Scientific Innovative Center Research

INTELLECTUAL PROPERTY: PROTECTION IN MODERN CONDITIONS

Monograph

Intellectual property: protection in modern conditions

Collective monograph edited by
Volodymyr Marchenko

Estonia, 2025

International databases and directories indexing publications:

- CrossRef (DOI: 10.36690);
- Google Scholar;
- National Library of Estonia;
- The ESTER e-catalog;

Recommended for publishing by the Academic Council of the Scientific Center of Innovative Research (№4 of 26.09.2025)

ISBN 978-9916-9389-5-9 (pdf)

Intellectual property: protection in modern conditions (2025). Monograph. In V. Marchenko (Ed.), Scientific Center of Innovative Research. Estonia. 208 p. https://doi.org/10.36690/IPP

The monograph examines a core challenge of the contemporary digital economy, namely how to protect and manage intellectual property under rapid technological change and the expansion of data driven environments. It analyzes the transformation of intellectual property rights under the influence of artificial intelligence, blockchain technologies, and global digital platforms, while also addressing the security challenges that the information society poses for public governance. The monograph integrates legal and technological perspectives by discussing not only contemporary legal mechanisms of protection, but also the practical use of innovative tools for registration, evidentiary substantiation, and enforcement of rights at national and international levels. Its structure consistently moves from issues of digital governance and information security, through legal and technological transformation of IP protection, to applied sectoral and procedural models, including trade secrets in corporate information flows, EU related operational IP management in digital product development, and online litigation as an enforcement pathway.

The monograph is intended for an academic and professional audience that needs a coherent, practice oriented understanding of intellectual property in the digitalized economy. It will be relevant for researchers and students working in law, public governance, and digital economy studies, as well as for legal practitioners, public officials, IT professionals, and corporate actors engaged in creating, managing, and protecting intellectual assets.

The monograph contributes an integrated framework that links doctrinal legal analysis with operational realities, emphasizing that effective IP protection today depends simultaneously on regulatory adaptability, technological instruments, evidence readiness, and enforceable procedures across jurisdictions and digital infrastructures.

Table of Contents

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Introduction

The monograph Intellectual Property: Protection in Modern Conditions examines how legal systems, public governance mechanisms, and organizational practices can secure intellectual property under conditions of accelerated digitalization, platform mediated markets, and the diffusion of advanced technologies. It proceeds from the assumption that contemporary intellectual property protection is not limited to formal registration or dispute resolution, because digital environments change both the nature of creative products and the pathways through which infringements occur. In this context, the practical effectiveness of intellectual property regimes depends on the coherence of legal norms, the availability of reliable evidence, and the capacity of institutions to enforce rights across borders and online infrastructures. At the same time, the scaling of digital production and distribution increases systemic exposure to legal and security risks, including unauthorized reuse, misappropriation of trade secrets, manipulation of digital evidence, and the emergence of new infringement modalities driven by automated tools. These premises position intellectual property protection as an integrated governance domain where law, technology, and institutional capacity must evolve together to preserve innovation incentives, fair competition, and public trust.

A central analytical focus of the monograph is that technological progress simultaneously expands the opportunities for creative and innovative activity and raises the costs of inadequate protection, since violations can be replicated at scale and disseminated instantly through digital channels. This is particularly visible in domains shaped by artificial intelligence and data intensive production, where questions arise about authorship, originality, lawful use of datasets, and the legal status of outputs generated with algorithmic support. Therefore, the monograph treats intellectual property not only as a private law category, but also as a field of regulatory coordination that includes evidence standards, procedural safeguards, and cross border enforcement capacity. It also highlights that modern protection strategies require operational instruments, such as digital traceability mechanisms, technologically informed legal expertise, and organizational policies that translate abstract rights into

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

implementable compliance routines. In this sense, digital tools are interpreted not as neutral innovations, but as instruments that can strengthen or undermine protection depending on institutional design, accountability structures, and the ability to monitor, detect, and respond to infringement in real time.

Structurally, the monograph is organized into three chapters that develop a coherent trajectory from the governance and security foundations of the data driven society to technology shaped legal transformations and, finally, to applied sectoral and procedural models of intellectual property management and enforcement. This architecture reflects the logic that intellectual property protection in contemporary conditions cannot be treated as a purely doctrinal legal field, because it increasingly depends on information security, organizational controls, and technologically competent enforcement mechanisms.

Chapter 1, *"Digital Governance and Information Security in the Data Driven Society: Public Administration and Corporate Information Protection,"* formulates the security and governance foundations of contemporary intellectual property protection. It analyses the information society of the digital era as a security sensitive environment by outlining the prevailing threat landscape and modern approaches to information storage in public governance, which clarifies how institutional vulnerabilities and data handling routines shape the protection of intangible assets. The chapter then moves from the public sector to the corporate domain and examines intellectual property protection within internal information flows, with particular attention to trade secrets, recurrent digital risks, and available remedies. By doing so, it demonstrates that effective protection relies not only on formal legal entitlements, but also on organizational controls, internal governance procedures, and disciplined information management that operationalize rights in everyday practice.

Chapter 2, *"Legal and Technological Transformation of Intellectual Property Protection in the Digital Environment,"* systematizes the ways in which intellectual property law and its protection instruments are reconfigured under conditions of rapid technological change. It examines contemporary challenges by connecting legal transformations with shifts in the technical infrastructures of

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

creation, circulation, and infringement, thereby substantiating the need for adaptive regulation and operationally viable compliance strategies. The chapter further develops an applied lens through the case of EU game developers, demonstrating how harmonization can be translated into scalable enforcement and why cross border digital industries require protection models that are implementable, repeatable, and responsive to platform based markets. In addition, it analyses the legal dimensions of blockchain use for intellectual property protection, approaching blockchain not as a universal remedy but as a technological instrument whose legal effectiveness depends on evidentiary architecture, governance design, and compatibility with established enforcement procedures.

Chapter 3, *"Sectoral and Procedural Models of Applied Intellectual Property Management and Enforcement,"* moves from general legal and technological transformations to applied contexts in which intellectual property functions as a measurable component of organizational value, professional practice, and enforcement strategy. It examines the features of intellectual property protection within corporate business reputation assessment, emphasizing international dimensions and showing how the robustness of rights protection shapes reputational capital and market trust. The chapter also analyses intellectual property management in polygraph methodology development projects through the lenses of policies, procedures, and compliance, demonstrating that specialized innovation settings require clearly articulated internal regimes for ownership allocation, confidentiality safeguards, and lawful reuse. In addition, it addresses intellectual property rights in the digital age by focusing on challenges generated by artificial intelligence and digital platforms, where questions of authorship, originality, data dependence, and platform governance complicate both protection design and practical enforcement. The chapter concludes with intellectual property protection in online litigation, outlining procedural pathways and enforcement logic that become decisive when infringements emerge in environments defined by rapid dissemination, scalable harm, and multi jurisdictional complexity.

The monograph is designed for researchers in law, public administration, and digital economy studies, as well as for practitioners who operate at the intersection of regulation,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

technology, and innovation management. It is relevant for policymakers and public sector professionals involved in designing legal frameworks and institutional procedures for protecting intellectual property in digital markets, where enforcement often requires cross sector cooperation and technologically competent oversight. For corporate managers, compliance specialists, and innovators, the book offers a consolidated perspective on how to build protection strategies that combine legal instruments with internal governance, contract design, and information security measures. For legal professionals, it provides a logically connected view of how modern disputes and evidentiary challenges emerge online, and which procedural mechanisms are most relevant for effective enforcement. For graduate students and early career professionals, the monograph functions as an analytically consistent entry point into contemporary intellectual property protection as a domain shaped by technological transformation and evolving governance requirements.

