

# STUDY

## **INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS IN THE E-COMMERCE SECTOR**

**AUGUST 2025**

1. Introduction.....	3
1.1. Relevance of the Issue .....	3
1.2. Purpose and Objectives of the Study .....	3
1.3. Object and Subject of the Study .....	4
1.4. Research Methodology .....	4
1.5. Definition of Key Terms.....	4
2. E-commerce as an environment for IP infringements .....	6
2.1. The Role of Online Platforms in Today's Global Trade System .....	6
2.2. Peculiarities of IP Infringements in the Online Environment.....	7
2.3. Types of Platforms and Distribution Channels.....	8
3. Main mechanisms of platform abuse.....	9
3.1. Trade in counterfeits through e-commerce.....	9
3.2. Abuse of Delivery Systems.....	10
3.3. Account Recovery and Fraudulent Networks.....	12
3.4. Use of Telegram and Social Media .....	13
3.5. Concealment of Goods and Content Duplication .....	14
4. Types of Risks and Consequences of Infringements.....	16
4.1. Economic Impact on Rightsholders and the State.....	17
4.2. Risks to Consumer Health and Safety .....	17
4.3. Undermining trust in e-commerce .....	18
4.4. Social and Cultural Consequences .....	19
5. Reaction of Institutions and Platforms.....	20
5.1. International Practices in Combating IP Infringement .....	21
5.2. National Legislation of Ukraine .....	24
5.3. Platform Policies on IP Protection .....	29
5.4. Examples of Positive Practices.....	30
6. IP Rights Protection Tools .....	32
6.1. Administrative Tools on Platforms .....	32
6.2. Judicial and Extrajudicial Protection .....	33
6.3. Cooperation with Customs and Law Enforcement Authorities.....	34
6.4. Online Mediation as a Modern Tool for IP Rights Protection .....	35
6.5. Technological Solutions and Automation.....	39
6.6. Awareness, Education and Prevention .....	43
7. Conclusions and Recommendations.....	43
7.1. Research Findings .....	43
7.2. Recommendations for Online Platforms.....	44
7.3. Recommendations for State Authorities.....	45
7.4. Recommendations for Right Holders and Businesses .....	45

# 1. Introduction

## 1.1. Relevance of the Issue

Online platforms and marketplaces are a key element of today's global trade, offering broad access to goods and services and helping to streamline cross-border transactions. At the same time, these platforms are increasingly used to distribute counterfeit goods, engage in the unauthorized use of trademarks, and infringe copyright and related rights, creating significant risks for rightsholders, consumers, and the economic interests of states.

Infringement of intellectual property (IP) rights on the Internet causes both direct economic losses for companies and broader social consequences. The figures confirm that online platforms are the main channel for the sale of counterfeit goods, thanks to their accessibility, scale, and relative anonymity for sellers. The Entrupy report "State of the Fake 2024"<sup>1</sup> notes that among the fashion items inspected, 8.4% were found to be counterfeit, with brands such as Louis Vuitton and Prada most frequently affected. Entrupy is an international company specializing in the development of technologies for authenticating goods using artificial intelligence and computer vision. The data presented in the report is based on the results of actual inspections of physical goods in the secondary market and in online sales, making it a practical and relevant indicator of the scale of the problem.

In Ukraine, this problem is particularly relevant due to the active growth of e-commerce in both domestic and international markets. Many consumers, especially since the start of the full-scale war, have shifted to online formats, and distribution has become the main channel for the sale of goods. The presence of counterfeit goods on these platforms calls into question the effectiveness of self-regulation and creates a demand for stronger state and international oversight.

## 1.2. Purpose and Objectives of the Study

The purpose of the study is to provide a comprehensive analysis of current challenges related to the infringement of intellectual property rights in the online environment, as well as to examine the effectiveness of existing legal protection mechanisms at both the Ukrainian and international levels.

Objectives of the study:

- to identify the specific features and scale of IP rights infringements in e-commerce;
- to analyze the most common schemes of misuse of online platforms;
- to examine existing platform policies and assess their effectiveness;
- to study the national and international legal framework for counteraction;
- to assess threats to the state, business, and consumers;
- to formulate comprehensive recommendations.

---

<sup>1</sup> Entrupy. State of the Fake 2024 [Online resource]. – Available at: <https://www.entrupy.com/report/state-of-the-fakereport-2024/>

### 1.3. Object and Subject of the Study

The object of the study is e-commerce as an environment for the infringement of intellectual property rights, as well as the activities of online platforms in this area.

The subject of the study comprises the mechanisms, forms, and scale of IP rights infringements; institutional, legal, and technological response tools; as well as regulatory approaches to counteraction in the national and international context. The study also includes analysis of judicial practice, administrative procedures, content moderation policies, and the use of AI and other digital solutions for monitoring infringements.

### 1.4. Research Methodology

The study employs legal analysis, content analysis of platform policies, case analysis, statistical data, and comparative legal analysis.

### 1.5. Definition of Key Terms

**E-commerce** - a set of commercial processes carried out in a digital environment, particularly via the Internet. This includes the sale of goods and services, payment processing, contract conclusion, and information exchange.

**Online platform** - any digital resource that facilitates interaction between sellers and buyers. This may include marketplaces, social networks, messengers, or specialized websites.

**Marketplace** - an online platform that aggregates offers from multiple independent sellers and enables the sale and purchase of goods or services through a single interface.

**Online store** - an individual website created by a single seller to offer their goods or services online. Online stores may operate independently or as part of a marketplace.

**Counterfeit goods** - a) goods that infringe intellectual property rights in a trademark in Ukraine and bear, without authorization, a sign identical to a trademark protected in Ukraine for the same type of goods, or one so similar that it may be confused with the trademark; b) goods that infringe intellectual property rights in a geographical indication in Ukraine and contain a name or term, or are described using a name or term, protected by such a geographical indication; c) any packaging, label, sticker, brochure, user manual, warranty, or other such document, even if presented separately, that infringes intellectual property rights in a trademark or geographical indication, and that bears a sign, name, or term identical to a protected trademark or geographical indication, or so similar that it may be confused with such a trademark or indication, used in relation to the same type of goods for which the trademark or geographical indication is protected in Ukraine.

**Fake products** - products manufactured in violation of production technology or through the unauthorized use of a trademark, or by copying the shape, packaging, external design, as well as through the unauthorized reproduction of another party's product.

**Seller verification** - a procedure for confirming the accuracy of information about a seller, which may include document checks, identity verification, and confirmation of contact details.

**Intermediary information service** - a service involving the transmission and/or storage of information and the allocation of network identifiers. If such a service is provided by an entity that initiates the transmission of information, is able to influence the selection of the recipient of the information, or can modify the content being transmitted, it shall not be considered an intermediary information service.

**Intermediary service providers (ISPs)** - providers of electronic communications services, payment infrastructure operators, registrars (administrators) assigning network identifiers, and other entities that ensure the transmission and storage of information through information and communication systems.

## 2. E-commerce as an environment for IP infringements

### 2.1. The Role of Online Platforms in Today's Global Trade System

Online platforms have become a driving force in reshaping the global economy, transforming the ways goods and services are sold, delivered, and consumed. Over the past decades, they have evolved from being mere distribution channels into complex ecosystems where competition is shaped, marketing strategies are executed, and – unfortunately – systemic intellectual property infringements also take place.

Within Ukraine, several large online platforms operate actively, covering segments such as marketplaces, online catalogs, classified ad platforms, and niche online stores. These platforms differ in their operating models (B2C, C2C, B2B), types of sellers, degree of content moderation, and seller verification policies. These online resources span various market segments - from universal marketplaces to niche platforms and classified ad services. According to general estimates, the largest platforms in Ukraine had a combined total of over 60 million visits per month in 2023, indicating an exceptionally high level of digital commercial activity in the country.

**Online platforms provide a number of advantages:**

- convenience and speed of purchasing goods;
- access to a wide range of products;
- price comparison and the ability to read reviews;
- facilitating market access for small-scale entrepreneurs;
- development of dropshipping and delivery to remote regions (platforms are often integrated with logistics operators, enabling delivery even to remote areas without the need for warehouse infrastructure on the seller's side).

However, these same characteristics create conditions for the active spread of counterfeit goods. According to the EUIPO report "Intellectual Property Crime Threat Assessment" (2022)<sup>2</sup>, more than 70% of counterfeit cosmetics and perfumes reaching consumers are distributed via online platforms. In Ukraine, this trend is reinforced by limited oversight of sellers, the absence of strict requirements for verifying the origin of goods, and insufficient transparency in moderation procedures.

The dynamics of small-scale sellers' participation play a significant role. In many cases, seller accounts on platforms are formally registered under the names of individual entrepreneurs with only minimal verification. This practice creates gaps in the mechanisms for identifying offenders and makes it difficult to hold them accountable, as accounts are often created without proper verification and can be easily replaced after being blocked. As a result, unscrupulous sellers can avoid liability, change accounts after blocking, and re-upload goods that infringe intellectual property rights.

---

<sup>2</sup> EUIPO. Intellectual Property Crime Threat Assessment, 2022 [Online resource]. – Available at: <https://www.euiipo.europa.eu/en/publications/ip-crime-threat-assessment-2022>

In addition, a large number of "independent" websites created using universal online store builders are often used as mirror websites of marketplaces or as covert platforms for selling counterfeit goods while evading moderation.

Due to the rapid digitalization of trade, the development of marketplaces, and the increase in transaction volumes in the online environment, there is a strengthening of the global trend toward the growth of intellectual property rights infringements specifically in the online segment. The main channels for the distribution of counterfeit goods are increasingly shifting into the digital space - in particular, to marketplaces, e-commerce platforms, and social networks. In most cases, IP rights infringements are recorded on platforms that lack effective mechanisms for pre-screening content or verifying sellers, which creates gaps in the online protection system.

Thus, online platforms are not only an important tool for the development of e-commerce but also a high-risk environment in terms of intellectual property protection. Their role in the dynamics of IP infringements requires special attention from both the state and the platforms themselves due to the need to implement preventive control mechanisms, ensure seller transparency, and foster close cooperation with rightsholders, as well as to conduct comparative analysis with international practices regarding platform policies in the field of intellectual property rights protection. For example, leading global e-commerce platforms such as Amazon and Alibaba have for several years been implementing seller verification programs (Brand Registry, IP Protection Platform), as well as machine learning algorithms to automatically detect potentially counterfeit content.

In the European Union, the Digital Services Act (DSA)<sup>3</sup> introduces new obligations for large platforms regarding transparency, accountability, and prompt response to infringements. Such initiatives can serve as a benchmark for the Ukrainian market.

## 2.2. Peculiarities of IP Infringements in the Online Environment

Intellectual property infringements in e-commerce have a number of distinctive features that set them apart from offline violations and significantly complicate detection and response. First and foremost is the high level of seller anonymity. Many operate under fictitious names without providing proof of identity or legal status, making it impossible or substantially more difficult to identify them in the event of an IP rights violation.

Another characteristic feature is the use of fake accounts or mass registration of accounts to quickly resume activities after being blocked. Offenders often operate entire networks of accounts, with some responsible for listing products, others for financial transactions, and still others for logistics and customer communication.

A common practice is posing as genuine brands. This is done through visual imitation of original products – using brand logos, color schemes, packaging, and photography styles. Often, the photos depict genuine branded items, while the buyer actually receives a counterfeit. In some

---

<sup>3</sup> Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [Online resource]. – Available at: <https://eurlex.europa.eu/eli/reg/2022/2065/oj>

cases, infringers deliberately alter brand names or introduce spelling errors to bypass automated filters.

The use of social networks and messengers (in particular, Telegram) for sharing links, QR codes, completing transactions, and bypassing platform policies is also widespread. In some cases, the actual sale does not take place on the marketplace but through a channel or chat disguised as a consultation or promotion.

Infringers often employ schemes to avoid customs control. These include shipping small batches of goods, declaring them as personal parcels, separating the packaging, instructions, and the product itself, and then reassembling them locally.

Content duplication also deserves special attention - posting identical listings on multiple platforms under different accounts. This reduces the risk of losing an audience if a particular account is blocked and ensures constant visibility in search engine results. Moreover, sellers use SEO-optimized product descriptions, which makes detecting infringements even with technical tools more difficult.

Thus, intellectual property rights infringements in the online environment are characterized by constant variability, significant technical complexity, and the ability to quickly adapt to new conditions, which substantially complicates efforts to counter such phenomena.

