs Commission illustrates an effective approach to tackling trademark counterfeiting on digital marketplaces through targeted verifications and joint enforcement actions.

Traditionally, Indecopi Distinctive Signs Commission had practices and alert systems in place specifically designed to combat trademark counterfeiting, as illustrated in the image below. These systems, since their implementation, allowed the authorities to promptly notify

trademark owners of possible infringements, thus speeding up the process to undertake the necessary enforcement actions.

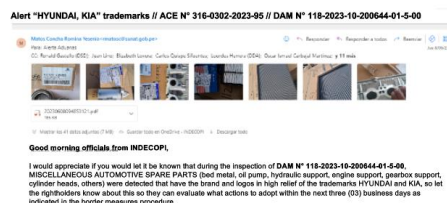
Image N° 14

STRENGTHENING OF MEASURES AT THE BORDERS

- Border measures system



- Alert system



Source: Chuez. S. (2024). Peruvian Initiatives to strengthen the fight against trademark counterfeiting in the digital environment

However, this scenario was different in the digital environment. Until 2018, the absence of a specific legal provision empowering Indecopi's Distinctive Signs Commission to order the removal of virtual sales points by e-commerce platform owners posed an enforcement challenge for this entity. For that reason, the public institution proposed a regulatory reform to the Executive Branch.

This effort led to the issuance of Legislative Decree 1397, published in September 2018. The decree granted trademark authorities the power to mandate —through precautionary measures or final resolutions— that third parties, such as e-commerce platforms, deactivate virtual sales points, with noncompliance subject to sanctions for contempt.

Within this revised regulatory framework, conversations with Mercado Libre began in 2019, culminating in the signing of a cooperation agreement in February 2020. Mercado Libre is a major digital marketplace in Latin America with extensive operations in 18 economies. The platform is considered a generalist marketplace, as it's used for both B2C and B2B transactions, and allows for C2C listings (Shepherd, 2023, p. 9).

In November 2020, the Distinctive Signs Commission conducted an operation on the website Mercado Libre —only on its Peruvian domain. The aim of the operation was to verify the existence of unauthorized use of registered trademarks on products such as toys, facemasks, and electrical goods.

The operation uncovered 47 listings that used registered trademarks, leading to the issuance of a precautionary measure against Mercado Libre. The platform was required to take measures to prevent the misuse of trademarks such as INDECO, B-TICINO, LEGO, STAR WARS, and LOL for the products involved. A subsequent search, extended to include toy listings, revealed a further 103 instances of suspected trademark infringement. This led to a second precautionary measure requiring joint action to protect trademarks, including 3M, LEGO, LOL, and others.

The actions taken by Mercado Libre and Indecopi resulted in significant progress in the fight against trademark counterfeiting on the platform. Following the identification of counterfeit listings, Mercado Libre removed all the products investigated from its site and provided detailed information on the identity of the advertisers involved.

This cooperation was crucial in facilitating legal action against the sellers responsible for the counterfeit goods. Indeed, ex officio complaints were also filed against each seller offering the infringing products, and the Distinctive Signs Commission imposed appropriate sanctions against them.

Several key factors contributed to the success of this operation. First, the strong inter-institutional collaboration between Indecopi and Mercado Libre was essential. The platform's proactive approach, in particular its willingness to maintain constant communication with Indecopi, ensured an efficient and effective response to the problem.

Secondly, Mercado Libre's prompt action in removing the infringing listings played a crucial role in preventing further exposure of counterfeit products to consumers. Finally, the platform's provision of information on the identity of advertisers potentially infringing trademark rights helped the authorities to take swift action, particularly in relation to products that posed a risk to public health and safety, such as toys and medical devices.