The internal logic of the book emphasizes that modern intellectual property protection is successful when it ensures both innovation enablement and legal reliability, rather than when it only expands the formal scope of rights without enforceable mechanisms. In this sense, the contribution of the monograph consists in treating intellectual property protection as a governance system that requires alignment between substantive norms, technological realities, and institutional capacity. A further contribution lies in linking the protection of intellectual assets with information security, corporate practices, and digitally mediated enforcement procedures, thereby demonstrating that the maturity of intellectual property regimes is inseparable from the quality of digital evidence, organizational discipline, and cross border legal coordination. Through this integrative perspective, the monograph supports applied decision making by showing how conceptual legal principles can be translated into operational instruments for prevention, monitoring, and enforcement.

The directions for further research derived from the monograph's problem field concern, first, the development of methodological criteria for evaluating originality, authorship, and lawful use in contexts where creative products are produced with

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

algorithmic assistance and where training data governance becomes legally salient. Second, future studies should deepen the analysis of evidentiary standards and procedural fairness in online litigation, particularly in cases involving digital traceability, platform responsibility, and the admissibility of technologically generated proof. Third, longitudinal research is needed to evaluate how blockchain based and other digital registry instruments affect enforcement effectiveness, transaction costs, and trust in rights attribution under real market conditions. Comparative research across jurisdictions remains essential, because intellectual property protection depends on the interaction between national legal traditions, supranational harmonization, and institutional capacity for cross border cooperation. In addition, the monograph's attention to corporate information flows suggests a research agenda on trade secret governance, including the balance between transparency requirements, employee mobility, cybersecurity safeguards, and the proportionality of restrictions. Finally, the digital governance perspective motivates further work on platform mediated markets, where enforcement involves a complex mix of private ordering, administrative oversight, and judicial protection, and where resilience depends on institutional learning and adaptable regulatory design.

Chief editor of the monograph
Prof., Dr., Volodymyr Marchenko

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Chapter 1
Digital Governance and Information Security in the Data-Driven Society: Public Administration and Corporate Information Protection

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Section 1.1. Digital-Age Information Society: Security Threats and Modern Methods of Information Storage in Public Governance

Volodymyr Marchenko[1]

[1]*Doctor of Science (Law), Professor, Professor of the Department of Law Enforcement, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-1921-3041*

Citation:
Marchenko, V. (2025). Digitalization of Public Administration: Conceptual Foundations, Institutional Change, and Implementation Policy. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 10-26). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-10-26

Abstract. *The rapid expansion of digital technologies has transformed information into a strategic resource that underpins modern public governance and socio-economic development. In the context of the information society, public authorities increasingly rely on electronic document management systems, which intensifies risks related to data integrity, confidentiality, availability, and long-term preservation. These challenges are particularly acute for states undergoing digital transformation and legal harmonisation with European standards, including Ukraine. The aim of this study is to provide a comprehensive analysis of information security as a fundamental element of public governance in the digital age, with particular emphasis on the legal regulation and technological support of electronic document management and long-term electronic archiving. The research methodology is based on an integrated use of formal-legal, comparative-legal, system-structural, and interdisciplinary methods. Ukrainian legislation is analysed in comparison with European Union regulatory frameworks and international standards in the field of information security. The study also draws on doctrinal analysis, synthesis, and generalisation, as well as the evaluation of practical experiences related to electronic governance and the application of advanced technologies, including blockchain and distributed ledger systems. The main results demonstrate that information security in electronic document management constitutes a multidimensional phenomenon encompassing legal norms, institutional arrangements, organisational practices, and technological solutions. The study identifies systemic shortcomings in Ukraine's regulatory and institutional framework, including fragmentation of legal regulation, insufficient interoperability of information systems, and limited mechanisms for ensuring long-term integrity of electronic records. At the same time, European experience illustrates the effectiveness of coherent regulatory models and specialised institutional structures. The study substantiates that while blockchain technologies offer significant potential for enhancing transparency and data integrity in public registries, their use in long-term archival storage remains limited at the current stage of technological and legal development. The findings support the need for an integrated approach to strengthening information security aligned with European standards.*

Keywords: *information society; information security; public governance; electronic document management; electronic archives; digital transformation; e-government; legal regulation; European Union standards; blockchain; distributed ledger technologies; data integrity; confidentiality; availability; cybersecurity.*

ISBN 978-9916-9389-5-9 (pdf)

1. The conceptual foundations of the information society. The concept of "information society" appeared in the process of scientific study of changes in the life of society, which began to manifest themselves with the onset of the last third of the last century, especially at the turn of the 20th and 21st centuries. The dominance of information and knowledge in the functioning and development of various spheres of social life (material production, employment and social structure, professional activity and lifestyle, culture, communications, etc.) is the basis of these changes. These changes have affected almost all spheres of social life. Thus, in the economic sphere, information products and services in recent years have begun to play a key role in the gross domestic product. In the political sphere, the availability of information related to state activities and political processes expands the possibilities for establishing effective feedback between the authorities and the population, which contributes to the development of social initiatives and civil society.

In the post-industrial era, information has rapidly evolved into a decisive strategic asset that shapes political, economic, and social development. Its quantitative and qualitative characteristics are constantly transforming: new forms of data emerge, the number of communication channels multiplies, and technological innovations continuously alter how information is produced, transmitted, stored, and consumed. As digital infrastructures expand, the circle of users who depend on information resources grows exponentially, increasing society’s general dependence on their stability and security.

These profound changes have generated a wide spectrum of institutional challenges. Modern states must confront declining public trust, rising financial burdens associated with the maintenance of state registers, and the difficulty of managing enormous and ever-growing data repositories. Additional risks stem from targeted information attacks, vulnerabilities within digital systems, and the possibility of losing or compromising data through fraud, theft, manipulation, or unauthorized access. Such challenges demonstrate that information security is not merely a technical issue, but an essential structural component of governance in the information society.

Furthermore, the work seeks to explore the institutional and procedural foundations of secure electronic document exchange and long-term digital archiving within the public sector, recognizing these processes as integral components of effective governance in the digital age. Special attention is devoted to assessing the potential of blockchain and related distributed-ledger technologies as innovative tools capable of enhancing transparency, reliability, and protection against unauthorized data manipulation. By

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

integrating these analytical dimensions, the study aspires to formulate a holistic approach to information-security policy that aligns with international standards while addressing the specific needs and vulnerabilities of the Ukrainian state.

The conceptual foundations of the information society have been shaped through several decades of interdisciplinary research. Although the term "information society" was formally introduced into scholarly discourse by Y. Hayashi in 1969, its intellectual origins can be traced to the broader sociological and technological transformations of the mid-twentieth century (Hayashi, 1969). Japanese theorists played a pivotal role in defining the paradigm: K. Koyama proposed one of the earliest systemic visions of an information-based societal model, while I. Masuda's seminal work "The Information Society as a Post-Industrial Society" provided a theoretical bridge between the ideas of post-industrialism and the emerging digital reality (Masuda, 1980). Masuda, along with Western futurists such as A. Toffler and J. Naisbitt, significantly influenced subsequent debates concerning the economic, political, and cultural implications of accelerated technological development (Toffler, 1980; Naisbitt, 1982).

By the early 1990s, the notion of the information society had entered mainstream academic and policy discourse, acquiring a central place in analyses of global digitalization and public governance reforms. Modern scholarship increasingly emphasizes that the evolution of the information society is inseparable from the rise of complex ICT infrastructures, high levels of digital interconnectedness, and the exponential growth of electronic data production. Researchers such as D. Tapscott, A. Tapscott, M. Swan, and M. Walport have contributed to the development of theoretical and applied perspectives on digital transformation, blockchain ecosystems, and cyber-governance, highlighting the corresponding challenges for legal regulation and public-sector modernization (Swan, 2015; Tapscott, & Tapscott, 2016; Walport, 2016).

Within the Ukrainian context, the literature reflects growing interest in adapting international approaches to national conditions. Ukrainian scholars – including O. Danilchenko, D. Dubov, and O. Karpenko – have examined various dimensions of digital governance, cyber resilience, and technological innovation in public administration (Danilchenko, 2017; Dubov, & Dubova 2006). Their work emphasizes the necessity of aligning national frameworks with European standards, especially given Ukraine's strategic course toward EU integration. The Concept for the Development of E-Government in Ukraine and related policy documents recognize the long-term preservation of electronic documents, the interoperability of

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

information systems, and the protection of state information resources as priority areas requiring scientific justification and regulatory development (Concept, 2010).