Effective counteraction to such infringements requires a systemic approach that includes modernized legislation, cross-platform cooperation, the implementation of automated monitoring mechanisms, and the active involvement of rightsholders in protecting their rights.

## 2.3. Types of Platforms and Distribution Channels

The sphere of e-commerce in Ukraine and worldwide encompasses a wide range of digital platforms that differ in format, target audience, and level of moderation. Intellectual property rights infringements occur not only on general-purpose marketplaces but also in niche online stores, social networks, messaging services, and even specialized forums.

For analytical purposes, online channels for the distribution of counterfeit goods can be conditionally classified into the following categories:

**Centralized Marketplaces.** These are large online platforms that aggregate offers from multiple sellers. While most such platforms implement certain control tools, the sheer volume of listings and the complexity of detecting infringements leave them vulnerable to counterfeit products.

**Online Stores.** These are standalone websites that can be quickly created using template-based site builders. They are often used as duplicate or backup sales points after a seller is blocked on major platforms.

**Online Classifieds Platforms and Social Networks.** Content infringing IP rights is often posted in the form of private ads, "special offers," or posts with comments. Social networks are used as a tool for initial contact or to redirect a buyer to another resource.



**Messengers (Telegram, Viber, etc.).** Due to the anonymity and encryption of messages, messengers serve as a convenient tool for completing transactions and providing instructions on payment and delivery. They are also actively used to create closed groups where counterfeit goods are distributed.

**Platforms operating in Ukraine but registered abroad.** Platforms that operate outside Ukrainian jurisdiction present a particular challenge for responding to infringements. As a result, rights holders often lack prompt access to mechanisms for removing counterfeit content or obtaining information about infringers.

Each of these channels has its own technical and legal specificities, which affect the speed of infringement dissemination, the complexity of detection, and the effectiveness of response. It is important to note that offenders often combine several channels: for example, advertising is placed on a social network, contact is made via a messenger, and the sale is completed on an independent website. This complicates the detection of the entire infringement chain and requires cross-platform analysis.

### 3. Main mechanisms of platform abuse

#### 3.1. Trade in counterfeits through e-commerce

Trade in counterfeits through e-commerce remains one of the most large-scale and threatening channels of intellectual property rights infringement worldwide. According to the joint OECD and EUIPO report "Mapping Global Trade in Fakes 2025"<sup>4</sup>, the volume of illegal trade in counterfeit goods in 2021 amounted to approximately USD 467 billion, which represents around 2.3% of global imports. In the European Union, this figure is even higher — the share of counterfeit products in total imports reached 4.7%.

Online sales of counterfeit products pose significant risks to consumers, cause economic losses to rights holders, and negatively affect the development of fair competition in digital markets. Modern offenders actively use online mechanisms to disguise goods, create proxy accounts, and quickly restore blocked listings, which significantly complicates the fight against infringements.

In the field of e-commerce, cases of using third-party platforms to duplicate listings are also widespread. In particular, some infringers create independent online stores based on platforms such as Shopify, WooCommerce, or Wix, where they sell products that appear to be genuine but are in fact counterfeits. Such resources are often used as channels for re-launching counterfeit content after it has been removed from the main platform.

In response to these growing challenges, major international platforms have introduced specialized programs, including Amazon Brand Registry<sup>5</sup>, eBay VeRO<sup>6</sup>, Alibaba IP Protection

---

<sup>4</sup> OECD/EUIPO. Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges [Online resource]. – Available at: [https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025\\_94d3b29f-en/full-report.html](https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en/full-report.html)

<sup>5</sup> Amazon. Amazon Brand Registry [Online resource]. – Available at: <https://sell.amazon.com/brand-registry>

<sup>6</sup> eBay. Verified Rights Owner (VeRO) Program [Online resource]. – Available at: <https://www.ebay.com/sellercenter/resources/verified-rights-owner-profiles>

Platform<sup>7</sup>. These mechanisms provide for the automated detection of counterfeit products, blocking of suspicious listings, creation of “blacklists” of sellers, and active cooperation with rights holders.

In Ukraine, there are currently no mandatory state requirements for platforms to verify sellers. At the same time, according to Article 7 of the Law of Ukraine “On Electronic Commerce (E-Commerce),” sellers are obliged to provide consumers with complete and accurate contact information. However, providing such data and verifying it are different processes. The law requires the seller to provide the data but does not obligate the platform to necessarily verify its authenticity. Thus, platforms may technically accept information without actually checking it, which creates gaps in control and may be exploited by unscrupulous sellers.

However, it is worth noting that certain initiatives demonstrate positive practices – in particular, the development of content moderation policies and the implementation of self-regulation elements at the level of individual platforms.

Overall, the situation with the sale of counterfeits in the online environment requires a strengthened, comprehensive approach that will include obligations for platforms regarding transparency, verification, cooperation with rightsholders, and prompt response to complaints. The Digital Services Act (DSA) can serve as a benchmark for national practice, as it requires large platforms to ensure an adequate level of content moderation, algorithmic transparency, and rapid response to illegal content.

#### **Recommendations:**

- Introduction of mandatory seller verification mechanisms on Ukrainian marketplaces.
- Development of platform-specific anti-counterfeiting policies following the examples of Amazon, eBay, and Alibaba.
- Creation of a national register of accounts blocked for intellectual property infringements.
- Development of a digital infrastructure for complaints and automated response to suspicious content.

### **3.2. Abuse of Delivery Systems**

One of the less regulated areas of concern is the use of delivery systems to conceal the origin of goods infringing intellectual property rights (IPR). Modern delivery services enable individuals and small businesses to ship goods without the direct identification of either the sender or the recipient, thereby complicating the detection and documentation of IPR infringements.

Some platforms offer integration with postal and courier services, allowing shipping labels to be generated automatically without any verification of the contents of consignments. In cases where counterfeit goods are delivered to parcel lockers, the actual identification of the

---

<sup>7</sup> Alibaba. Alibaba Intellectual Property Protection Platform [Online resource]. – Available at: [https://ipp.aidcgroup.net/index.htm?language=en\\_US#/ippHome](https://ipp.aidcgroup.net/index.htm?language=en_US#/ippHome)

purchaser or recipient may be hindered, particularly when transactions are carried out via temporary or unauthenticated accounts.

Criminal actors also take advantage of cross-border delivery options, including the use of transit warehouses that repackage goods and dispatch them from another country under the guise of new consignments, in order to avoid identification or taxation. At the same time, the lack of coordinated interaction between platforms, logistics companies, and customs authorities creates gaps in the traceability of counterfeit goods in transit.

#### **Example from Ukrainian Practice:**

In March 2023, the Economic Security Bureau of Ukraine (ESBU) uncovered a large-scale scheme for the supply of components and the manufacture of counterfeit perfumery products in Odesa region<sup>8</sup>.

The goods were sold through online channels, including websites, social networks, and messaging applications, while delivery was carried out via postal operators without adequate control. Counterfeit products with a total value exceeding UAH 9.2 million were seized, and supply channels for components used in production were identified.

During additional searches in a retail store selling perfumes and in warehouse premises located in the suburbs of Odesa, investigators found approximately 4,000 boxes containing bottles, dispensers, and sprayers intended for the production of counterfeit goods, with an estimated value exceeding UAH 8 million.

In addition, BEB investigators conducted a search at the "Pivdennyi Port" customs post, where they discovered nearly 140,000 bottles for bulk perfume refilling, with a total estimated value of more than UAH 1.2 million.

It was established that the colourless glass bottles, in various sizes, had been delivered to Ukraine from Poland. The consignee was a company owned by the proprietor of a business engaged in the production of counterfeit perfumery products.

This case illustrates how the use of anonymous delivery channels enables infringers to scale up illegal activities and evade liability. In practice, offenders can easily reorganise their logistics after one delivery channel is blocked — particularly when oversight at the delivery stage is limited.

An example of an international approach to addressing this issue is provided by initiatives of the World Customs Organization (WCO), including the introduction of systems for advance electronic declaration of goods and the implementation of automated risk-management systems to detect suspicious shipments.

---

<sup>8</sup> Economic Security Bureau of Ukraine. ESBU in Odesa region uncovered a scheme for importing components for the production of counterfeit perfumery products [Online resource]. – Available at: <https://esbu.gov.ua/news/beb-na-odeshchyni-vykrylo-skhemu-postavky-z-za-kordonu-komponentiv-dlia-vyrobnystva-pidroblenoi-parfumerii>

### Recommendations:

- Develop requirements for the integration of platforms with delivery services to ensure the transfer of information on the sender and the goods.
- Introduce mandatory verification of recipients when receiving goods with signs of intellectual property infringement.
- Strengthen customs control over transit shipments with a high risk of counterfeit goods.
- Establish information exchange between logistics operators, platforms, and government authorities.

## 3.3. Account Recovery and Fraudulent Networks

One of the most common methods for evading liability on online platforms is the systematic recovery of blocked accounts and the use of fraudulent networks. Offenders engaged in the distribution of counterfeit goods or other illegal content create multiple accounts, which are quickly blocked by platform moderators but subsequently replaced with new ones.

### Abuse Mechanisms:

**Multi-accounting:** Creating a large number of accounts on one or several platforms, used either in parallel or sequentially to distribute prohibited content.

**Use of fake or proxy data:** Registering accounts with forged documents, virtual phone numbers, proxy servers, and VPNs to conceal geolocation.

**Fraudulent networks:** Coordinating groups of multiple individuals who create, manage, and protect such accounts, often offering services to other infringers to bypass blocking measures.

**Account recovery:** Exploiting technical and legal loopholes to appeal or reactivate accounts after blocking, sometimes by filing false complaints against legitimate users to distract moderators. An individual violates the rules—their account is blocked. They then contact customer support with an appeal to restore it. Due to platform policies granting the right to appeal, accounts are sometimes reinstated even for repeat offenders.

### Reasons for Recurrence:

- Platforms guarantee protection against unjustified blocking and therefore grant users the right to appeal.
- Moderators are not always able to promptly and accurately review each complaint due to the high volume of accounts and requests.
- It is often difficult to determine intentional violations, especially in cases involving automated content moderation.

As a result, infringers are able to return repeatedly, which significantly complicates enforcement efforts against them.

### **Ukrainian Context:**

In Ukraine, these practices have become widespread on major marketplaces, online stores, and classified ad platforms. The absence of a unified centralized database of blocked accounts complicates the identification of repeat offenders and the demonstration of systemic violations. Some infringers operate networks consisting of dozens or even hundreds of accounts, enabling them to quickly re-establish their presence after removal.

It is recommended that Ukraine adopt and implement global best practices for account monitoring and control, including automated violation detection systems already implemented on leading international platforms.

### **International Practice:**

Major international marketplaces (Amazon, eBay, AliExpress) employ centralized account monitoring systems and cooperate with law enforcement authorities through Brand Protection and IP Enforcement programmes. They implement multi-factor authentication, seller verification requirements, and IP address blocking.

The European Digital Services Act (DSA) requires platforms to provide transparent reporting on account removals and encourages cross-platform information sharing on infringers.

### **Recommendations:**

- Establish a centralized database of blocked accounts with access for platforms and law enforcement authorities.
- Introduce mandatory two-factor authentication and stricter seller verification requirements.
- Implement automated user behaviour analysis tools to detect anomalies.
- Conduct user awareness campaigns on fraud risks and protection methods.

## **3.4. Use of Telegram and Social Media**

In the current digital environment, Telegram has emerged as a significant global challenge, widely exploited by sellers of counterfeit goods and other infringers of intellectual property rights to circumvent filters and moderation measures on official marketplaces and social media platforms. Owing to its relative anonymity and the high speed of information dissemination, Telegram enables the effective organisation of sales outside the oversight of established platforms.

### **Key Mechanisms:**

#### **Links and QR Codes**

Buyers are frequently provided with direct links or QR codes redirecting them to alternative “mirror” versions of official websites or to specially created accounts where purchases can be completed without interference. Such mirrors replicate the functionality of the main site while evading the sanctions and blocking measures imposed by major platforms.

## Covert Marketing on Social Media

The use of “stories” containing links to external resources, comments posted under popular publications, as well as the dissemination of pseudo-reviews and “recommendations” are common practices of covert advertising. These techniques create an illusion of organic interest, thereby complicating the detection and removal of unlawful advertising.

### Threats and Challenges:

**Lack of direct control:** Telegram, as a messenger, is not regulated as strictly as official marketplaces and has a complex monitoring architecture, allowing channels to operate with a high degree of anonymity.