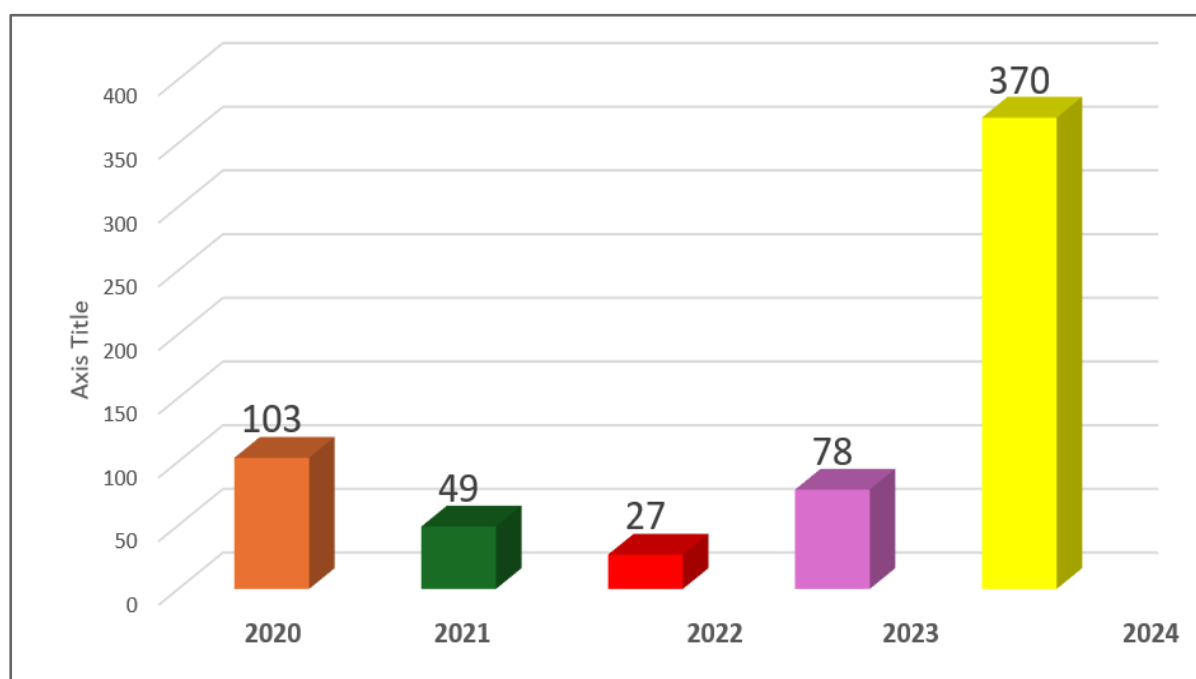
It must be noted that the cooperation agreement between Indecopi and Mercado Libre has evolved to prioritize not only the removal of infringing content but also the initiation of formal

infringement proceedings against counterfeiters. In this way, each takedown of illegal content carries significant weight, as it is closely tied to subsequent legal actions.

By establishing a clear framework for cooperation, the agreement has enhanced the capacity of both Indecopi and Mercado Libre to proactively combat trademark counterfeiting, improving both the efficiency and scope of enforcement efforts. Evidence of this is the functioning of the Digital Compliance Alerts System, which over the years has reported multiple infringements that have been addressed through the corresponding sanctioning procedures. This system has been particularly useful in recent years due to the substantial number of alerts generated regarding counterfeit goods, as shown in the following graph.

Figure N° 7

Digital compliance alerts (yearly)



This partnership provides a sustainable model for combatting digital counterfeiting and demonstrates the importance of ongoing, structured engagement between public authorities and private platforms to protect IP and consumers in the digital marketplace.

This case highlights the effectiveness of collaboration between public authorities and private platforms in combating trademark counterfeiting in the digital environment. The timely removal

of counterfeit goods and the imposition of penalties on sellers serve as a deterrent and demonstrate the potential for proactive enforcement to protect IP and consumer safety.

CONCLUSION

The rapid growth of e-commerce has transformed global trade, bringing immense opportunities for businesses and consumers, but also new challenges, particularly in the form of trademark counterfeiting. Counterfeit goods not only threaten consumer safety and undermine brand integrity, but also undermine the trust and efficiency that e-commerce platforms seek to foster. Tackling this problem requires a robust, coordinated effort tailored to the unique realities of the digital marketplace.