Despite these initiatives, the literature identifies persistent systemic weaknesses. Scholars consistently draw attention to regulatory fragmentation, insufficient standardization of digital archival procedures, and the absence of unified mechanisms for validating electronic documents over extended timeframes. The Draft Green Paper on E-Government in Ukraine further underscores the lack of legally defined protocols for electronic archiving, authenticity verification, and the preservation of documents submitted by service users – shortcomings that impede the expansion of electronic public services and complicate cross-institutional cooperation (Green Paper, 2014).

A substantial body of research also focuses on the broader global trends that redefine information-security frameworks. The rapid diffusion of information and communication technologies, digitization of administrative interactions, and transition to electronic document workflows have led to the accumulation of unprecedented volumes of digital data. This intensifies concerns about ensuring the confidentiality, integrity, availability, and sustainability of electronic assets. Scholars argue that the solution to these challenges increasingly depends on the adoption of advanced technological instruments, among which blockchain is considered one of the most promising due to its decentralized architecture, tamper-resistant mechanisms, and suitability for maintaining immutable records.

International literature on blockchain applications in the public sector is expanding rapidly. Studies demonstrate its potential for establishing transparent audit trails, reducing transaction costs, preventing unauthorized modifications, and ensuring long-term data integrity. However, researchers also highlight technological immaturity, scalability limitations, legal uncertainties, and unresolved issues related to personal-data protection (e.g., GDPR's right to be forgotten) as significant barriers to large-scale governmental deployment. These debates are particularly relevant for Ukraine, where blockchain has been proposed as a mechanism for modernizing state registries, optimizing electronic service delivery, and enhancing anti-corruption efforts.

In summary, the reviewed literature reveals a continuously evolving research field situated at the intersection of information-society theory, digital governance, and cybersecurity studies. While considerable progress has been achieved globally and nationally, scholars highlight enduring gaps – most notably in legal harmonization, institutional coordination, and the

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

establishment of reliable mechanisms for the long-term preservation and protection of electronic documents. These unresolved issues substantiate the need for further theoretical elaboration and empirical investigation, thus positioning the current study within the broader scientific effort to develop resilient, future-oriented models of information security in public administration.

2. The Information Society and Information Security as Objects of Legal Regulation. Information security, in its broad conceptualization, may be described as a multifaceted system of legal norms, technological safeguards, and organizational practices intended to forestall any improper interaction with data – whether this concerns unauthorized access, manipulation, falsification, or destruction. Under the Law of Ukraine *On Information*, the notion of *information* encompasses an extensive array of data and knowledge that may be fixed on material carriers or expressed digitally. In practical circulation, this category spans verbal and written messages, symbolic representations, digital outputs, and the results of automated computational processes.

Despite the longstanding scholarly attention accorded to the phenomenon of information, the dynamics of contemporary digitalization require a continuous reconsideration of its defining characteristics. This reassessment is necessary to enhance the reliability, operability, and rational utilization of information resources. As information is deployed across virtually all domains of public life – political, economic, social, and cultural – the prevention of its unauthorized disclosure has become an essential condition for protecting individuals, institutions, and the state from adverse consequences.

Information may be regarded as adequately protected only when the system within which it circulates is fortified against the entire spectrum of internal and external risks. Statistical assessments indicate that the majority of incidents relate to personal data and payment-information breaches, comprising roughly four-fifths of known cases. Accordingly, contemporary information-security policy is inherently preventive: it prioritizes the anticipation of vulnerabilities and the mitigation of risks before they culminate in material damage.

From a functional perspective, information security is frequently defined as the set of procedures designed to ensure the lawful use, transmission, and storage of data. Threats to data integrity – regardless of their provenance – possess the potential to disrupt broader social or international interactions and to inflict harm on specific individuals or entities.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

In this sense, information protection constitutes a regulated system of legal, technical, and organizational tools directed at controlling the conditions under which data may be accessed, processed, or disseminated. These mechanisms are built into information systems and operate through intertwined administrative and technical measures designed to prevent interference with the integrity and stability of the information environment.

Information security has also evolved into an independent field of scientific inquiry. Its principal objective is to ensure the continuity and stability of information resources while guaranteeing the rights and freedoms of individuals and society at large. Any intrusion – deliberate or accidental – into an information system may result in disclosure, distortion, or loss of data, which necessitates a structured methodology for identifying the objects requiring protection, assessing internal and external threat factors, and selecting the methods capable of mitigating such threats.

Traditionally, the foundational components of information security include **availability**, **confidentiality**, and **integrity** of data and of the infrastructure upon which it relies. The need to prevent unauthorized access remains the most intensively regulated dimension of this triad.

Availability refers to the capacity of legitimate users to access required information without excessive obstacles. Restrictions may apply in instances where disclosure would adversely affect individuals or state institutions. In everyday practice, banking services, utilities payments, transportation ticketing systems, and other digital services exemplify resources that must remain broadly accessible.

Integrity presupposes the maintenance of data accuracy and consistency. This requirement encompasses both the preservation of the initial data state and the prevention of improper alteration during operational processes. Breaches of integrity often entail significant social or economic consequences.

Confidentiality limits access to data to entities legally authorized to work with it. This principle is deeply embedded in legal doctrine and often regulated by specialized legislation governing the handling of personal, organizational, or state information.

In Ukraine, the relevance of information security has increased markedly due to the rapid integration of the country into the global digital environment. The establishment of a national information society – where technological development largely determines administrative, economic, and social processes – requires a coherent and systematic approach to information-security regulation. This imperative corresponds to

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

constitutional provisions that identify human dignity, life, and security as paramount social values.

The modern information society is defined by the ability of individuals to generate, access, exchange, and apply knowledge. Its overarching purpose is to create conditions that allow for the full realization of human intellectual capacities. Scholarly literature commonly identifies three broad models of the information society: European, American, and Asian.

The ***European model*** is distinguished by the significant role of public institutions and international organizations. The European Union invests considerable resources into forming a unified digital space, ensuring the protection of civil rights, developing inclusive digital infrastructure, and promoting technological entrepreneurship. A defining feature of this model is the diversity of national strategies shaped by geopolitical factors and varying degrees of technological advancement.

The ***American model*** is predominantly market-oriented, with technological development led by private enterprises. The state's primary function is to regulate competition and support large-scale initiatives rather than to exercise direct operational control over digital transformation.

The ***Asian model***, by contrast, is characterized by coordinated interactions between state institutions and corporate actors, with an emphasis on wide accessibility of digital services and their integration into everyday social practices.

Ukraine, in aligning itself with global developments, has pursued the construction of its own model of the information society, supported by legislative initiatives such as the National Informatization Program and a growing body of norms regulating electronic resources, digital document management, and information protection. The expansion of the domestic ICT sector provides a favorable foundation for further technological evolution.

As Ukraine continues harmonizing its legislation with European standards, it becomes imperative to analyze foreign approaches to information security, adapt them to national needs, and develop a coherent strategy for strengthening the domestic security framework. Although scholarly interest in this topic is steadily growing, Ukraine still lacks a unified doctrinal assessment of legal mechanisms for ensuring information security considering EU best practices.

3. European Union Standards and Comparative Models of Information Security. European experience in the field of information security offers a comprehensive and conceptually mature framework that has been shaped through several decades of regulatory, institutional, and

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

technological development. As early as the beginning of the 1990s, European states recognised information security as a distinct area of public policy and legal regulation. One of the first milestones in this process was the adoption of the European IT Security Criteria, which articulated fundamental objectives of information protection, including the prevention of unauthorised access, destruction, alteration, or disclosure of data. These early standards laid the groundwork for a systematic approach to securing information systems used in both the public and private sectors.