**Technical challenges in blocking:** Frequent changes in channel names, the use of new links and QR codes complicate the work of law enforcement agencies and platforms.

**Spread of disinformation:** Fake reviews and comments can mislead consumers, increasing the risk of purchasing low-quality or unsafe products.

### Recommendations:

- Development of specialized tools for monitoring Telegram channels using artificial intelligence and text analytics to detect illegal advertisements and links.
- Facilitate cooperation between competent law enforcement authorities and messenger administrators to ensure prompt blocking of channels infringing IP rights.
- Conduct awareness campaigns among consumers regarding the risks of purchasing goods outside official channels.
- Strengthen international coordination in combating cross-border trade in counterfeit goods via messengers.

## 3.5. Concealment of Goods and Content Duplication

Infringers of intellectual property rights increasingly employ sophisticated techniques for concealing goods and duplicating content in order to circumvent moderation systems of marketplaces and social platforms. These methods significantly complicate the identification and suppression of illegal activities.

### Main Forms of Concealment and Duplication:

#### Concealment of Goods

**Modification of descriptions and keywords.** Infringers use synonyms, misspellings, special characters, or codes instead of direct brand and product names to evade search algorithms and filters. Analytical data from the OECD/EUIPO indicates that a significant proportion of goods exploiting online filters use altered descriptions and images to conceal their nature. This practice complicates the automated detection of counterfeit products.

**Visual duplication with variations.** Duplication of images with minor changes, such as cropping, adding watermarks, altering backgrounds, or changing colors, helps avoid detection by computer vision–based image recognition systems.

**Image Recognition (Computer Vision)** - is an artificial intelligence technology that enables computers to "see" and analyze visual information, such as photographs or videos. Specifically, it is the ability of a computer to recognize objects, text, colors, shapes, and even more complex patterns in images - in a manner similar to how humans perceive them, but automatically and quickly.

In the context of marketplaces and intellectual property rights protection:

- Image recognition technologies help platforms automatically detect copies of product images (e.g., counterfeits), even if the images have been slightly modified (cropped, background changed, etc.).
- This makes it possible to block illegal content that infringes copyright or trademark rights more effectively. For example, if an infringer uploads an image of an original brand with minor alterations, the system will identify the similarity and flag the listing for review.

This technology is widely used by major international marketplaces (Amazon, eBay) and social media platforms to combat counterfeiting.

## **Content Duplication**

**Creation of "mirror" websites and accounts.** Infringers create copies of official websites and accounts on other domains or platforms with minimal differences in name or design. This enables them to quickly resume sales after the primary resources are blocked.

**Use of automated bots for mass duplication.** Automated systems generate thousands of ad variations with minor modifications, making their prompt removal virtually impossible.

**Use of multiple platforms and channels.** After being blocked on a marketplace, infringers actively migrate content to social networks, messengers, or specially created Telegram channels, where they duplicate ads containing hidden links and QR codes.

In the European Union, the Digital Services Act (DSA) introduces new obligations for online platforms, including marketplaces. Platforms are required to implement advanced technologies to detect and combat content duplication and masking, as well as to conduct regular random checks of goods and report on the effectiveness of measures aimed at ensuring a safe digital environment. Furthermore, the DSA requires prompt responses to infringement notifications and imposes obligations to ensure the transparency of moderation and content removal algorithms.

These requirements are particularly relevant in combating the masking of counterfeit goods, where sellers deliberately alter descriptions, images, or keywords to evade detection.



On Amazon seller forums (including Reddit), there have been repeated reports of accounts being suspended following complaints of intellectual property infringements, with sellers quickly creating new accounts - sometimes within just 24 hours. After setting up new accounts, they duplicated their previous listings, using slightly altered photos and deliberately modified product descriptions. Such actions allow sellers to temporarily bypass automated detection algorithms and continue sales, even though this practice violates the platform's rules.

Similar schemes are also observed in Ukraine, particularly on local marketplaces. Counterfeit products often reappear after being blocked - under modified names, in different product categories, or through newly created seller accounts. In some cases, sellers deliberately provide misleading or incomplete information about the product to conceal its origin.

These practices call for stronger seller verification, the introduction of mechanisms to detect linked accounts, monitoring of duplicated content, and systematic oversight by platforms.

In international practice, certain platforms have already implemented comprehensive technical solutions to identify related accounts in order to prevent content duplication and the circumvention of restrictions following account suspensions.

In particular, Amazon and eBay actively employ multi-level algorithms to analyze IP addresses, payment details, contact information, access devices, and user behavioral patterns. Such systems make it possible to identify technical and financial links between accounts and to respond promptly to attempts to resume activities after blocking.

The use of such mechanisms enables a more effective response to repeated postings of counterfeit content, including cases where infringers attempt to duplicate listings with minimally altered data or to create new accounts to continue sales.

The introduction of such comprehensive algorithms on Ukrainian marketplaces would be an appropriate step to enhance the protection of intellectual property rights and to minimize the risks of abuse by unscrupulous sellers.

## 4. Types of Risks and Consequences of Infringements

In today's globalized world, the rapid growth of e-commerce and international trade has created both significant opportunities for economic development and serious challenges in the field of intellectual property rights protection. While the expansion of global supply chains fosters innovation and efficiency, it has also become a channel for the distribution of counterfeit goods, causing harm to rightsholders, states, consumers, and society as a whole.

The illicit trade in counterfeit goods undermines the rule of law, inflicts serious damage on the economy, poses risks to consumer health, erodes trust in digital trade channels, and even fuels organized crime. Abuse of online platforms and free trade zones further exacerbates these threats. This section examines the key consequences of such infringements and the risks they generate for rightsholders, the state, consumers, and society as a whole.



## 4.1. Economic Impact on Rightsholders and the State

One of the most significant economic consequences of intellectual property rights infringements on online platforms is the loss of revenues and market share for rightsholders. When a company becomes the target of an IPR infringement - for example, through the appearance of counterfeit products on marketplaces that copy its goods or services – this directly affects its sales volumes. Infringers often sell counterfeits at significantly lower prices, without bearing the costs of development, quality control, marketing, or licensing. Such unfair competition attracts part of the consumers and weakens the market position of the legitimate producer.

In addition to direct revenue losses, a rightsholder may gradually lose market share to entities that exploit unlawfully appropriated technologies, designs, or brands. This is particularly critical in highly competitive industries, where the ability to react quickly to innovation and protect the brand determines the long-term sustainability of a business. Companies that are systematically subjected to IP infringements report declining sales volumes, loss of customer base, and, in some cases, even forced reductions in investments in new products or withdrawal from the market.

Ultimately, the loss of revenue and market share not only undermines the financial stability of a particular company but also distorts the market, where legitimate players face competition from those who comply with neither legal norms nor ethical standards. This situation is especially dangerous in the online environment, where infringements can spread rapidly and on a large scale, while identifying the infringer is complicated by the anonymity of platforms..

In addition to direct losses for individual companies and state budgets, counterfeiting and piracy have broader socio-economic consequences. According to studies conducted by such organizations as the Organisation for Economic Co-operation and Development (OECD) and the European Union Intellectual Property Office (EUIPO), intellectual property infringements negatively affect international trade, the volume of foreign direct investment, innovation activity, employment levels, and also contribute to the growth of crime and environmental harm. Although the number of comprehensive assessments in this area remains limited due to the lack of comparable cross-country data, existing empirical research indicates that weak IP protection regimes hinder economic growth and reduce investment attractiveness.

## 4.2. Risks to Consumer Health and Safety

Counterfeit products distributed through online platforms pose a serious threat to consumer health, safety, and well-being. The production of such goods is usually carried out without compliance with basic quality and safety standards and, therefore, outside the scope of state regulation and control. This creates a high risk of products entering the market that are manufactured from uncertified, toxic, or defective materials.

Particularly dangerous are counterfeits in the categories of medicines, food products and supplements, children's toys, cosmetics, electronics, and automotive parts. According to estimates of international organizations, these groups of goods not only regularly appear among items seized by customs but are also directly associated with serious health risks –

ranging from allergic reactions to life-threatening conditions. In some cases, consumers may not even suspect they are purchasing a counterfeit due to its external similarity to the original product.

In 2023, the report Review of Notorious Markets for Counterfeiting and Piracy<sup>9</sup>, prepared by the Office of the United States Trade Representative, Executive Office of the President, specifically focused on the impact of counterfeit goods on consumer health and safety. In the section “Issue Focus: The Potential Health and Safety Risks Posed by Counterfeit Goods”, a detailed analysis is provided of the serious risks associated with the fact that the production of counterfeits usually takes place outside of regulatory oversight and safety requirements. This results in the emergence of low-quality, ineffective, and often dangerous products. The document highlights the most risky categories of goods, in particular: children’s toys, auto parts, electronics, pharmaceuticals, cosmetics, clothing, and footwear. Some of these marketplaces combine legal and illegal activities, while others operate exclusively as platforms for the distribution of counterfeit goods.

The report also notes that infringers are increasingly adapting to market changes and responding quickly to demand - for example, producing new batches of popular products under the guise of branded ones, using aggressive advertising, SEO manipulation, and pop-up ads. In order to avoid customs detection, they often split the delivery of packaging, instructions, and the product itself, assembling the item locally.

Attention should be drawn to the fact that about 60% of dangerous counterfeit products are supplied specifically through international postal and courier services, mainly for sale in the online segment. At the same time, China and Hong Kong continue to remain the main countries of origin of such goods. This situation indicates a high level of potential risk for consumers, since a significant share of counterfeit products is distributed through e-commerce and, as a rule, does not undergo proper verification and control procedures, which is due to the overload of customs authorities - according to the OECD/EUIPO report Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks, 2022<sup>10</sup>.

In summary, the consumption of counterfeit goods is not only an infringement of intellectual property rights but also a serious risk to life and health.

### 4.3. Undermining trust in e-commerce

Online shopping currently accounts for nearly 20% of all retail spending, reflecting the rapid growth of e-commerce. However, this growth is accompanied by a simultaneous increase in the volume of counterfeit products sold online. This fact seriously undermines consumer trust in brands and in e-commerce as a whole.

---

<sup>9</sup> Office of the United States Trade Representative. 2023 Review of Notorious Markets for Counterfeiting and Piracy [Online resource]. – Available at: [https://ustr.gov/sites/default/files/2023\\_Review\\_of\\_Notorious\\_Markets\\_for\\_Counterfeiting\\_and\\_Piracy\\_Notorious\\_Markets\\_List\\_final.pdf](https://ustr.gov/sites/default/files/2023_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_Notorious_Markets_List_final.pdf)

<sup>10</sup> OECD/EUIPO. Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks, 2022 [Online resource]. – Available at: [https://www.oecd.org/en/publications/dangerous-fakes\\_117e352b-en/full-report/component-7.html#chapter-d1e2055](https://www.oecd.org/en/publications/dangerous-fakes_117e352b-en/full-report/component-7.html#chapter-d1e2055)

According to Corsearch<sup>11</sup> - a company specializing in brand protection and related services - 46% of consumers in the United Kingdom stopped purchasing on a particular online marketplace after receiving counterfeit goods, while 44% confirmed that they ceased buying a certain brand because they feared its products might be counterfeit. In addition, 57% of those who had been deceived reported the presence of counterfeits on the online marketplace.

A study by the American company MarkMonitor<sup>12</sup>, which develops software for protecting brands against online counterfeiting, fraud, piracy, and cybersquatting, confirms these trends: 22% of buyers, upon discovering they had purchased a counterfeit, stated that their perception of the brand had significantly worsened, 26% completely stopped buying that brand's products, and 27% warn their family and friends about it. Such a loss of trust can lead to a large-scale decline in customer loyalty and significant reputational damage for brands.

This situation poses a serious threat not only to individual companies but also to e-commerce as a whole, since counterfeits create doubts among consumers regarding the quality and safety of goods they order online. If buyers fear being deceived or purchasing poor-quality products, it will significantly hinder the development of online markets and reduce overall sales levels.

Additionally, the spread of counterfeits undermines trust in e-commerce platforms and marketplaces, especially when they fail to effectively combat illegal trade. The lack of proper control and transparency deepens consumer concerns, while the growing circulation of high-quality "super fakes" makes it increasingly difficult to distinguish counterfeits, even for experienced buyers. To restore and maintain trust, it is essential that both brand owners and online platforms actively deploy modern monitoring and protection technologies.