This Guidebook has been developed to strengthen the capacity of APEC economies to combat trademark counterfeiting in the digital environment. In doing so, it has provided a comprehensive analysis of the challenges posed by the anonymity and cross-border nature of digital commerce, highlighting critical obstacles such as the lack of a consistent global framework, technological limitations, and jurisdictional complexities. By examining the modalities of counterfeiting, including online marketplaces, social media platforms and darknet services, the Guidebook paints a detailed picture of the evolving threats faced by enforcement authorities and stakeholders.

To address these challenges, the Guidebook offers legal and digital enforcement recommendations that aim to create a proactive and adaptive framework for combating counterfeit goods. The legal recommendations focus on establishing robust regulatory standards and strengthening international cooperation, while the digital recommendations emphasize the use of advanced technologies, such as AI for monitoring, detection, and enforcement. These measures aim to close the gaps that counterfeiters exploit and ensure a safer and more reliable digital marketplace.

The inclusion of case studies helps to underline the importance of collaboration and innovation in addressing these challenges. By showcasing successful initiatives, such as Peru's collaboration with major e-commerce platforms, and advanced technological solutions implemented by stakeholders, the Guidebook provides actionable insights and best practices. These examples demonstrate the potential of partnerships between public authorities, private entities, and technology providers to mitigate the impact of counterfeiting.

Ultimately, the Guidebook aims to promote a unified, collaborative approach among APEC economies that recognizes the shared responsibility of governments, businesses, and consumers in combating digital trademark counterfeiting. By adopting the strategies and

recommendations outlined here, APEC economies can enhance their enforcement capabilities, protect IP rights, and build a safer and more trustworthy e-commerce ecosystem.

REFERENCES

- APEC Economic Committee. (2024). Study on Economy Legal Frameworks for the Implementation of ODR under the APEC Collaborative Framework.
- APEC. (2019). Cross-border privacy rules system policies, rules and guidelines.
- APEC. (2020). About us. Retrieved from: <https://www.sciencedirect.com/science/article/abs/pii/S104900789290002G>
- Arana, M. (2017). La protección jurídica de los signos distintivos: marcas, nombres y lemas comerciales. Fondo Editorial de la PUCP.
- Aura Blockchain Consortium. (2022). Aura Blockchain Consortium Launches Aura SaaS for Luxury Brands. Press Release
- Bhadauria, S., Kumar, P., and Mohanty, T. (2021, December). Intellectual Property Protection using Blockchain and Digital Watermarking. In 2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (pp. 1-6). IEEE.
- Buiten, M. C. (2021). The digital services act from intermediary liability to platform regulation. *J. Intell. Prop. Info. Tech. and Elec. Com. L.*, 12, 361.
- Bulayenko, O., Frosio, G., Mangal, N., and Lawrynowicz-Drewiek, A. (2022). Cross Border Enforcement of Intellectual Property Rights in the EU. Centre for International Intellectual Property Studies (CEIPI).
- Bumatay, A. (2015). A Look at the TradeKey: Shifting Policing Burdens from Trademark Owners to Online Marketplaces. *Hastings Bus. LJ*, 11, 341.
- Calliess, G. P., and Heetkamp, S. J. (2019). Online Dispute Resolution: Conceptual and Regulatory Framework. TLI Think.
- CAPECE (2024). Reporte oficial de la industria Ecommerce en Perú. Cámara Peruana de Comercio Electrónico.
- Casino, F. et al., (2022) "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," in *IEEE Access*, vol. 10, pp. 25464-25493.
- Cedrola, E., Kulaga, B., and Pomi, G. L. (2024). Blockchain: Technology Transforming the Fashion Industry. In *Digital Transformation for Fashion and Luxury Brands: Theory and Practice* (pp. 27-46). Cham: Springer International Publishing.
- Chatterjee, A. (2016). Elements of information organization and dissemination. Chandos Publishing.