Further conceptual consolidation occurred with the adoption of the Information Technology Security Evaluation Criteria (1996), which formally established the now-canonical triad of information security: confidentiality, integrity, and availability. This triad has since become the cornerstone of European and international information-security doctrine, shaping subsequent legislative instruments, technical standards, and administrative practices. Its significance lies not only in defining security objectives but also in providing a common conceptual language for regulators, public authorities, and technology providers.

A major policy breakthrough was achieved with the European Commission's communication Network and Information Security: A European Policy Approach (2001), which framed information security as a shared responsibility of states, private actors, and civil society. This document outlined a set of strategic priorities, including the enhancement of public awareness, the establishment of unified early-warning and incident-response systems, support for secure technological solutions, the development of certification and standardisation mechanisms, the strengthening of legal protection against cyber threats, and the expansion of international cooperation. Importantly, this approach marked a shift from fragmented national initiatives toward coordinated governance at the supranational level.

European Union law places particular emphasis on balancing transparency in public administration with the protection of personal data and fundamental rights. Directive 95/46/EC (1995), later replaced and significantly expanded by the General Data Protection Regulation (GDPR), introduced strict requirements regarding lawful data processing, user consent, purpose limitation, breach notification, and accountability of data controllers. These instruments substantially enhanced institutional responsibility and legal certainty, while also reinforcing public trust in digital governance mechanisms. The GDPR has become a global benchmark for data-protection regulation, influencing legislative reforms far beyond the EU.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

A comparative analysis demonstrates that EU member states achieved coherence and systematic regulation in the field of information security at an earlier stage than Ukraine. This progress is reflected in the development of precise legal terminology, comprehensive classifications of information-security threats, and stable institutional frameworks responsible for policy coordination and enforcement. National practices further illustrate the effectiveness of specialised agencies, such as Germany's Federal Office for Information Security (BSI), as well as the positive role of civil society and professional associations in promoting digital resilience, as exemplified by Poland.

In the context of the rapidly evolving global information society and the pervasive integration of information and communication technologies across all spheres of public life, information security has acquired heightened strategic significance. Ukraine's aspiration to attain full membership in the European Union necessitates alignment with European principles, norms, and standards in this domain. Of particular importance are normative instruments that directly influence the harmonisation of national legal frameworks, including Directive 95/46/EC (1995), Directive 98/34/EC (1998) on technical standards, Directive 1999/93/EC on electronic signatures (1999), Directive 2002/21/EC on electronic communications (2002), and Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January 1981).

Taken together, European regulatory and institutional approaches demonstrate viable pathways for the development of an effective and resilient national information-security system. Their selective adaptation to Ukrainian realities may significantly contribute to strengthening legal certainty, institutional capacity, and technological sustainability within public administration, thereby supporting Ukraine's broader objectives of digital transformation and European integration.

4. Electronic Document Management and Innovative Technologies in Ensuring Information Security. At the domestic level, Ukraine has identified several strategic directions for addressing information security challenges. These include the creation of a fully functional national information infrastructure and the protection of its critical elements; enhancing interagency coordination in detecting, assessing, and forecasting threats to information security, as well as in preventing such threats and mitigating their consequences; improving the regulatory and legal framework governing information security, including the protection of information resources, counteraction to cybercrime, and safeguarding of

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

personal data; strengthening law enforcement activities in the information sphere; and expanding the National System of Confidential Communications as a secure technological foundation capable of integrating geographically dispersed systems processing confidential information.

As D.V. Dubov aptly observes, information security may be conceptualised as the capacity to neutralise harmful influences emanating from various forms of social information (Dubov, & Dubova 2006). Security, in this sense, denotes either the absence of threats or the ability to shield oneself effectively from them. Accordingly, information protection within a system involves preventing unauthorised actions pertaining to information stored or processed therein. Consequently, any informational influence that produces destabilising consequences or infringes the interests of individuals, society, or the state must be regarded as threatening.

Building on this premise, the concept of information security in electronic document management may be approached as a complex system comprising the following interrelated components:

A condition in which informational risks are absent or adequately neutralized – including harm caused by inaccurate, incomplete, or untimely information; unauthorised access to state electronic resources; breaches of confidentiality, integrity, or availability; as well as espionage and cybercrime in the digital environment.

A key domain of state policy and an essential function of public administration.

A mechanism proportionates to existing information risks, ensuring the protection of the information space of e-government and the information processed within electronic document workflows through a combination of principles, methods, and technological safeguards for secure provision, transmission, use, and storage of information.

A system of organisational, administrative-legal, technical, technological, personnel, financial, and methodological measures that ensure the protection of electronic document management systems and the information they contain.

Major threats to information security include:

1) theft of information or data constituting legally protected secrets;
2) destruction of information or software necessary for data processing and systems functioning;
3) unlawful interception of information;
4) modification of data and software;
5) unauthorised use of information;
6) disruption or incapacitation of computer systems and networks;

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

7) the concealment or suppression of information affecting the interests of individuals, citizens, or society; as well as the unlawful collection or use of personal data.

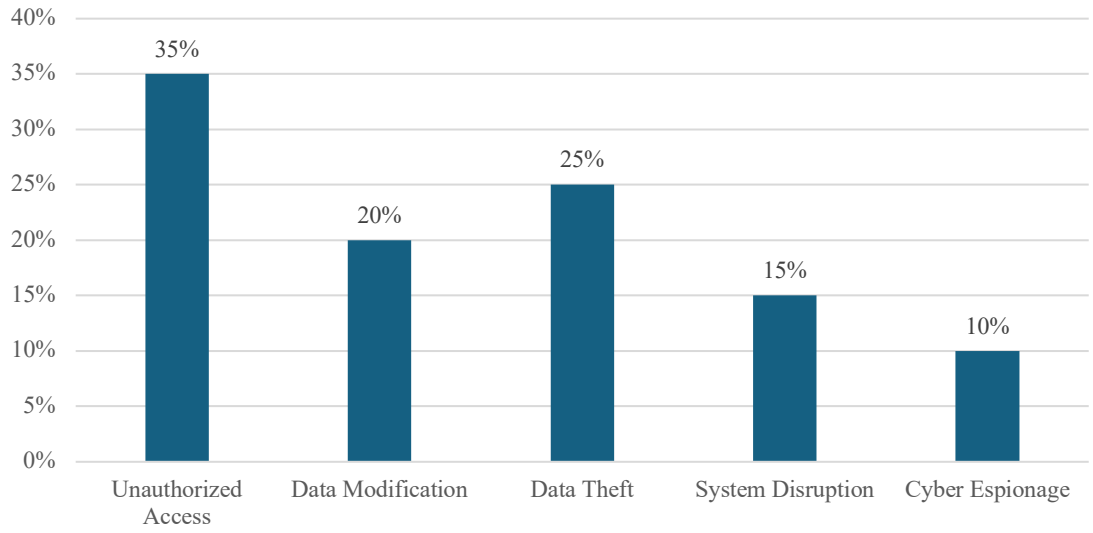

Figure 1.1. Illustrative Distribution of Information Security Threats
Source: systematized by the author

Within the framework of electronic document management in executive authorities – defined in Ukrainian legislation as the set of processes related to the creation, processing, transmission, reception, storage, use, and destruction of electronic documents carried out with verification of integrity (and confirmation of receipt where required) – one of the most problematic areas concerns ensuring the integrity of electronic documents. Ukrainian law requires that such integrity be verified, typically through examination of a digital signature that simultaneously serves as a means of authenticating the document's author.

However, as noted by I.S. Kuspliak and A.O. Serenok, evaluating electronic document management systems is complicated by numerous legislative inconsistencies surrounding their implementation and use in public administration. These inconsistencies, in our view, directly affect information security. D.S. Tymofieiev similarly asserts that electronic document systems must ensure the integrity, availability, and confidentiality of information, yet, due to their relatively recent introduction, numerous unresolved issues remain regarding the protection of data they process. Although such systems normally include built-in security features – such as role-based access controls – these measures do not eliminate risks arising from authorised users misusing confidential information. Accordingly,

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

electronic document systems must be integrated into a broader, unified information security policy rather than protected in isolation, as their security ultimately depends on the resilience of the surrounding infrastructure.