Thus, the erosion of consumer trust caused by counterfeiting represents one of the key threats to the sustainable development of e-commerce, which must be addressed through systemic measures combining technology, legislation, and close cooperation between businesses and platforms.

#### 4.4. Social and Cultural Consequences

The spread of counterfeit products has not only economic and security consequences, but also profound social and cultural impacts. Counterfeit goods undermine social values, contribute to the spread of crime, and negatively affect cultural diversity.

One of the main social consequences is the erosion of trust in the legal system and state authorities, which, from the perspective of citizens, fail to effectively protect the rights of consumers and rightsholders. The mass prevalence of counterfeiting, especially in e-commerce, often creates a sense of impunity for offenders. This contributes to the expansion of the shadow economy and strengthens organized crime, which actively uses the profits from illegal trade to finance other criminal activities.

---

<sup>11</sup> Corsearch. UK Consumers Shun Online Marketplaces Due to Counterfeit Goods, 2023 [Online resource]. – Available at <https://corsearch.com/content-library/ebooks/counterfeit-products-are-endemic-and-it-is-damaging-brand-value/>

<sup>12</sup> Potter Clarkson. How Does Counterfeiting Impact Online Brand Protection? [Online resource]. – Available at: <https://www.potterclarkson.com/insights/how-does-counterfeiting-affect-brands/>

From a cultural perspective, counterfeit goods devalue intellectual work, particularly in the creative industries such as music, cinema, design, fashion, and literature. The loss of income and recognition for creators reduces their motivation to produce new cultural products, complicates professional growth, and slows down the development of cultural identity. As highlighted in the OECD report “The Economic Impact of Counterfeiting and Piracy”<sup>13</sup>, countries with a low level of IP protection face growing cultural dependence on imports, while local initiatives remain financially vulnerable.

Thus, the fight against counterfeiting and piracy is not limited to the protection of intellectual property rights. It also involves ensuring social stability, safeguarding cultural heritage, and shaping responsible consumer behavior. Addressing these challenges requires coordinated efforts by governments, businesses, international organizations, and civil society to strengthen enforcement mechanisms, promote awareness campaigns, and foster respect for creativity and innovation as essential values in modern society. This leads to negative trends in counterfeit consumption - according to a study by the Office of the United States Trade Representative Executive Office of the President<sup>14</sup>, more than 40% of young online consumers do not consider purchasing counterfeits a serious violation, especially if the product is cheaper or “looks like the original.”

Moreover, illegal trade in counterfeits often exploits vulnerable social groups - for example, through the use of cheap or child labor in countries with weak regulatory frameworks. This not only exacerbates social inequality but also undermines the achievement of the Sustainable Development Goals, particularly in the areas of decent work, economic growth, peace, and justice.

Thus, combating counterfeiting is not only a legal and economic issue but also a critical socio-cultural one. Systematic violations of intellectual property rights undermine the cultural value of innovation, discourage creators, fuel the shadow economy, and normalize unethical behavior, especially in the digital environment.

## 5. Reaction of Institutions and Platforms

This section is devoted to the study of national legal regulation of e-commerce and measures for the protection of intellectual property rights on Ukrainian e-commerce platforms.

The analysis combines both qualitative and quantitative approaches. The primary tool applied was content analysis of open sources, including the official websites of 25 leading Ukrainian platforms. A systematic review was conducted of terms of use, product publication guidelines, contact forms, and documents directly or indirectly related to IP rights.

---

<sup>13</sup> OECD. The Economic Impact of Counterfeiting and Piracy [Online resource]. – Available at: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2008/06/the-economic-impact-of-counterfeiting-and-piracy\\_g1gh906c/9789264045521-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2008/06/the-economic-impact-of-counterfeiting-and-piracy_g1gh906c/9789264045521-en.pdf)

<sup>14</sup> Office of the United States Trade Representative. Special 301 Report, 2023 [Online resource]. – Available at: [https://ustr.gov/sites/default/files/2023\\_Review\\_of\\_Notorious\\_Markets\\_for\\_Counterfeiting\\_and\\_Piracy\\_Notorious\\_Markets\\_List\\_final.pdf](https://ustr.gov/sites/default/files/2023_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_Notorious_Markets_List_final.pdf)

In addition, the analysis draws upon comparative review with international practices (Amazon, eBay, Alibaba), which allows for identifying structural differences and assessing the degree to which Ukrainian platforms are aligned with European and global standards. The study also examines examples of positive practices within the Ukrainian e-commerce market.

It should be noted that UANIPIO initiated an anonymous survey among Ukrainian e-commerce platforms with the aim of obtaining up-to-date information on intellectual property rights protection practices. At the same time, due to the limited level of feedback, further analysis was focused on open sources.

UANIPIO remains open to constructive dialogue with representatives of the e-commerce market, as the involvement of platforms in such initiatives contributes not only to the improvement of state policy in the field of IP, but also to increasing user trust, strengthening the business reputation, and reducing the risks of legal conflicts.

## 5.1. International Practices in Combating IP Infringement

Global online platforms have developed a wide range of tools to combat counterfeiting and piracy. Several notable examples can be highlighted.

Amazon - one of the leaders in IP protection. Amazon operates the Brand Registry program, which by 2023 had already been joined by more than 700,000 brands. Registered rightsholders can quickly report infringements through a user-friendly interface and even gain access to the Project Zero<sup>15</sup> tool, which allows them to independently remove counterfeit listings without administrator involvement.

Amazon has invested over \$1 billion in brand protection systems and engaged 15,000 employees to fight counterfeiting. As a result, more than 99% of infringements are detected and blocked proactively, before they are noticed by the brands themselves. This level of efficiency has been achieved thanks to artificial intelligence: Amazon screens new sellers (blocking 800,000 suspicious account registration attempts in 2022) and analyzes product characteristics for compliance with originals.

In addition, Amazon established the Counterfeit Crimes Unit<sup>16</sup>, which cooperates with police and customs authorities worldwide, helping to track down and prosecute manufacturers and sellers of counterfeits. In 2022 alone, Amazon initiated more than 1,300 lawsuits or referred cases for investigation against counterfeiters. This comprehensive strategy - combining verification, AI-driven monitoring, brand protection tools, and legal enforcement - makes Amazon one of the safest platforms in terms of IP protection. Notably, the number of complaints from brands on Amazon is decreasing: in 2022 there were 35% fewer complaints compared to 2021<sup>17</sup>, since counterfeit goods simply do not reach consumers.

---

<sup>15</sup> Amazon. Project Zero [Online resource]. – Available at: <https://sell.amazon.com/brand-registry/project-zero>

<sup>16</sup> Amazon. Counterfeit Crimes Unit [Online resource]. – Available at: <https://trustworthyshopping.aboutamazon.com/counterfeitcrimesunit>

<sup>17</sup> U.S. Chamber of Commerce. New Amazon Report Shows Dedication to Protecting Brands and Customers [Online resource]. – Available at: <https://www.uschamber.com/intellectual-property/new-amazon-report-shows-dedication-to-protecting-brands-and-customers#:~:text=Amazon%20recently%20published%20its%20third,platform%20are%20safe%20and%20authentic>

eBay - a pioneer in online commerce, which as early as 1998 launched the VeRO (Verified Rights Owner)<sup>18</sup> program to protect rights. The VeRO program allows rightsholders to submit notices regarding any listings that infringe their rights – upon receiving such notice, eBay promptly removes the listing and notifies the seller. Trademark, copyright, and patent owners can register with VeRO, obtain verified status, and then have their complaints processed very quickly (sometimes within hours).

eBay also maintains ongoing dialogue with major brands: “blacklists” of prohibited items for sale (for example, certain limited collections) are created, as well as keyword filters. eBay itself is not as proactive as Amazon in terms of AI-driven scanning (at least, publicly available data is more limited). However, eBay’s policies clearly state: “Counterfeit, fake, or otherwise inauthentic items are prohibited, and accounts may be suspended for listing them.” eBay applies sanctions to repeat offenders: if a seller repeatedly violates rules (receives VeRO complaints), their account is permanently closed.

In recent years, eBay has also introduced an authorization program: certain product categories (for example, designer handbags) may only be sold by verified sellers. Brands issue “authorizations” to such sellers, and eBay grants them access to list those products, while blocking others. This practice gradually reduces the space for counterfeits.

Thus, eBay relies on close cooperation with rightsholders and strict responses to complaints - VeRO has been in place for a long time and is quite effective (according to eBay, the majority of infringing listings are removed within 24 hours of a complaint, and many even preemptively).

Alibaba<sup>19</sup> - the Chinese e-commerce giant, which historically faced major challenges with the proliferation of counterfeits, has in recent years made significant efforts to improve the situation. Alibaba Group has established a comprehensive IP Protection Platform (IPP): rightsholders can register their rights and submit complaints through a single portal that covers multiple group platforms (Alibaba.com, 1688.com, AliExpress, Taobao, etc.). Complaints are processed fairly quickly - Alibaba states that 96% of reported listings are removed within 24 hours.

Alibaba has also implemented the Good Faith Takedown program: if a brand has a high credibility rating for its past complaints, its new complaints are processed almost immediately, without detailed manual review. This has simplified procedures for large companies, which previously complained about bureaucracy on AliExpress. In addition, Alibaba applies big data and machine learning technologies: it tracks abnormal patterns (for example, if a new seller suddenly lists 1,000 branded items at low prices, they are automatically flagged for review or blocked)

---

<sup>18</sup> eBay. eBay Verified Rights Owner Program and Intellectual Property Policy [Online resource]. – Available at: <https://export.ebay.com/en/regulations/ebay-policies/ebay-verified-rights-owner-program-and-intellectual-property-policy/>

<sup>19</sup> WIPO Magazine. Intellectual Property and E-Commerce: Alibaba’s Perspective [Online resource]. – Available at: <https://www.wipo.int/web/wipo-magazine/articles/intellectual-property-and-e-commerce-alibabas-perspective-40514>



Another step - in 2017, Alibaba created an alliance with 30 major brands (Intel, Swarovski, Louis Vuitton, etc.) to share information on counterfeiting trends and to cooperate in combating infringements. Under pressure from these brands, Alibaba even launched the Intellectual Property Joint-Force System, where brands and the platform jointly monitor suspicious goods - within a couple of years, this system received positive feedback from participants.

Alibaba also works with Chinese police to shut down underground factories. According to their 2020 report, they helped seize more than 300 million counterfeit goods worth around ~\$700 million. Thus, Alibaba is moving from a reputation as a “hub for fakes” to one of “transparent partnership with brands.” Although the problem has not been fully solved (due to the platform’s scale), the international community recognizes Alibaba’s progress in IP protection.

## Other International Practices

E-commerce platforms across Europe and the United States often join voluntary initiatives. For example, the EU Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet<sup>20</sup> signed back in 2016 by platforms such as Amazon, eBay, Alibaba, Rakuten, Facebook, and rightsholders (Nike, Adobe, Philips, and others), set out joint approaches: rapid information-sharing on new types of counterfeits, improved notice-and-takedown mechanisms, and the introduction of “notice-and-stay-down” (so that once-removed counterfeit content does not reappear). In the revised 2021 version of the Memorandum, new provisions were added on proactive monitoring - large platforms committed to using automated filters to detect obvious counterfeits.

In parallel, some social networks have also introduced direct bans on the sale of counterfeit goods and simplified complaint procedures. Meta (Facebook<sup>21</sup> i Instagram<sup>22</sup>) explicitly prohibits the sale of counterfeits and actively enforces intellectual property protection measures. The platforms provide simple and accessible complaint mechanisms (notice-and-takedown) that enable brands to remove counterfeit posts, advertisements, and profiles. Meta also employs advanced technologies such as machine learning, automated filters, and image search to identify and block counterfeit content even before it is published or advertised.

Etsy<sup>23</sup> (a handmade marketplace) faced the problem of counterfeit goods being sold “as vintage” and responded by creating a Trust and Safety team that reviews suspicious listings. It also introduced mandatory authorship verification for sellers of original works to avoid copyright infringements.