- Chavis, Kami. (2008). The politics of policing: ensuring stakeholder collaboration in the federal reform of local law enforcement agencies. *Journal of Criminal Law and Criminology*, 98(2), 489-546.
- Cosearch. (2024). Trade in Counterfeit Goods Market Set To Reach \$1.79 Trillion in 2030. Press-releases.
- Data Insight. (2024). Investigación de mercados: Comercio por Internet en Rusia 2024.
- Desai, V. M. (2018). Collaborative stakeholder engagement: An integration between theories of organizational legitimacy and learning. *Academy of Management Journal*, 61(1), 220-244.
- Dutta, M. (1992). "Asia-Pacific economic cooperation: Structure of a common economic region". *Journal of Asian Economics*, 3(1).
- EUIPO. (2016). Research on online business models infringing intellectual property rights. European Union Intellectual Property Office.
- EUIPO. (2019). Status report on IPR infringement.
- EUIPO. (2021). Domain Names, Discussion Paper. Challenges and good practices from registrars and registries to prevent the misuse of domain names for IP infringement activities.
- EUIPO. (2021). New Development of Online Counterfeiting and Piracy in China: Legislation, Cases and Practice. IPKey.
- EUIPO. (2023). EU enforcement of intellectual property rights: Results at the EU border and in the EU internal market 2022.
- Federal Antimonopoly Service. (2024). Twenty-Second Intergovernmental Group of Experts on Competition Law and Policy.
- Frosio, G. F. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. *Nw. UL Rev. Online*, 112, 18.
- Gangjee, D. S. (2024). Panoptic Brand Protection? Algorithmic Ascendancy in Online Marketplaces. *Algorithmic Ascendancy in Online Marketplaces. European Intellectual Property Review*.
- Grandón, E. E., and Pearson, J. M. (2004). Perceptions of strategic value and adoption of e-Commerce: a theoretical framework and empirical test. In *Value creation from e-business models* (pp. 178-210). Butterworth-Heinemann.
- ICANN (2022) Submission to the European Commission Call for Evidence on the EU Toolbox Against Counterfeiting.
- Ishikawa, N., and Takiguchi, A. (2024). Amended Provider Liability Limitation Act (Act on Measures against Information Distribution Platforms). Lexology.

- Islam, M. M., Merlec, M. M., and Hoh, P. I. (2022, July). A comparative analysis of proof-of-authority consensus algorithms: Aura vs Clique. In 2022 IEEE International Conference on Services Computing (SCC) (pp. 327-332). IEEE.
- JP Morgan (2024). Global e-commerce trends report. JP Morgan.
- Katherine B. Forrest and Jerrold Wexler (2023). Is Justice Real When “Reality is Not?: Constructing Ethical Digital Environments. Elsevier.
- KIPO Trademark Police (2024) Best Practices in Korea: Public-Private Collaboration through the Anti-Counterfeit Council.
- Kobayashi, Y. (2022). Stand your ground against anonymous online harassers with Amended Provider Liability Limitation Act. CHUO SOGO LAW.
- Konopliov, A. (2024). Mobile Commerce Statistics 2024: Trends and Key Insights.
- Lin, J., Long, W., Zhang, A., and Chai, Y. (2020). Blockchain and IoT-based architecture design for intellectual property protection. International Journal of Crowd Science, 4(3), 283-293.
- Maraví, A. (2014). Introducción al Derecho de los Marcas y otros Signos Distintivos en el Perú. Foro jurídico, (13), 58-68.
- Marks, D., and Nordemann, J. B. (2022). The role of the domain name system and its operators in online copyright enforcement (No. 2). BRIP Working Paper.
- Momen, M. N. (2021). Multi-stakeholder partnerships in public policy. In Partnerships for the Goals (pp. 768-776). Cham: Springer International Publishing.
- Mostert, F. W., and Schwimmer, M. B. (2011). Notice and takedown for trademarks. Trademark Rep., 101, 249.
- Mostert, F., and Lambert, J. (2019). Study on IP enforcement measures, especially anti-piracy measures in the digital environment.
- OECD (2019), Unpacking E-commerce: Business Models, Trends and Policies, OECD Publishing
- OECD (2021), Development Co-operation Report 2021: Shaping a Just Digital Transformation, OECD Publishing,
- OECD (2022), "The role of online marketplaces in protecting and empowering consumers: Country and business survey findings", OECD Digital Economy Papers, No. 329, OECD Publishing.
- OECD/EUIPO (2021), Global Trade in Fakes: A Worrying Threat, Illicit Trade, OECD Publishing
- OECD/EUIPO (2023), Why Do Countries Import Fakes?: Linkages and Correlations with Main Socio-Economic Indicators, Illicit Trade, OECD Publishing