O.R. Harasym, M.V. Komova, and V.V. Lytvyn argue that a comprehensive information security system must encompass technological measures such as protection against data leakage, antivirus and antispam safeguards, vulnerability assessment, intrusion detection and prevention, firewalling, access differentiation, cryptographic protection, and continuous monitoring (Harasym, Komova, & Lytvyn, 2010).

The Law of Ukraine "On Electronic Documents and Electronic Document Management" (22 May 2003, No. 851-IV) establishes detailed procedures and requirements governing the storage of electronic documents – defined as documents in electronic form containing essential requisites and capable of being created, transmitted, stored, and converted into a visual representation through electronic means. Article 13 of the Law outlines procedures for the storage and archiving of electronic documents, including requirements for integrity verification, preservation periods equivalent to those for paper documents, duplication on multiple storage media where necessary, ensuring future accessibility and recoverability of documents, and maintaining metadata concerning their origin, purpose, and transmission.

For efficient management of documentation in public institutions, comprehensive information about all documents must be stored in institutional databases, regardless of the information medium. Incoming electronic documents typically arrive as XML files containing embedded electronic files, metadata, and requisite information. To guarantee immutability, such documents must be stored in read-only mode.

Electronic documents remain within an institution's archival system from the moment of creation or receipt until they are either transferred to a state archival facility or destroyed. Access rights to these documents – including the right to create or modify requisites – are strictly regulated based on institutional hierarchy and functional responsibilities. Moreover, documents slated for permanent or long-term storage (more than ten years) must be accompanied by paper copies created immediately after completion. Their appraisal follows the same legal principles and criteria as apply to paper-based documents.

The Central State Electronic Archive of Ukraine plays the primary role in managing state electronic archives, ensuring the preservation, accounting, and regulated use of electronic documents and information resources included in the National Archival Fund. Consequently, Ukraine possesses the essential institutional and technological prerequisites for developing an

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

effective system of long-term electronic records preservation—an indispensable component of modern e-government.

Nevertheless, as I.V. Klymenko notes, an effective unified repository must also facilitate convenient access for both public officials and citizens, irrespective of their location or time of request. The rapid growth in the volume of electronic documents underscores the urgency of developing robust mechanisms for long-term preservation and ensuring simplified access procedures.

Modern archival systems typically include tape or disk libraries, specialised server access infrastructures, data-management software, service-quality monitoring systems, and centralised backup and recovery tools. Among the most functional solutions currently used internationally are Qstar HSM (Qstar Technologies, USA) and Saperion (Saperion AG, Germany), although their high cost is a significant drawback. In Ukraine, archival institutions frequently rely on hard-disk storage supplemented by tape, optical media, or UDO-based technologies.

Over the past decade, significant technological advancements – particularly in Big Data, digital innovations, and public administration – have stimulated interest in blockchain technologies. The ISO Technical Committee TC 307 defines a distributed ledger as a registry maintained in a decentralised manner across numerous network nodes, and blockchain as a specific form of distributed ledger in which groups of verified transactions are stored in blocks linked sequentially in a tamper-resistant chain beginning with a genesis block, each block containing a hash of the preceding one.

The core idea of blockchain is the decentralised storage of records across multiple nodes, thereby eliminating the need for a single central repository. As transactions typically involve multiple parties, each participant possesses an identical copy of the relevant records. Distributed ledger technologies ensure that all copies remain synchronised and verifiable, thereby guaranteeing transaction integrity and auditability.

According to ISO experts, blockchain and distributed ledger technologies represent a significant new direction in the development of information systems, with potential applications in domains requiring trustworthy, immutable documentation without reliance on a central trusted authority. These technologies can reduce transaction costs, expand possibilities for managing electronic registries, and improve the integrity of information flows in networked environments.

O. Danilchenko argues that blockchain may be adapted to any activities involving registration, accounting, or transfer of diverse assets, regardless of the number, type, or geographic distribution of participants – developments

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

that could ultimately transform models of public governance (Danilchenko, 2017).

Potential areas of blockchain application in the public sector include electronic document management, public opinion polling, auditing of public procurement, intellectual property protection via smart contracts, energy redistribution among network users, maintenance of registries of banking guarantees, monitoring pharmaceutical supply chains, and managing patient registries in healthcare.

A distinct and highly promising application lies in public administration itself: blockchain enables the maintenance of decentralised state registries, including land-title and real-estate registries, ensuring tamper-proof recording and significantly enhancing public trust.

Conclusions. The conducted research demonstrates that the rapid digital transformation of public administration fundamentally reshapes the nature of information security and elevates it to one of the central strategic priorities for modern states. In Ukraine, where the transition toward a mature information society is closely linked with European integration, the establishment of a coherent, resilient, and technologically advanced system of electronic document management is not merely desirable but essential for democratic governance, institutional transparency, and the protection of citizens' rights.

The study reveals that despite certain institutional achievements and ongoing reforms, the Ukrainian system of electronic document management continues to face structural and conceptual challenges.

The most significant among them include:

1) deficiencies in the legal framework, manifested in the absence of a unified national strategy for information security in electronic document management, inconsistencies in the regulation of digital signatures, and fragmentation of institutional responsibilities across different executive bodies;

2) insufficient technical, technological, organisational, personnel, financial, and methodological capacities necessary to support secure and efficient document workflows;

3) lack of an integrated information infrastructure, including limited interagency interoperability, weak coordination, and insufficient oversight mechanisms;

4) the absence of protective mechanisms proportionate to existing information risks, particularly with regard to safeguarding integrity, confidentiality, and availability of electronic records across their life cycle;

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

5) a high level of inherent information risks, including cybercrime, industrial espionage, unauthorised access, fraudulent manipulation of data, and the vulnerability of electronic networks and state systems to external interference or internal misuse.

These problems inhibit the development of digital public services, undermine trust in electronic governance systems, and create barriers to the effective functioning of the state. Addressing them is therefore critical for enhancing the overall quality, transparency, and accountability of public administration.

The research also highlights the considerable advantages of electronic archives, including higher levels of information security, reduced risks of document deterioration or loss, improved retrieval speed, multiuser access to shared resources, and the possibility of remote use - features that collectively make them indispensable for the modern executive branch. At the same time, their successful deployment depends on sustained investments in infrastructure, personnel training, and legal harmonisation with EU standards.

A separate focus of the study concerns the potential of blockchain and other distributed-ledger technologies. These technologies offer promising opportunities for enhancing the integrity, transparency, and accountability of state registries, as well as for reducing transaction costs and increasing trust in public information systems. However, their successful implementation in e-government requires the fulfillment of several critical preconditions: the creation of a legally robust procedure for recording data in public registries; clear definition of access rights; adoption of multi-factor biometric identification systems; global synchronisation of datasets; and development of validation mechanisms for user interfaces and system-level interactions. Challenges include limited technological maturity, high implementation costs, legislative constraints, lack of specialized personnel, and insufficient institutional support.