---

<sup>20</sup> European Commission. Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet (Updated 2021) [Online resource]. – Available at: <https://ec.europa.eu/docsroom/documents/18023/attachments/1/translations/>

<sup>21</sup> Meta. Facebook Help Center. Reporting Intellectual Property Violations [Online resource]. – Available at: <https://www.facebook.com/help/399224883474207>

<sup>22</sup> Meta. Instagram Help Center. Intellectual Property Policies [Online resource]. – Available at: <https://help.instagram.com/intellectualproperty>

<sup>23</sup> Etsy. Etsy Transparency Report 2023 [Online resource]. – Available at: [https://storage.googleapis.com/etsy-extfiles-prod/2023\\_Transparency\\_Report.pdf?ref=news](https://storage.googleapis.com/etsy-extfiles-prod/2023_Transparency_Report.pdf?ref=news)

Google<sup>24</sup> as an online advertising platform, has also joined these efforts: Google Ads enforces a policy that prohibits advertising websites selling counterfeits - violations result in the blocking of the advertiser's account. This is particularly important because it prevents counterfeit goods from being promoted through search advertising.

In conclusion, international practice shows that a comprehensive approach of “filter, respond, cooperate” is the most effective. Some invest in filtering technologies, others build strong channels of cooperation with rightsholders, while social networks integrate anti-counterfeit policies into their community standards. Ukrainian platforms have plenty to build on: many of these measures are already being partially implemented, and as Ukraine moves closer to the European market, this trend will only intensify.

## 5.2. National Legislation of Ukraine

The regulatory framework of Ukraine in the field of e-commerce and the protection of intellectual property rights currently consists of a number of legal acts, the main of which are outlined below.

The Law of Ukraine “On Electronic Commerce (E-Commerce)”<sup>25</sup> regulates legal relations in the field of e-commerce during the conclusion of electronic transactions. In particular, it establishes the foundations of the activities of online platforms and other electronic intermediaries, including sellers, marketplaces, classified platforms, hosting providers, and other intermediaries.

### Online platforms, depending on their business model, may have different statuses:

- if they only provide the technical possibility for posting content (advertisements) and do not interfere in the sales process - they are considered intermediary service providers in the information sphere;
- if, however, they act as a party to the transaction or control the sales process (for example, by processing orders, handling payments, or managing delivery), they are also regarded as full-fledged e-commerce entities, with all corresponding obligations towards the buyer.

For sellers (e-commerce entities), Article 7 of the Law provides for the obligation to supply consumers with accurate information about themselves: name, address, contact details, registration and tax data, etc. At the same time, the legislation does not require platforms to verify the accuracy of this information, which creates gaps in the mechanisms of preliminary control.

The Law defines the legal status of intermediary service providers in the information sphere (such as hosting providers and online platforms) and establishes for them the principle of

---

<sup>24</sup> Google. Google Ads Policy – Counterfeit Goods [Online resource]. – Available at: <https://support.google.com/adspolicy/answer/176017?hl=en>

<sup>25</sup> Law of Ukraine “On Electronic Commerce” of 03.09.2015 No. 675-VIII I [Online resource]. – Available at: <https://zakon.rada.gov.ua/laws/show/675-19#n2>



limited liability for infringements in the field of e-commerce, including intellectual property rights violations (Articles 9 and 17 of the Law of Ukraine “On Electronic Commerce(E-Commerce)”), provided that they do not alter the content of the information, are not its initiators, and, after receiving a reliable notice of infringement (for example, of IP rights), take prompt action to restrict access to the relevant content.

### Key Provisions:

1. Intermediary service providers in the information sphere are not parties to transactions concerning goods or services, except for the provision of intermediary information services themselves (such as Internet access, domain registration, etc.).
2. Intermediary service providers in the information sphere are not liable for the content of information that users upload or transmit, provided that they:
  - a. do not initiate the transmission of content;
  - b. do not determine the recipient;
  - c. do not alter the content of messages.
3. For hosting providers that offer temporary storage, the law permits automatic intermediate storage of information without liability, provided that:
  - a. the content is not altered;
  - b. access is ensured in accordance with industry standards;
  - c. upon receiving information about an infringement, access is blocked;
  - d. if the content is removed at the primary source, the provider restricts access to the corresponding content.
4. For the same group of hosting providers engaged in permanent storage at the request of the user, a similar mechanism applies: liability arises only after obtaining knowledge of illegal activity, including copyright infringement, and if the provider fails to take prompt measures to restrict access.
5. If such a provider goes beyond mere technical intermediation - by initiating transmission, selecting the recipient, or altering content - it loses this protection. In such cases, it becomes fully liable for the content and must:
  - a. provide contact information (name, address, email, identifiers, licences, etc.);
  - b. comply with tax obligations for the services provided.

Within the framework of this Law, intermediary service providers in the information sphere are exempt from liability for content under certain conditions – this corresponds to the “safe harbour” principle established in EU law (in particular, Directive 2000/31/EC on electronic commerce)<sup>26</sup>, according to which technical intermediaries are not liable for illegal content if specific conditions are met.

---

<sup>26</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [Online resource]. – Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0031>

The Laws of Ukraine “On Copyright and Related Rights”<sup>27</sup> and “On Protection of Rights to Trademarks for Goods and Services”<sup>28</sup> define the scope of intellectual property rights and the means of their protection. In the new version of the Law “On Copyright and Related Rights” dated 1 December 2022, the Internet dimension has been expanded: Article 56 of this Law for the first time introduced the procedure for terminating copyright and related rights infringements committed through the use of the Internet.

Article 56 of the Law of Ukraine “On Copyright and Related Rights” establishes a detailed administrative procedure to be followed by online platforms, hosting providers, and website owners in the event of copyright or related rights infringements on the Internet. This procedure has become a key element in the legal regulation of e-commerce, as it sets out a clear “notice-and-takedown” mechanism – from the moment a rightsholder submits a request to the website owner or hosting provider to the obligation to restrict access to the content or to restore it in the event of an unfounded claim. It also introduces liability for inaction, establishes response timeframes, standards for identifying the parties, and methods of communication. In this way, the Article aims to ensure the prompt protection of IP rights in the online environment, while minimizing abuses and balancing the interests of rightsholders, providers, and users.

Article 57 of the Law of Ukraine “On Copyright and Related Rights” sets out the obligations of hosting service providers – key technical intermediaries in the e-commerce ecosystem – to ensure compliance with intellectual property rights on the Internet. In particular, hosting providers are required to include in their contracts with users provisions prohibiting the placement of content that infringes copyright or related rights, as well as to require the provision of accurate contact information. Provided that these requirements are met and the response procedure established by Article 56 is followed, hosting providers are exempt from liability for the actions of their clients, thereby ensuring a balance between the protection of IP rights and the stable functioning of online platforms.

Article 58 of the Law of Ukraine “On Copyright and Related Rights” defines the liability of content-sharing service providers. This article establishes rules and liability for platforms that facilitate the exchange of large volumes of user-generated content (e.g., video hosting services, streaming platforms, social networks). If such providers do not have authorization to host copyright-protected works and fail to take sufficient measures to prevent and stop infringements, they are held liable regardless of notification. The article specifies the measures that providers must take to avoid liability, the criteria for assessing the adequacy of such actions, as well as exemptions for non-profit or small-scale platforms. Its purpose is to encourage large platforms to actively cooperate with rightsholders and to prevent piracy.

At the same time, in the field of trademark protection on the Internet, no special administrative “notice-and-takedown” mechanism has yet been established – the relevant infringements are considered within the framework of the general judicial or administrative procedure. However, under the Law of Ukraine “On Protection of Rights to Trademarks for Goods and Services” such infringements may also serve as grounds for filing a request with the platform to stop the

---

<sup>27</sup> Law of Ukraine “On Copyright and Related Rights” of 01.12.2022 № 2811-IX [Online resource]. – Available at: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>

<sup>28</sup> Law of Ukraine “On Protection of Rights to Trademarks for Goods and Services” of 15.12.1993 № 3689-XII [Online resource]. – Available at: <https://zakon.rada.gov.ua/laws/show/3689-12#Text>

unlawful use of a trademark, particularly in cases involving fake accounts, unauthorized labeling of goods, or the use of trademarks in advertising.

In this context, e-commerce platforms - especially marketplaces, social networks, and classified ad websites - can and should introduce internal procedures for reviewing complaints about trademark infringements by analogy with the procedure set out in Articles 56-58 of the Law on Copyright. Equally important is the development of preventive policies (terms of service), the obligation of users to provide accurate contact information, and the prompt moderation of content that infringes intellectual property rights. Such an approach allows for greater predictability, transparency, and speed in responding to infringements in the field of e-commerce.

Law of Ukraine "On Consumer Rights Protection"<sup>29</sup> - contains the definition of falsified products (manufactured in violation of technology or through the unlawful use of a trademark, or by copying the form, packaging, external design, as well as the unauthorized reproduction of another person's product) and prohibits the sale of such falsified goods (Article 6). This Law allows a consumer to file a complaint with the State Service of Ukraine on Food Safety and Consumer Protection (SSUFSCP) if they purchased a counterfeit product online. The Law also expands the powers of public consumer organizations - they may initiate examinations and submit proposals to terminate the sale of falsified goods (Article 25). In turn, the SSUFSCP has the authority to remove falsified products from the market, conduct inspections and sampling, impose fines, issue orders, and apply to the court regarding violations (Article 26).

Criminal law protection of intellectual property rights in Ukraine is provided, in particular, by Articles 176, 177, 229, and 231 of the Criminal Code of Ukraine<sup>30</sup>, which establish liability for:

Infringement of copyright and related rights (Art. 176);

Infringement of rights to an invention, utility model, industrial design, topography of integrated circuits, plant variety, or rationalization proposal (Art. 177);

Illegal use of a trademark, trade name, or qualified indication of the origin of goods (Art. 229);

Illegal collection with the intent to use, or the use of, information constituting commercial or banking secrecy (Art. 231).

In practice, the application of criminal law mechanisms in the field of intellectual property remains limited, which is due to the complexity of collecting evidence, including in online sales, as well as the predominant focus of law enforcement agencies on other priority areas.

This problem becomes particularly relevant in the context of the rapid development of e-commerce, where a significant share of IP infringements occurs on marketplaces, in social networks, and on specialized online trading platforms. Common practices include the sale of counterfeit goods, the unlawful use of trademarks in account names or product descriptions,

---

<sup>29</sup> Law of Ukraine "On Consumer Rights Protection" of 12.05.1991 № 1023-XII [Online resource]. – Available at: <https://zakon.rada.gov.ua/laws/show/1023-12#Text>

<sup>30</sup> Criminal Code of Ukraine of 05.04.2001 № 2341-III [Online resource]. – Available at: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

content copying, or the unauthorized use of copyrighted images and videos in online advertising.

In the field of customs control in Ukraine, the provisions of Articles 397-403 of the Customs Code of Ukraine<sup>31</sup>, apply, which regulate the rules for facilitating the protection of intellectual property rights during the movement of goods across the customs border of Ukraine.

**In particular, these articles establish the following key mechanisms:**

- Procedure for customs control and customs clearance of goods containing intellectual property items (Art. 397);
- Customs register of intellectual property items (Art. 398);
- Suspension of customs clearance of goods on the basis of the customs register data (Art. 399);
- Suspension of customs clearance of goods at the initiative of the customs authority (Art. 400);
- Early release of goods whose customs clearance is suspended on suspicion of infringement of intellectual property rights (Art. 400-1);
- Destruction of goods whose customs clearance is suspended on suspicion of infringement of intellectual property rights (Art. 401);
- Specific aspects of suspension of customs clearance and destruction of small consignments of goods moved (shipped) across the customs border of Ukraine in international postal and express items (Art. 401-1);
- Change of marking on goods and their packing (Art. 402);
- Specific aspects of customs control with respect to certain goods (Art. 402-1);
- Interaction of customs authorities with other state authorities in the field of protection of intellectual property rights (Art. 403).

These provisions are important not only for traditional trade but also in the context of e-commerce, as a significant share of online orders involves the international shipment of goods that may potentially infringe intellectual property rights. Effective work of customs in detecting and blocking the import of counterfeit products, particularly through marketplaces, helps to prevent the further spread of counterfeits on the domestic market.

Both criminal-law and customs mechanisms must adapt to the new challenges of the digital economy, including the development of specialized tools for responding to IP infringements in online sales, simplified procedures for access to digital evidence, and the establishment of

---

<sup>31</sup> Customs Code of Ukraine of 13.03.2012 № 4495-VI [Online resource]. – Available at: <https://zakon.rada.gov.ua/laws/show/4495-17#Text>

standards for cooperation between state authorities, rightsholders, and e-commerce platform administrations.

Thus, Ukrainian legislation does not yet contain comprehensive regulation of the activities of online platforms and marketplaces aimed at preventing intellectual property infringements by third parties. The absence of special procedures for content moderation, mandatory seller verification, and unified standards for responding to complaints creates increased risks for rightsholders.