- Ostergard, R. L. (2000). The making of a regime: intellectual property rights in the international system. *Journal of International Business Studies*, 31, 2 (Second Quarter 2000): 349-360.
- Paun, C. (2011). Between collaboration and competition: global public-private partnerships against intellectual property crimes.
- Paun, C. (2013). Globalization of Law Enforcement-A Study of Transnational Public-Private Partnerships Against Intellectual Property Crimes (Doctoral dissertation, Universität Bremen).
- PCMI (2024). E-commerce Data Portrait of Peru How Peruvians buy online. Payments and Commerce Market Intelligence.
- Potluri, J., Gummadi, H., Alladi, K., and Ramesh, G. (2023). Securing Intellectual Property in the Digital Age through Blockchain Innovation. In 2023 Global Conference on Information Technologies and Communications (GCITC) (pp. 1-5). IEEE.
- Research and Markets. (2023). Philippines B2C Ecommerce Market Opportunities Databook Q1 2023. Research and Markets.
- Rodríguez, V. (2020). How does Mercado Libre deal with online IP infringements?
- Rosati, E. (2023). The localization of IP infringements in the online environment: from Web 2.0 to Web 3.0 and the Metaverse. *Journal Of Intellectual Property Law and Practice*, 18(10), 720-742.
- Shaw, S. (1999). JISC Technology Applications Programme (JTAP)—Overview of Watermarks, Fingerprints, and Digital Signatures. The University of Edinburgh
- Shepherd, D. W. J., Whitman, K. M., Wilson, J. M., and Baloka, A. (2023). Practices Used by Online Marketplaces to Tackle the Trade in Counterfeits.
- Snyder, K. (2024), 35 E-Commerce Statistics of 2024. Forbes Advisor.
- Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer law and security review*, 35(4), 380-397.
- Tan, J. G. (2008). A Comparative Study of the APEC Privacy Framework- A New Voice in the Data Protection Dialogue? *Asian Journal of Comparative Law*, 3, 1–44.
- Thio, R., Christiawan, R., and Wagiman, W. (2024). Trademark Law in the Digital Age: Challenges and Solutions for Online Brand Protection. *Global International Journal of Innovative Research*, 2(4), 710-721.
- Tiffany (NJ) Inc. v. eBay Inc., 600 F.3d 93 (2d Cir. 2010)-
- Turillazzi, A., Taddeo, M., Floridi, L., and Casolari, F. (2023). The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15(1), 83-106.

- Tursunov, S. (2024). The growing challenge of trademark infringement in the digital age. *Elita. uz-Elektron Ilmiy Jurnal*, 2(2), 39-48.
- Van Greunen, L., and Gobac, I. (2021). Building respect for intellectual property—The journey toward balanced intellectual property enforcement. *The Journal of World Intellectual Property*, 24(1-2), 167-185.
- Wai, A, Nitivattananon, V, and Kim, S. M. (2018). Multi-stakeholder and multi-benefit approaches for enhanced utilization of public open spaces in Mandalay city, Myanmar. *Sustainable Cities and Society*, 37, 323-335.
- World Law Group. (2023). *Germany: Trademark Protection for Blockchain and Other Crypto Projects*.
- Xiong, G., Liu, Z., Liu, X., Zhu, F., and Shen, D. (2012). *Service Science, Management, and Engineering:: Theory and Applications*. Academic Press.