Moreover, blockchain technology, despite its transformative potential, is currently ill-suited for the long-term archival preservation of legally significant documents – particularly those requiring guaranteed authenticity over intervals exceeding ten years. Its application in this field is associated with substantial legal and technical risks, especially given emerging concerns related to quantum computing and changes in cryptographic standards. Therefore, blockchain solutions should presently be considered primarily for short- and medium-term document management processes, supported by a robust regulatory and judicial framework.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Taken together, the findings of this research underscore that information security in electronic document management is not a narrowly technical problem, but a multidimensional phenomenon that encompasses legal regulation, institutional design, administrative capacity, technological infrastructure, and human factors. The development of an effective national information-security system requires an integrated approach that simultaneously strengthens the regulatory framework, modernizes technological capacities, fosters interagency coordination, and introduces innovative digital solutions where they demonstrably increase resilience and trust. In the long term, aligning Ukrainian practices with European Union standards, combined with selective adoption of advanced technologies such as blockchain, will significantly enhance the reliability and transparency of public administration. Ultimately, this will contribute to the broader goals of democratic governance, rule of law, and integration into the European and global information space.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. 100 mist – krok vpered. Monitorynh vprovadzhennia instrumentiv elektronnoho uriaduvannia, yak osnovy nadannia administratyvnykh posluh v elektronnomu vyhliadi [100 Cities – A Step Forward. Monitoring the Implementation of E-Governance Tools as the Basis for Providing Administrative Services in Electronic.
2. Concept for the Development of E-Government in Ukraine. (2010). URL: http://zakon2.rada.gov.ua/laws/show/2250-2010-%D1%80/ed20110926
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.108. [E-resource]. – Access mode: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
4. Danilchenko, O. (2017). Blokchejn: yurist iz mashiny [Blockchain: Lawyer in the Car]. [YURIST&ZAKON. 2017. № 21]. URL: http://uz.ligazakon.ua/magazine_article/EA010438
5. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

and on the free movement of such data // Official Journal L 281. 23/11/1995. - P. 0031-0050.
6. Directive 98/34/EC Of the European Parliament and of the Council of 22 June 1998 on the laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services // Official Journal L 204. 21.7.1998. – P.37
7. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. URL: https://surl.lu/bpozhj
8. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). URL: https://surl.li/vpnsdn
9. Dubov, D. Dubova S. (2006). Osnovy elektronnoho uriaduvannia. Navchalnyi posibnyk [Fundamentals of electronic governance. Textbook]. [Kyiv: Tsentr navchalnoi literatury]. –176p.
10. Harasym, O. R., Komova, M. V., & Lytvyn, V. V. (2010). Orhanizatsiia zakhyshchenoho elektronnoho dokumentoobihu v merezhakh elektronnoho uriaduvannia [Organization of Secure Electronic Document Workflow in E-Governance Networks]. URL: https://lnk.ua/q462yyO4J
11. Hayashi Y., Johoka Shakai (1969). Hado no Shakai Kara Sofuto no Shakai e [The Information Society: From Hard to Soft Society]. Tokyo: Kodansha Gendai Shinso, 1969. 209 p.
12. Law of Ukraine “Pro elektronni dokumenty ta elektronnyi dokumentoobih” [On Electronic Documents and Electronic Document Management] (2003). (No. 851-IV). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
13. Marchenko V. V. Elektronne uriaduvannia v orhanakh vykonavchoi vlady: administratyvno-pravovi zasady [Electronic Governance in Executive Bodies: Administrative and Legal Basis] : Monograph / V. V. Marchenko. – Kharkiv: Panov, 2016. – 444p.
14. Marchenko, V.. The Evolution of Information Security Framework in Ukraine: European Integration and Legal Perspectives. In *International conference on Economics, Accounting and Finance*. Retrieved from https://conf.scnchub.com/index.php/ICEAF/ICEAF-2024/paper/view/806
15. Masuda, Y. (1980). The information society as a post-industrial society. World Future Society.
16. Naisbitt, J. (1982). Megatrends: Ten new directions transforming our lives. Warner Books.
17. Swan, M. (2015). Blockchain: Blueprint for a new economy. O’Reilly Media.
18. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.
19. The Green Paper on the Electronic Governance in Ukraine. URL: http://etransformation.org.ua/2014/11/24/355/
20. Toffler, A. (1980). The third wave. Morrow. URL: https://surl.li/qfsbhv
21. Walport, M. (2016). Distributed ledger technology: Beyond blockchain. UK Government Office for Science.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Section 1.2. Intellectual Property Protection in Corporate Information Flows: Trade Secrets, Digital Risks, and Remedies

Hisham Jadallah Mansour Shakhatreh[1]

[1]*Ph.D. (Law), Assistant Professor, Middle East University, Amman, Jordan, ORCID: https://orcid.org/0000-0001-8693-5744*

Citation:
Shakhatreh, H.J.M. (2025). Intellectual Property Protection in Corporate Information Flows: Trade Secrets, Digital Risks, and Remedies. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 27-43). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-27-43

Abstract. *Corporate information flows constitute the practical environment in which intellectual assets are created, refined, accessed, and exchanged across the firm and its external ecosystem, increasingly through cloud platforms and shared digital workspaces. In such settings, a significant share of high value knowledge is not designed for public disclosure or registration, so its protection depends on controlled accessibility, governance discipline, and the ability to demonstrate that discipline with consistent organizational practice. The study develops an integrated framework for protecting trade secrets in corporate information flows by linking legal protectability criteria, digital risk drivers, and remedy readiness. The chapter applies analytical and doctrinal synthesis of the trade secret protectability test and translates the legal elements into operational governance models. It operationalizes lifecycle continuity and distributed responsibility as the core mechanisms for producing "reasonable steps" evidence across creation, internal use, collaboration, third party transfer, retention, and incident response. The analysis indicates that enforceability improves when controls and proof artifacts are produced continuously across the information lifecycle rather than introduced only after an incident. It shows that secrecy governance is inherently multi actor and depends on aligned roles across executive management, legal and IP functions, information security, business owners, procurement, and users, because consistent behavior becomes part of the protectability narrative. It also demonstrates that digital risks destabilize secrecy by multiplying access points and normalizing micro disclosures across platforms and partners, which can make confidentiality handling appear inconsistent if not governed and evidenced. Corporate information flow governance should be treated as an IP control environment in which "reasonable steps" are operationalized as measurable controls that both reduce leakage probability and generate auditable proof for confidentiality preserving enforcement. Future work should validate indicator sets and evidence packs against sector specific incident datasets and quantify how evidence readiness and enforcement timing influence dispute outcomes, containment time, and trust recovery.*

Keywords: *corporate information flows; trade secrets; reasonable steps; lifecycle governance; access control; evidence readiness; cloud collaboration risk; third-party risk; confidentiality governance; incident response; enforcement readiness; digital risk management.*

ISBN 978-9916-9389-5-9 (pdf)

1. Corporate information flows as an IP control environment. Corporate information flows constitute the practical environment in which intellectual assets are created, refined, accessed, and exchanged across the firm and its external ecosystem. In modern corporations, economically valuable intangibles do not circulate only within research and development units. They also move through procurement, marketing, legal and compliance functions, customer relationship management, finance, and cross-border partner collaboration, often via cloud platforms and shared digital workspaces. This matters for intellectual property protection because a significant portion of high-value corporate knowledge is not designed for public disclosure and registration. Instead, its economic value depends on controlled accessibility, timing, contextual integrity, and the ability to demonstrate disciplined governance over who may access, use, and further disseminate it.

The legal relevance of this perspective becomes clear when trade secret protection is treated as an operational status rather than a formal label. The TRIPS Agreement establishes that undisclosed information can be protected when it is secret, commercially valuable because it is secret, and subject to reasonable steps to keep it secret (World Trade Organization, 1994). The EU Trade Secrets Directive adopts the same three-part logic and strengthens it with remedies against unlawful acquisition, use, or disclosure, including cases grounded in breaches of confidentiality and duties limiting use (European Parliament and Council, 2016). In practical terms, these standards imply that corporate information flow governance is part of the definition of the right itself. If the organization cannot show that it intentionally limited access, marked or classified sensitive content, and implemented proportionate safeguards, then enforceability becomes fragile in disputes. WIPO further emphasizes that "reasonable steps" should be calibrated to the value of the information and the risk environment, which makes managerial proportionality and documentary evidence central to defensible protection (World Intellectual Property Organization, 2019).