At present, Ukraine is actively working on the harmonization of its legislation with that of the European Union, including the gradual introduction of elements of the Digital Services Act (DSA). The relevant changes provide for the adaptation of transparency requirements for algorithms, strengthening of content moderation, implementation of procedures for responding to infringements, and increased liability of online platforms.

The implementation of the relevant elements of the DSA, as well as the development of out-of-court dispute resolution procedures, including online mediation, are relevant directions for improving the national system of intellectual property rights protection, especially in the context of increasing volumes of trade in the online environment.

Taking into account modern challenges requires the development of new legislative approaches that allow for the effective protection of intellectual property rights in the digital environment, ensure seller verification, and create effective mechanisms of control at the platform level.

### **5.3. Platform Policies on IP Protection**

The results of the content analysis indicate a systemic absence or insufficient level of institutionalization of intellectual property protection policies on most Ukrainian online platforms. In rare cases, such policies are formally present, but they are integrated into the general terms of use or content publication rules without separate procedural support. The content of such provisions is mostly limited to declarative prohibitions on the placement of counterfeit products, while there is no description of complaint-handling mechanisms, liability of the parties, or standards of interaction with rightsholders.

This demonstrates an insufficient degree of formalization of IP policies and shows that the relevant obligations are either not considered a priority by online platforms or remain in the domain of voluntary self-regulation.

#### **Preventive Measures: Nature and Effectiveness**

In most of the analyzed cases, preventive IP protection tools are limited or purely nominal. Platforms primarily apply reactive mechanisms, including:

- manual moderation of content after a complaint is received;
- deactivation of individual listings or accounts based on a confirmed infringement;
- verification of business users at the registration stage in the form of providing basic registration documents (only on a limited number of platforms).

Automated mechanisms for pre-screening content, detecting potentially infringing listings, or keyword-based filtering algorithms are hardly ever applied. The main focus of platforms is placed on monitoring compliance with ethical norms, advertising restrictions, or safety requirements, while intellectual property rights remain at the periphery of the regulatory field.

### **Complaint Submission and Review Mechanisms**

The procedure for submitting complaints regarding IP rights infringements is generally neither unified nor standardized. About half of the analyzed platforms provide only general communication channels (feedback form, customer support email), without designating a separate category for IP-related complaints. Only a few cases demonstrate the existence of a specialized complaint mechanism that specifies the required evidence, the expected review period, and possible sanctions against the infringer.

Another persistent issue is the lack of a transparent procedure for tracking the status of a complaint, the absence of clear communication with the rightsholder, and the practical uncertainty regarding the platform's role as an intermediary between the parties to the conflict. In several cases, it is explicitly stated that disputes between users (including those concerning IP rights) must be resolved in court, without the platform's involvement.

### **Key Structural Problems**

Among the main problematic aspects identified as hindering the effective protection of IP rights on Ukrainian platforms, the following should be highlighted:

- the absence of centralized policies or regulations defining standards for interaction with rightsholders;
- minimal automation in the detection of infringements, which makes large-scale content control impossible;
- the unpredictability of complaint-handling procedures, including the lack of fixed deadlines and transparency;
- the absence of a mechanism of liability for repeat infringements;
- a complete lack of proactive monitoring: platforms do not detect infringements on their own, waiting instead for a rightsholder to file a complaint.

## **5.4. Examples of Positive Practices**

Despite the generally insufficient level of IP rights protection on online platforms, some platforms demonstrate positive dynamics. In particular:

- certain marketplaces have already adapted the basic elements of the "notice and takedown" model, which provides for the removal of content on the basis of a substantiated complaint;
- procedures for the verification of business users have been introduced, reducing the risks of anonymous trade in counterfeit goods;

- there are cases of effective cooperation with rightsholders, leading to the blocking of significant amounts of illegitimate content – especially in sensitive product categories such as branded perfumes, electronics, and clothing.

### Example: Prom.ua

Prom.ua, a large platform focusing on small businesses and operating under a marketplace model, has implemented mandatory seller verification and also conducts selective checks of licenses or certificates of conformity for certain product categories. Complaints from rightsholders are accepted through a specialized form and may result in the blocking of a seller or the removal of their product listings.

Prom.ua has introduced a transparent system of reporting and cooperation with rightsholders<sup>32</sup>. They regularly publish a Copyright Protection Report that provides statistics on removed items and processed complaints. In 2024, Prom deleted nearly one million infringing listings and reduced the average response time to 21 minutes<sup>33</sup>. This demonstrates a genuinely functioning “notice and takedown” system at the national level.

### Example: OLX Ukraine

OLX Ukraine, one of the largest classifieds platforms, has already implemented a dedicated section prohibiting intellectual property rights infringements, clearly stating the inadmissibility of posting counterfeit items. In addition, it actively moderates content and cooperates with rightsholders in removing listings that infringe copyrights or trademark rights.

Instead of passive observation, OLX Ukraine joined the educational campaign «Trust the Original»<sup>34</sup> together with the Ukrainian National Office of Intellectual Property and Innovations (UANIPIO). Within this campaign, the platform informs sellers and buyers about the dangers of counterfeiting, explains the rules, and calls on users not to sell or purchase counterfeit goods. This serves as a positive example of corporate social responsibility.

Thus, the experience of Ukrainian platforms such as Prom.ua and OLX Ukraine demonstrates the gradual integration of international approaches to intellectual property rights protection. Despite the limited level of regulatory pressure, their initiatives indicate the potential for developing internal self-regulation mechanisms and raising standards in the field of intellectual property rights protection in e-commerce.

<sup>32</sup> Prom.ua. Support Center: Copyright Protection Reports [Online resource]. – Available at: <https://support.prom.ua/hc/uk/sections/27557388464285>

<sup>33</sup> Prom.ua. Copyright Protection Report [Online resource]. – Available at: <https://support.prom.ua/hc/uk/articles/18237035925661-%D0%97%D0%B2%D1%96%D1%82-%D1%89%D0%BE%D0%B4%D0%BE-%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83-%D0%B0%D0%B2%D1%82%D0%BE%D1%80%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0-2024#:~:text=,950>

<sup>34</sup> Ukrainian National Office of Intellectual Property and Innovations (UANIPIO) and online platform OLX.UA. Campaign “Trust the Original” [Online resource]. – Available at: <https://nipo.gov.ua/ne-daj-sebe-pidrobyty/>



## Cooperation with Law Enforcement Authorities

In the field of intellectual property rights protection, cooperation between e-commerce platforms and law enforcement authorities is of particular importance. Such platforms can play an active role by providing data about sellers, assisting investigations, and cooperating in court proceedings. Although official reports do not always disclose the names of the services involved, the participation of marketplaces in detecting and halting online sales of counterfeit products represents a positive trend.

In 2024, the Economic Security Bureau of Ukraine (ESBU), together with the Cyber Police, exposed a group of individuals engaged in the illegal sale of counterfeit gadgets under a well-known brand. The counterfeit products were advertised and sold via websites, Instagram pages, and Telegram channels. Buyers were offered a wide assortment of devices, including chargers, headphones, and smartwatches. The branded goods were delivered by post throughout Ukraine. More than 4,000 counterfeit items were seized, and the rightsholder's losses were estimated at UAH 25 million<sup>35</sup>.

## 6. IP Rights Protection Tools

Online platforms and marketplaces, as key instruments of e-commerce, create both new opportunities for rightsholders and significant risks of intellectual property rights infringements. In response to these challenges, a system of legal and technical tools has been developed, encompassing both internal response mechanisms implemented by the platforms themselves and external protection measures - in particular, judicial and extrajudicial procedures. International practice confirms that properly implemented notice-and-takedown mechanisms (see study: Understanding WIPO's Role in Copyright Protection and International Enforcement, Legal IP Strategies Staff, 2024)<sup>36</sup>, administrative complaint-handling procedures, as well as alternative dispute resolution mechanisms, can ensure prompt and effective termination of intellectual property rights infringements in the digital environment.

### 6.1. Administrative Tools on Platforms

Administrative tools for the protection of intellectual property rights on online platforms are internal mechanisms that allow rightsholders or their authorized representatives to submit complaints regarding IP infringements.

Within the framework of the Digital Millennium Copyright Act (DMCA)<sup>37</sup> - the U.S. copyright law adopted in 1998 - a mechanism was established to protect online platforms from liability for user-generated content, provided they respond promptly to rightsholders' complaints. The DMCA introduced the notice-and-takedown procedure, under which a platform is obliged to

---

<sup>35</sup> Economic Security Bureau of Ukraine. ESBU and Cyber Police Exposed a Network Selling Counterfeit Gadgets under a Well-Known Brand [Online resource]. – Available at: <https://esbu.gov.ua/news/beb-ta-kiberpolitsiia-vykrly-merezhu-z-prodazhu-pidroblenoi-tekhniky-vidomoho-brendu>

<sup>36</sup> WIPO. Understanding WIPO's Role in Copyright Protection and International Enforcement, Legal IP Strategies Staff, 2024 [Online resource]. – Available at: <https://legalipstrategies.com/wipos-role-in-copyright-protection/>

<sup>37</sup> Digital Millennium Copyright Act (DMCA) of 1998, Public Law 105–304, United States Copyright Law [Online resource]. – Available at: <https://www.copyright.gov/legislation/dmca.pdf>



promptly remove or block access to content or goods upon receipt of a duly formatted complaint. These tools constitute the first and most immediate level of IP protection in the digital environment, allowing significant reduction of harm from infringements and minimizing the need to resort to judicial proceedings.

International data confirm the effectiveness of the notice-and-takedown procedure: according to a Berkeley/USC<sup>38</sup>, most requests are successful, although risks of abuse remain.

In Ukrainian practice, administrative IP protection tools on platforms are increasingly being applied in the context of marketplaces and social networks. Large marketplaces such as Prom.ua, OLX, and Rozetka have introduced mechanisms for processing rightsholders' complaints leading to the blocking or removal of counterfeit products. Similar procedures are also implemented by social networks - Meta, YouTube, and TikTok - in cooperation with Ukrainian rightsholders, which significantly increases the speed of response to infringements.

## 6.2. Judicial and Extrajudicial Protection

Judicial and extrajudicial protection of intellectual property rights remains a key mechanism in cases where administrative tools on platforms do not provide full or timely restoration of infringed rights.

The judicial mechanism of IP protection involves the rightsholder filing a claim with a competent court seeking restoration of the infringed right, cessation of the infringement, and, if necessary, recovery of compensation.

One of the main forms of such protection in Ukraine is the filing of a claim by the rightsholder for the cessation of copyright infringement and the recovery of compensation. This mechanism is provided for in Article 53 of the Law of Ukraine "On Copyright and Related Rights" and applies in cases where a copyright object - for example, a musical work, video content, software, or literary work - has been illegally used without the rightsholder's consent. In the field of e-commerce, such infringements most often occur in the form of unauthorized use of content on marketplaces, online sales platforms, streaming services, or in advertisements. Judicial protection in this case makes it possible not only to stop the infringement (by obliging removal of content, blocking a seller's account, or halting the distribution of counterfeit products) but also to recover monetary compensation from the infringer. This form of protection is an effective tool against digital piracy, the commercialization of third-party content without permission, and systematic violations within e-commerce.

Extrajudicial (alternative) protection of intellectual property rights refers to mechanisms that allow parties to resolve disputes without going to court, usually through mediation, arbitration, or other alternative dispute resolution (ADR) procedures. This approach provides flexibility, confidentiality, time efficiency, and cost reduction, while preserving business relationships between the parties. ADR procedures include:

---

<sup>38</sup> CREATE. 21 for 2021: Notice and Takedown in Copyright Intermediary Liability [Online resource]. – Available at: <https://www.create.ac.uk/blog/2021/06/25/21-for-2021-notice-and-takedown-in-copyright-intermediary-liability/>

Mediation — a bilateral or multilateral negotiation process with the involvement of a neutral third party (mediator) who assists the parties in finding a mutually acceptable solution;

Arbitration — a formal but faster and less costly alternative to court proceedings, which concludes with a binding decision of an arbitral tribunal.

According to WIPO<sup>39</sup>, in 2024 the WIPO Arbitration and Mediation Center resolved 858 intellectual property disputes, of which 77% concerned copyright and digital content. This demonstrates the rapid growth of ADR practices (an increase of 25% compared to the previous year).

In the field of domain name disputes <sup>40</sup> under the UDRP procedure, WIPO recorded over 6,000 complaints in 2023, with 93% of cases decided in favor of rightsholders.

Thus, ADR tools in the field of intellectual property are gaining increasing application. They serve as an effective complement to judicial procedures, particularly in disputes related to digital content, cooperation between platforms, and licensing agreements, contributing to the timely and efficient resolution of conflicts.

### 6.3. Cooperation with Customs and Law Enforcement Authorities

Effective combat against intellectual property rights infringements in Ukraine is impossible without close interaction between customs and law enforcement authorities. Such cooperation facilitates the timely detection and termination of illegal imports of counterfeit goods, which negatively affect the economy and the reputation of legitimate manufacturers. Customs authorities act as the first line of defense, preventing the illegal import and export of counterfeit goods that harm legitimate producers and rightsholders. Ukrainian legislation provides for mechanisms of information exchange and joint response between customs, police, prosecution authorities, and other law enforcement structures.

A key tool in this cooperation is the conduct of joint actions, customs inspections, and checks based on analytical data and reports of suspicious activity. An important aspect is also the introduction of modern monitoring and control technologies, which increases the speed and quality of responses to cases of infringement. In recent years, cooperation between agencies has significantly intensified due to the introduction of clear procedures for interaction and information exchange, which contributes to reducing the volume of counterfeit goods on the market.

An important role in this process is played by the Intellectual Property Rights Infringement Monitoring Center<sup>41</sup>, which operates under UANIPIO. The Monitoring Center performs analytical, communication, and coordination functions, provides informational support to

---

<sup>39</sup> WIPO Arbitration and Mediation Center. WIPO ADR Highlights 2024: WIPO Out-of-Court IP Dispute Resolution Services Continue to Grow [Online resource]. – Available at: <https://www.wipo.int/amc/en/center/summary2024.html>

<sup>40</sup> World Trademark Review. Recent Trends in WIPO Arbitration and Mediation [Online resource]. – Available at: <https://www.worldtrademarkreview.com/guide/the-guide-ip-arbitration/third-edition/article/recent-trends-in-wipo-arbitration-and-mediation>

<sup>41</sup> Available at: <https://nipo.gov.ua/ukr-tsentr-sposterezhenia-porushen-ip-prav/>

customs and law enforcement authorities, facilitates the detection of infringements on online platforms and marketplaces, and organizes relevant awareness-raising campaigns.

In addition, the Monitoring Center organizes events for representatives of customs, law enforcement authorities, and businesses, conducts analytical studies on the scale and trends of IP rights infringements on marketplaces, and develops expert networking in this field.

## 6.4 Online Mediation as a Modern Tool for IP Rights Protection

Given the large-scale role of marketplaces in modern e-commerce, mediation is becoming a key mechanism for the swift and effective resolution of disputes concerning intellectual property rights infringements arising in the digital environment.

Online mediation is a form of alternative dispute resolution (ADR) conducted with the involvement of a neutral intermediary (mediator) through digital platforms, without the need for a physical meeting of the parties to the conflict.

This mechanism makes it possible to effectively resolve disputes related to infringements of copyrights, patents, trademarks, or other intellectual property objects in the online environment.

Who can be parties to mediation?

Participant	Who are they?	Role in Mediation
Rightsholder	Authors, companies, IP owners	Protect their rights, initiate or participate in mediation
Seller	Online stores, entrepreneurs	Resolve issues related to the use of content or goods
Platform	Marketplaces, hosting services	Intermediaries providing a trading venue and may also be a party to the conflict
Consumer	Users, buyers	May be parties to a dispute in cases of IP rights infringement

## Why is Online Mediation Needed in the Field of IP?

Online mediation has a number of characteristics that make it an effective mechanism for alternative dispute resolution (ADR) in the field of intellectual property, particularly in the context of digitalization and the globalization of trade

### 1. Efficiency and Time-Saving

One of the key advantages of online mediation is the significant reduction in the time required to resolve a dispute. Unlike traditional court proceedings, which in cross-border disputes may last for years, mediation makes it possible to reach a compromise within days or weeks. This is particularly important in cases where delays may have direct commercial or reputational consequences (e.g., the spread of plagiarism or the sale of counterfeit goods)

### 2. Flexibility of the Procedure and Creative Solutions

Mediation is not bound by strict procedural requirements, allowing the parties to independently determine the format of communication (e-mail, video conferencing, messengers), the language of the process, as well as the timing and pace of negotiations. Moreover, the parties can agree not only on financial compensation but also on other forms of settlement, such as:

- signing a licensing agreement;
- recognition of co-authorship;
- opportunities for joint commercialization of the IP asset;
- public retraction or apology.

### 3. Economic Feasibility

Online mediation is more affordable compared to litigation. It reduces costs associated with court fees, travel, legal services, translation of documents, and filing claims in multiple jurisdictions. This makes mediation particularly attractive for small businesses, creative industries, and startups that may have limited resources.

### 4. Confidentiality

The mediation process is closed, and its results are not subject to mandatory disclosure. This enables the parties to maintain the confidentiality of commercial information, avoid public exposure of the conflict, and reduce potential reputational risks.

### 5. Possibility of Preserving Business Relations

Mediation is based on cooperation rather than confrontation. This allows parties to preserve - or even improve - their business relationships. The process creates a safe space for constructive dialogue, which in many cases not only helps to resolve the dispute but also opens up opportunities for future collaboration.

## 6. Cross-Border Accessibility

Online mediation enables the effective resolution of disputes between parties located in different countries, jurisdictions, and time zones. Its application is particularly relevant in situations such as:

- disputes between Ukrainian sellers and international platforms (e.g., Amazon, Etsy);
- infringements of rights to domain names in global zones (.com, .eu, etc.);
- unauthorized use of digital IP objects in cloud services, on websites, or in social media.

### Examples of Online Mediation in the Field of Intellectual Property in the European Union

In the European Union, online mediation is developing as a key element of the strategy to ensure the security of e-commerce and the protection of consumer and rightsholder rights in the digital environment. The EU demonstrates a systemic and multi-level approach to the implementation of alternative dispute resolution (ADR) mechanisms, particularly in the online format (ODR – Online Dispute Resolution).

#### 1. European ODR Platform

The Online Dispute Resolution (ODR) platform was established under Regulation (EU) No. 524/2013<sup>42</sup> and operates under the management of the European Commission. Its main characteristics include:

- Access to certified ADR bodies in all EU countries, as well as Iceland, Liechtenstein, and Norway.
- The platform enables the initiation of dispute resolution between consumers and online sellers in a cross-border context.
- All online shops are obliged to place a link to this platform on their websites, which encourages its active use.

This creates a transparent and accessible mechanism for resolving consumer disputes, including cases of unauthorized use of IP objects in goods or advertising.

#### 3. Proprietary ODR Systems on Marketplaces

Major trading platforms operating in the EU are actively introducing internal ODR mechanisms to resolve disputes between sellers, buyers, and third parties (including rightsholders). For example:

- eBay and similar platforms process tens of millions of disputes annually.
- The process often begins with automated negotiations between the parties.
- If the dispute is not resolved, mediation or other ADR methods with strict deadlines are offered (for instance, the option to file a claim within 30 days after the delivery of goods).

---

<sup>42</sup> Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) [Online resource]. – Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0524>

It is popular among IT companies, media businesses, and digital content platforms.

WIPO ADR has gained particular prominence in cross-border disputes concerning intellectual property rights infringements in the online space.

Mediation has been officially recognized in Ukraine: on December 15, 2021, the Law of Ukraine "On Mediation"<sup>43</sup>, adopted on November 16, 2021, entered into force. The law has a framework character: it establishes the legal status of a mediator, the procedure, requirements, and areas of application, including civil, commercial, labor, administrative disputes, as well as certain criminal cases.

Ukraine has adapted the Council of Europe's Guidelines on ODR, ensuring compliance with standards of fair trial, data protection, and related safeguards.

Government strategies for the digitalization of justice have also been approved, providing for electronic consultations, online case reviews, and digital document circulation - in particular for simplified proceedings

At present, the system of online dispute resolution in Ukraine is still at an early stage of development and does not yet function as a fully operational tool for alternative dispute resolution. Despite the general trend toward digitalization in the legal sphere, online mechanisms for resolving disputes are mostly applied in narrow areas - such as e-commerce or financial services - and lack proper regulatory support.

Nevertheless, certain initiatives aimed at launching relevant online platforms have been undertaken. In particular, some pilot projects have been implemented to test the potential of digital tools for pre-trial conflict resolution. For example, within the framework of initiatives by certain non-governmental organizations and with the support of international partners, online platforms for mediation and pre-trial settlement of disputes in the field of consumer protection have been tested.

Some freelance platforms have also introduced internal dispute resolution procedures between clients and contractors, modeled on international practices such as Upwork Dispute Resolution. However, such mechanisms have not yet become widespread and most often remain part of private services of specific platforms.

In the field of e-commerce, Ukrainian marketplaces provide users with the possibility to file complaints with the moderation service, particularly in cases of intellectual property rights infringements and other disputes. However, at present, these procedures do not include the use of formalized alternative dispute resolution mechanisms.

There are organizations that provide mediation services in an online format, including in the field of intellectual property. One such example is the Mediation Center under the Ukrainian National Office of Intellectual Property and Innovations (UANIPPIO)<sup>44</sup>, which specializes in

---

<sup>43</sup> Law of Ukraine "On Mediation" of 16.11.2021 № 1875-IX [Online resource]. – Available at: <https://zakon.rada.gov.ua/laws/show/1875-20#Text>

<sup>44</sup> Available at: <https://nipo.gov.ua/ukr-tsentr-sposterezhenia-porushen-ip-prav/>

alternative dispute resolution related to intellectual property rights using modern digital technologies.

One of the most promising areas for launching such instruments is intellectual property. In this field, conflicts often have a cross-border nature, arise in the digital environment, require prompt response, and do not always necessitate judicial intervention. At the same time, international experience demonstrates that online mediation in the field of IP can be an effective tool that combines speed, flexibility, and rights protection.

Online mediation in the field of intellectual property is not merely a convenient tool for dispute resolution but a response to the challenges of the digital era. At a time when creating an idea, product, or content has become easier than ever, the issue of their protection requires new approaches.

## 6.5. Technological Solutions and Automation

The protection of intellectual property rights in the online environment today cannot be imagined without the widespread implementation of technological tools and automated solutions. In response to the exponential growth of e-commerce, the rapid evolution of infringement methods, and the increasing reliance on organized fraudulent networks, leading global platforms are adopting advanced proactive monitoring technologies to detect, block, and prevent violations.

In particular, artificial intelligence and machine learning algorithms have become the foundation of the technological strategies of the largest e-commerce platforms. According to the Amazon Brand Protection Report 2024<sup>45</sup>, more than 99% of counterfeit listings were detected pre-publication through automated pattern recognition systems that analyze text, images, and behavioral signals. Similar approaches are deployed by other global players, including Alibaba and eBay.

An important element of current monitoring systems is the use of computer vision technology enabling the detection of image copies even when subject to partial editing. For example, Alibaba reports that its automated systems process over 200 million listings daily, identifying visual manipulations such as background alteration, cropping, or watermark addition.

To effectively combat systemic violations related to repeated account registrations, platforms are actively implementing user network analysis technologies. In particular, Amazon and eBay analyze IP addresses, payment details, devices, browser fingerprints, and behavioral patterns to detect linked accounts and prevent their reappearance after blocking. Importantly, these technologies make it possible to identify entire fraudulent networks and promptly stop their activities.

Another key component of platform strategies is the deployment of bot detection and mitigation algorithms. On many platforms, infringers use automated bots to mass-generate fake listings with minor alterations designed to bypass filters. Modern detection technologies

---

<sup>45</sup> Amazon. Amazon Brand Protection Report 2024 [Online resource]. – Available at: <https://assets.aboutamazon.com/22/3b/a9c54c7940f683f90022a3d1aaec/amazon-bpr-2024-3-21-2024-final.pdf>



allow platforms to identify such activity by flagging atypical posting patterns, thereby significantly enhancing resilience against automated abuse.

International practice increasingly focuses on blockchain-based solutions for supply chain transparency and product authentication. For instance, Nike has introduced a pilot program employing blockchain technology that enables consumers to verify authenticity through a QR code scan. The patented “CryptoKicks”<sup>46</sup>: system assigns each pair of physical shoes a unique identifier (ID) linked to a digital token in the blockchain, stored in the owner’s digital locker. This mechanism ensures authentication and records ownership rights, even in the case of resale.