The concept of an "IP control environment" therefore requires two complementary capabilities. The first is legal routing, meaning that the firm can map information types to an appropriate protection posture, for example trade secret, copyright, trademark, or a hybrid structure. The second is control continuity, meaning that protections follow the information across its lifecycle from creation and internal use to collaboration, third-party transfer, retention, and disposal. Without this continuity, corporate information flows tend to produce predictable leakage points, such as over-permissive sharing links, uncontrolled copying into external tools, and unmonitored third-party

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

access, each of which weakens the secrecy and reasonable-steps conditions that trade secret protection requires (European Parliament and Council, 2016; World Intellectual Property Organization, 2019).

The table 1.1 frames information flows as a lifecycle system and identifies IP-relevant governance artifacts at each stage.

Table 1.1. Information lifecycle governance artifacts that support trade secret protectability

Lifecycle stage	Typical corporate activity	IP-sensitive artifacts in the flow	Minimum governance outputs
Creation and capture	Drafting, R&D notes, bid strategy formation	Early prototypes, draft code, negotiation playbooks	Classification decision, ownership attribution, secure authoring space
Internal use and refinement	Engineering, pricing, compliance preparation	Design files, scoring parameters, internal reports	Least-privilege access, logging, version control
Collaboration and sharing	Cross-team work, internal training	Shared folders, slide decks, templates	Approved collaboration zones, dissemination rules, watermarking where feasible
Third-party transfer	Vendors, consultants, outsourcing	SOW deliverables, datasets, model files	NDA and use limitation, audit rights, secure handoff records
Retention and disposal	Archiving, data minimization	Backups, archives, legacy repositories	Retention schedule, secure deletion, access reviews
Incident response and recovery	Containment, investigation, remediation	Forensic logs, evidence packs	Legal hold, evidence preservation, post-incident control improvement

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; World Intellectual Property Organization, 2019).

Table 1.1 indicates that secrecy is sustained when controls and evidence are produced continuously across the lifecycle, rather than being introduced only after an incident occurs.

Because information flows are multi-actor systems, role clarity is also essential for enforceability. The table 1.2 links core corporate roles to trade secret governance responsibilities that support the legal test.

Table 1.2 shows that enforceability depends on distributed responsibility, since secrecy and reasonable steps require consistent behavior across legal, technical, and operational functions.

Corporate information flows should be treated as an IP control environment because trade secret protection under international and EU standards depends on demonstrable secrecy governance, value-linked confidentiality, and reasonable steps embedded into everyday information lifecycle practices (World Trade Organization, 1994; European Parliament and Council, 2016; World Intellectual Property Organization, 2019).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 1.2. Role responsibility model for trade secret governance in corporate information flows

Role	Primary responsibility	Typical control contribution	Evidence contribution
Executive management	Risk appetite and accountability	Governance mandate and resourcing	Policies, oversight records
Legal and IP function	Legal routing and enforcement readiness	Contract templates, escalation pathways	Chain of title, legal holds, claim documentation
Information security	Control design and monitoring	Access governance, logging, DLP, incident response	Audit trails, incident records
Business unit owners	Asset definition and value justification	Crown-jewel identification, tiering decisions	Trade secret register entries, valuation rationale
Procurement and vendor management	Third-party boundary control	NDA, use limitation, audits	Vendor access reviews, audit reports
Employees and contractors	Compliance with duties	Correct use of tools and sharing channels	Policy acknowledgements, training completion records

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; World Intellectual Property Organization, 2019).

2. Digital risks that destabilize secrecy in information flows. Digital risks undermine trade secret protection primarily by weakening controlled accessibility and by expanding the number of "micro-disclosures" that, cumulatively, make confidential information functionally reachable beyond its intended boundary. In corporate information flows, this destabilization rarely results from a single technical defect. More often, it emerges from systemic organizational conditions such as fragmented identity management, permissive collaboration configurations, uncontrolled replication across cloud services, and unmanaged third-party access. These conditions are legally relevant because the trade secret test is sensitive to whether information remains non-public and not readily accessible, and to whether the holder can demonstrate reasonable steps under the circumstances (European Parliament and Council, 2016; World Intellectual Property Organization, 2019).

ENISA's threat landscape reporting describes a high-pressure environment in which disruptive incidents, data theft, and multi-stage attack patterns remain salient across sectors, and in which attacker capability and operational disruption interact with information exfiltration risks (European Union Agency for Cybersecurity, 2024). In trade secret terms, the practical issue is not only that information may be stolen, but also that confidentiality controls may appear inconsistent, informal, or poorly enforced. When that occurs, a defendant can challenge whether the information was truly protected as a trade secret or whether it became broadly accessible through

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

the owner's own permissive handling (European Parliament and Council, 2016; World Intellectual Property Organization, 2019).

A further destabilizing factor is the increasing normalization of cross-platform work patterns. Confidential materials now travel across email, enterprise chat, shared drives, ticketing systems, project wikis, and AI-enabled assistants. This creates a "boundary multiplication" effect: each additional platform becomes another place where confidentiality must be sustained through access rules, logging, retention discipline, and user behavior. In governance terms, this aligns with the NIST CSF 2.0 emphasis on organizational governance and risk management as prerequisites for effective protection, since the core challenge is consistent control across heterogeneous systems rather than isolated technical hardening (National Institute of Standards and Technology, 2024).

The table 1.3 structures the main digital risk families that destabilize secrecy and explains why each family matters for trade secret enforceability.

Table 1.3. Digital risk families that destabilize secrecy and their trade secret relevance

Digital risk family	How it destabilizes secrecy in information flows	Typical corporate manifestation	Trade secret relevance
Identity and privilege weaknesses	Expands who can access confidential assets	Shared accounts, excessive privileges, weak MFA coverage	Undercuts claims of controlled access and reasonable steps
Collaboration and sharing misconfiguration	Makes restricted content reachable via links	Public links, permissive folders, uncontrolled guest access	Can make information "readily accessible" in practice
Insider misuse and negligent disclosure	Creates direct unauthorized dissemination	Forwarding to personal email, shadow IT, screenshots	Challenges evidence of reasonable steps and supervision
Cloud and data sprawl	Multiplies copies and retention surfaces	Redundant backups, unmanaged repositories	Enlarges exposure window and weakens containment credibility
Third-party and supply chain access	Extends confidentiality boundary to outsiders	Vendors with broad access, weak use limits	Elevates the need for contractual and audit controls
Ransomware with exfiltration	Couples disruption with leakage	Double extortion, data theft from shared drives	Requires evidence readiness and fast containment
AI-assisted leakage	Moves content into tools outside boundary	Prompting with confidential data, auto-summarization	Requires proportional guardrails and demonstrable policy enforcement

Sources: (European Union Agency for Cybersecurity, 2024; European Parliament and Council, 2016; World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 1.3 indicates that the legal and operational failure mode is frequently the same: loss of boundary control. This convergence is why trade secret governance cannot be separated from digital risk governance in contemporary corporations.

A second analytical layer concerns the "flow points" where trade secrets are most likely to leak. These points tend to be routine and high-volume, which is why they are often underestimated. Training sessions, partner onboarding, cross-functional handoffs, customer escalations, and executive reporting all generate predictable disclosure pressure. In such contexts, the organization's ability to prove reasonable steps depends on whether it treated these routine flow points as controlled processes with stable rules rather than as informal exchanges (World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024).

Table 1.4. Flow points with elevated disclosure pressure and typical leakage mechanics

Flow point	Why pressure is high	Typical leakage mechanics	Governance implication
Cross-team collaboration	Speed and convenience dominate	Copying into chats, shared links, uncontrolled attachments	Require approved collaboration zones and tiered access
Vendor onboarding and delivery	Outsider access is necessary	Broad repository access, re-use across clients	Need-to-know vendor access, use limitations, audits
Customer escalation and support	Rapid problem-solving incentives	Sharing internal documents, logs, screenshots	Standardized redaction and disclosure rules
Executive and board reporting	High summarization and distribution	Forwarded decks, personal device storage	Controlled distribution, watermarking, retention discipline
Security incident response	Many parties handle evidence	Uncontrolled evidence circulation	Legal hold, evidence packs, limited access handling
AI-enabled productivity workflows	Automation encourages upload	Prompts, file ingestion into assistants	Tool governance, restricted data policies, monitoring

Sources: (European Union Agency for Cybersecurity, 2024; World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024).