Alongside the cases of Amazon, Alibaba, and Nike, a notable technological innovation was introduced by the UK company Opsydia<sup>47</sup>, which developed a unique laser process to embed tamper-proof identifiers inside the structure of diamonds. These microscopic markings (less than one micron deep) cannot be erased or altered without destroying the gemstone. Registered in blockchain-based provenance systems, such codes allow reliable tracing of a diamond’s origin, even after resale. This integration of physical marking with digital certification provides an unprecedented level of product security and traceability, already deployed in the jewelry industry and with potential application in other high-risk categories such as luxury watches, fine art, and critical components of the aviation and automotive sectors.

In practice, international platforms are also actively integrating WIPO ALERT – a specialized database of the World Intellectual Property Organization that contains a list of websites systematically infringing intellectual property rights. This enables platforms to automatically block suspicious content without the need for additional checks.

A key requirement of European regulation, in particular the Digital Services Act (DSA), is to ensure algorithmic transparency and public reporting. Platforms are obliged to regularly publish data on the number of detected infringements, response times, and the effectiveness of their moderation systems, as well as to undergo independent audits. Such practices are already implemented by Amazon, eBay, and AliExpress, which publish detailed annual reports on their anti-counterfeiting efforts.

As part of the discussions at the International IP Enforcement Summit 2025<sup>48</sup>, a number of additional technological solutions were presented that reflect the current global trends in the automation of intellectual property rights protection.

In particular, the World Customs Organization (WCO) emphasizes the introduction of AI-supported X-ray scanning and the Smart Customs Portal for parcel inspections at customs checkpoints. These solutions allow for more effective detection of suspicious goods amid the rapid growth of e-commerce, where over 70% of identified infringements are linked specifically to online trade.

---

<sup>46</sup> United States Patent and Trademark Office. US Patent No. US10505726B1. Digital Asset for Footwear [Online resource]. – Available at: <https://patents.google.com/patent/US10505726B1/en>

<sup>47</sup> Institute of Physics. Opsydia: Previous Business Awards Winners [Online resource]. – Available at: <https://www.iop.org/about/awards/business-awards/previous-business-awards-winners/opsydia>

<sup>48</sup> Available at: <https://www.euiipo.europa.eu/en/landing-pages/international-ip-enforcement-summit-2025>



Particular attention should be paid to the hybrid monitoring model of CoreSearch<sup>49</sup>, which combines automated AI analysis of textual and visual elements of product listings with mandatory human expert involvement at the final stage. This approach ensures a balance between high processing speed and the necessary quality of verification, while also allowing compliance with brand policies and legal requirements.

An interesting example is the practice of LaLiga, which has implemented its own AI platform to detect pirated broadcasts in real time, using fingerprinting technology – unique codes embedded into the video stream. Similar solutions could potentially be applied on marketplaces to tag the visual content of products in order to quickly detect counterfeits.

New directions were also discussed for the use of AI in combating piracy and counterfeit trade in cryptocurrency networks and the Darknet, particularly within the framework of the ISOP (Interpol)<sup>50</sup>.

At the same time, experts highlight the risks associated with data poisoning (the deliberate injection of false data to mislead AI) and AI hallucination (the erroneous generation of results without real evidence), which are especially relevant in the context of automated content moderation.

CounterCheck<sup>51</sup> presented the use of AI for risk analysis of goods flows in warehouses, including RFID tagging, barcoding, and the integration of blockchain technologies for supply chain traceability.

CounterCheck has developed a system that enables automatic inspection of goods in warehouses using artificial intelligence. Their technology helps detect suspicious batches of products even before they reach store shelves or online platforms.

**To achieve this, the company applies:**

- RFID tagging: special tags attached to products, enabling fast identification and verification via radio waves.
- Barcodes: standard barcodes scanned by the system to check product information.
- Blockchain: a digital ledger storing the entire history of a product's movement - from manufacturer to warehouse – which cannot be falsified.
- AI risk analysis: artificial intelligence automatically analyzes the origin of goods, delivery routes, and suppliers, cross-checking these data against official databases. If the system detects discrepancies or suspicious patterns, such goods are flagged for additional inspection.

---

<sup>49</sup> Available at: <https://corsearch.com/>

<sup>50</sup> INTERPOL. Project I-SOP: INTERPOL Stop Online Piracy. Coordinating a Global Cross-Sector Response to Digital Piracy [Online resource]. – Available at: <https://www.interpol.int/en/Crimes/Illicit-goods/Projects/Project-I-SOP>

<sup>51</sup> Available at: <https://www.countercheck.com/>

This technology allows companies and platforms to identify potentially counterfeit products already at the logistics stage, minimizing the risk of such goods reaching consumers.

A separate modern challenge is the spread of counterfeit goods through virtual influencers (CGI), digital twins, temporary stories, and private channels such as WhatsApp. This requires platforms to update algorithms and adapt to new distribution channels. Among the promising directions, the European Union is actively preparing to implement the (Digital Product Passport, DPP)<sup>52</sup>, which will become mandatory starting in 2027. This passport is expected to contain information on the product's origin, composition, environmental indicators, and other key attributes, enabling consumers and platforms to more effectively verify product authenticity.

In Ukraine, the application of such technological solutions is still at an early stage. Ukrainian marketplaces should align with international standards and gradually implement modern automation technologies, including:

- pre-publication content analysis algorithms for moderation;
- systems for identifying linked accounts through IP address, payment method, and behavioral pattern analysis;
- integration with international databases, such as WIPO ALERT;
- user behavior analysis technologies to detect fraudulent networks;
- elements of blockchain solutions for transparent supply chain control;
- regular public reporting on detected infringements and moderation performance;
- systematic training of content moderators with a focus on intellectual property rights protection.

The main challenges for implementing such solutions in Ukraine remain: the high cost of developing and maintaining proprietary technological systems, limited technical resources, the absence of regulatory obligations for public reporting, and the low level of awareness among businesses and consumers regarding the importance of transparent IP rights protection mechanisms.

Successful implementation of technological solutions by Ukrainian platforms requires a strategic vision, readiness to invest, as well as adequate state support through awareness-raising, consultations, and - in the longer term - through gradual implementation of requirements aligned with the European Digital Services Act (DSA). Such an approach will help create a safer and more competitive online environment capable of effectively countering intellectual property rights infringements.

---

<sup>52</sup> European Commission. Digital Product Passport: Overview and Next Steps [Online resource]. – Available at: [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14382-Digital-product-passport-rules-for-service-providers\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14382-Digital-product-passport-rules-for-service-providers_en)

## 6.6. Awareness, Education, and Prevention

In Ukraine, intellectual property is actively protected through a combination of educational, informational, and preventive measures. These initiatives are aimed at raising awareness among citizens, entrepreneurs, and creative professionals about the importance of protecting IP rights. UANIPIO regularly conducts educational campaigns, seminars, and webinars, fostering a culture of respect for intellectual property.

One example of effective cooperation between state institutions and business is the “Trust the Original” information campaign, initiated by the Intellectual Property Rights Infringement Monitoring Center of UANIPIO in partnership with the online platform OLX, which was mentioned earlier. The campaign focuses on informing consumers about the risks of purchasing counterfeit goods and the importance of supporting legitimate producers. It includes educational materials, publications, and other resources. Such initiatives foster conscious consumer behavior and support the development of a fair business environment in Ukraine.

Given the successful experience of cooperation with OLX within the “Trust the Original” campaign, it is advisable to recommend expanding such partnerships with other major online platforms and marketplaces operating in Ukraine. Joint information initiatives with platforms not only help increase consumer awareness but also provide added value for the platforms themselves by strengthening user trust and enhancing their reputation.

## 7. Conclusions and Recommendations

### 7.1. Research Findings

Online platforms and marketplaces play a key role in the development of modern e-commerce, simplifying market access for sellers and offering convenience for consumers. At the same time, these platforms have become the primary environment for the distribution of counterfeit products and items that infringe intellectual property rights.

**The conducted research confirms:**

- The absence of effective barriers to listing counterfeit products on many Ukrainian marketplaces.
- An insufficient level of seller verification, low transparency, and limited use of modern technological solutions for the automated detection of infringements.
- Limited application of administrative, technological, and judicial instruments for effective response to IP rights violations in the online environment.
- A high level of technical mobility and organization of fraudulent networks, which are capable of quickly adapting to blockings and circumventing existing moderation systems.

International experience (Amazon, Alibaba, eBay, Nike, Opsydia) demonstrates that the introduction of comprehensive technological solutions - including automated moderation, multi-account analysis, seller verification, blockchain and RFID tagging, as well as public reporting - represents the most effective pathway to protecting IP rights in the digital space.

The European Union, within the framework of implementing the Digital Services Act (DSA), has established new requirements for platforms regarding transparency, public reporting, and obligations to ensure the safety of the digital marketplace. Considering its European integration commitments, Ukraine must strategically move in this direction, adapting international practices and gradually harmonizing its legislation.

## 7.2. Recommendations for Online Platforms

Online platforms bear direct responsibility for the quality of content posted on their resources. They have the ability to create technical and organizational conditions that may either facilitate the spread of counterfeit products or, conversely, effectively restrict it. Therefore, the introduction of modern verification systems, automated moderation, and public reporting is a key prerequisite for developing a safe online environment.

### Recommendations:

- Implement algorithms for automated pre-publication moderation of goods to detect infringements before listings go live.
- Introduce mandatory verification of seller data through document checks, contact validation, and payment details verification.
- Establish systems for detecting linked accounts and fraudulent networks, including analysis of IP addresses, devices, payment methods, and behavioral patterns.
- Develop and publish clear rules for handling complaints, including defined review timelines and liability for non-compliance.
- Ensure regular public reporting on detected infringements, removed goods, and response times.
- Deploy technological solutions based on AI, blockchain, and RFID to strengthen product screening and prevent violations.
- Integrate platforms into international monitoring systems, such as WIPO ALERT, for timely detection of infringements.
- Consider participation in pilot projects for the implementation of the Digital Product Passport (DPP) for high-risk goods.
- Provide regular training for content moderators, particularly in identifying counterfeit products.

### 7.3. Recommendations for State Authorities

The state plays a systemic role in shaping the regulatory environment and ensuring a balance between the development of e-commerce and the proper level of intellectual property rights protection. Legislative and administrative instruments introduced by the state must set clear requirements for platforms and ensure effective coordination with law enforcement and customs authorities.

#### Recommendations:

- Establish mandatory minimum requirements for seller verification across all online platforms, with the introduction of control mechanisms.
- Define requirements for automated content moderation and provide for liability in case of non-compliance.
- Introduce mandatory public reporting by online platforms regarding the number of infringements detected, response times, and the effectiveness of moderation services.
- Strengthen inter-agency cooperation between the State Customs Service, the National Police, the judiciary, and platforms to ensure prompt response to infringements.
- Develop a regulatory framework for the implementation of the Digital Product Passport (DPP), with gradual harmonization with the requirements of the Digital Services Act (DSA).
- Step up participation in international initiatives such as I-SOP (Interpol), WCO, and WIPO ALERT for information exchange and joint actions aimed at detecting and countering infringements.
- Provide state support for the implementation of technological solutions on platforms, in particular through advisory and awareness-raising campaigns.
- Organize a capacity-building program for law enforcement officers, customs officials, judges, and platform content moderators, with a focus on IP infringements in the online environment

### 7.4. Recommendations for Right Holders and Businesses

Right holders, manufacturers, suppliers, and trading companies are the primary stakeholders in ensuring the protection of their rights. Their active participation, both in monitoring and in developing industry standards, is critically important for the effective functioning of the entire system of countering intellectual property rights infringements.

It should be noted that in Ukraine, the principle of private prosecution largely applies: initiating criminal or administrative proceedings is generally possible only upon a complaint filed by the right holder. This increases the responsibility and role of right holders in the timely detection of infringements and in taking measures to stop them.

### Recommendations:

- Regularly monitor their own brands on marketplaces and social media.
- Actively use complaint mechanisms on online platforms and track the effectiveness of their handling.
- Implement technological solutions for product marking: RFID tags, QR codes, digital certificates, and blockchain-based solutions to confirm authenticity.
- Develop in-house legal and technical brand protection teams, particularly for rapid response to infringements.
- Participate in the development of industry standards and codes of ethics in the field of e-commerce and take initiatives for self-regulation within the sector.