Table 1.4 shows that trade secret leakage is often a by-product of legitimate work. Therefore, the decisive governance question is whether the firm designed "safe pathways" for necessary sharing that preserve confidentiality by default.

Finally, trade secret enforceability is strengthened when corporations can demonstrate measurable control performance. This does not require disclosing all internal security details, but it does require evidence that

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

protection was proportionate and consistently applied, which is consistent with WIPO's emphasis on reasonable steps as a practical management discipline (World Intellectual Property Organization, 2019).

Table 1.5. Operational indicators that support the "reasonable steps" narrative in trade secret disputes

Indicator category	Examples of measurable signals	Why it matters legally
Access discipline	Privileged access review cadence, MFA coverage, least-privilege compliance	Supports controlled accessibility claims
Sharing containment	External sharing volume, link expiry rates, DLP alert resolution time	Shows active prevention of broad accessibility
Third-party boundary control	Vendor access inventory, audit completion rate, offboarding latency	Shows enforceable boundary management
Training and policy enforcement	Completion rates, policy acknowledgements, violations handled	Demonstrates consistent secrecy culture
Incident responsiveness	Time to contain, time to preserve evidence, recurrence rate	Supports proportionality and diligence under pressure

Sources: (National Institute of Standards and Technology, 2024; World Intellectual Property Organization, 2019; European Parliament and Council, 2016).

Table 1.5 indicates that legal defensibility improves when governance is demonstrable through routine metrics and records, since disputes often turn on whether confidentiality controls were real, consistent, and proportionate.

Digital risks destabilize trade secrets mainly by multiplying access points and by normalizing informal disclosure across platforms and partners. In this environment, trade secret protection depends on demonstrable reasonable steps that preserve controlled accessibility across routine flow points, supported by governance practices and auditable indicators aligned with contemporary risk management expectations (European Parliament and Council, 2016; European Union Agency for Cybersecurity, 2024; World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024).

3. "Reasonable steps" as flow-based governance and measurable controls. The legal requirement of "reasonable steps" should be operationalized as a flow-based governance model in which confidentiality controls travel with information across its lifecycle, from creation and internal use to collaboration, third-party transfer, retention, and disposal. This approach is consistent with the TRIPS standard for protecting undisclosed information, which conditions protection on secrecy, commercial value because of secrecy, and reasonable steps to keep the information secret (World Trade Organization, 1994). The same three-part

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

logic is embedded in the EU Trade Secrets Directive, which also clarifies that unlawful use or disclosure may be grounded in breaches of confidentiality agreements or duties limiting use (European Parliament & Council, 2016).

A key implication is that trade secret protection is not only a legal status but also an evidentiary posture. WIPO emphasizes that "reasonable steps" should be treated as a practical management discipline calibrated to the organization's context, including internal and external threats, and translated into identifiable technical, physical, and documentary measures (World Intellectual Property Organization, 2019). In disputes, the central question often becomes whether the firm can show a coherent chain of actions that plausibly sustained secrecy under real operational conditions. For this reason, reasonable steps should be designed as a control architecture that simultaneously reduces leakage probability and produces durable proof artifacts, such as registers, access matrices, logs, contractual instruments, training attestations, and incident records.

The first analytical layer is the legal-to-control translation: each element of the trade secret test should correspond to a defined control family and to a standard evidence output (Table 1.6).

Table 1.6. Translating the trade secret test into control families and proof artifacts

Legal element	Operational meaning in corporate flows	Control families	Minimum proof artifacts typically expected
Secrecy	Information is not generally known and is practically restricted	Classification; segmentation; least privilege	Trade secret register; access matrix; restricted repositories
Value because of secrecy	Advantage depends on restricted accessibility	Asset valuation; crown-jewel mapping	Business rationale; criticality mapping; risk register entries
Reasonable steps	Proportionate measures under the circumstances	Governance; monitoring; training; response	Policies; acknowledgements; logs; incident playbooks and records

Sources: (World Trade Organization, 1994; European Parliament & Council, 2016; World Intellectual Property Organization, 2019).

Table 1.6 indicates that "reasonable steps" becomes legally persuasive when the organization can show structured governance and consistent outputs that make secrecy credible in practice, rather than relying on informal expectations.

A second layer is lifecycle continuity. In corporate environments, many trade secret failures arise not from the absence of controls, but from breaks

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

between stages, for example secure creation but permissive collaboration, or strict third-party terms but weak disposal discipline. A flow-based model reduces these breaks by specifying controls per lifecycle stage and by ensuring that each stage produces evidence consistent with the secrecy narrative required by TRIPS and EU law (World Trade Organization, 1994; European Parliament & Council, 2016).

Table 1.7. Lifecycle control map for trade secrets in corporate information flows

Lifecycle stage	Typical leakage mechanism	Controls that preserve secrecy	Evidence artifact that demonstrates reasonable steps
Creation and capture	Unmarked drafts and uncontrolled copies	Secure authoring spaces; confidentiality tagging	Classification records; version control logs
Internal use and refinement	Excess privilege and lateral visibility	Role-based access; least privilege; logging	Access reviews; audit trails
Collaboration and sharing	Link-based oversharing, external guests	Approved collaboration zones; DLP; link expiry	Distribution registers; DLP alerts and resolutions
Third-party transfer	Use beyond scope; vendor retention	NDA; use limitation; audit rights; secure handoffs	Signed terms; audit reports; transfer records
Retention and disposal	Data sprawl and long exposure windows	Retention schedules; secure deletion; archiving rules	Deletion attestations; repository inventories
Incident response	Evidence loss and uncontrolled disclosure	Legal hold; forensics readiness; containment playbooks	Legal hold records; sealed evidence bundles; incident timeline

Sources: (World Trade Organization, 1994; European Parliament & Council, 2016; World Intellectual Property Organization, 2019).

Table 1.7 supports a core governance conclusion: reasonable steps are most defensible when they are continuous and traceable across the lifecycle, since the legal test is sensitive to practical accessibility, not merely to intended secrecy.

The third layer is measurability and auditability. Here, cybersecurity governance frameworks help transform legal standards into repeatable management practices that can be evidenced. NIST CSF 2.0 is particularly relevant because it elevates “Govern” as a core function and emphasizes risk management roles, policies, oversight, and organizational accountability, which are precisely the elements typically scrutinized when assessing the credibility of protective measures (National Institute of Standards and Technology, 2024).

ISO/IEC 27001 defines requirements for an information security management system, and ISO/IEC 27002 provides a reference set of security

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

controls and guidance, both of which can be used to structure confidentiality controls for assets such as intellectual property and sensitive business information (International Organization for Standardization, 2022a, 2022b).

Table 1.8. Evidence-oriented metrics that operationalize "reasonable steps"

Metric domain	Illustrative indicators	Legal relevance in trade secret disputes
Access discipline	MFA coverage; privileged access review frequency; least-privilege compliance rate	Supports controlled accessibility and proportionality arguments
Sharing containment	External link volume; link expiry adoption; DLP alert closure time	Demonstrates active prevention of broad accessibility
Third-party boundary control	Vendor access inventory accuracy; audit completion rate; offboarding latency	Shows enforceable confidentiality boundary management
Policy and training enforcement	Completion rates; violation handling records; no-recording compliance	Supports consistency of secrecy governance
Incident readiness	Time to contain; time to preserve evidence; recurrence rate	Shows diligence under pressure and protects evidentiary integrity

Sources: (World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022a).

Table 1.8 indicates that reasonable steps can be strengthened when governance is demonstrable through routine indicators, since litigation often turns on whether protective measures were consistent, proportionate, and actively maintained.

A fourth and increasingly important layer concerns AI-enabled workflow risks. The normalization of generative AI tools changes the secrecy boundary because confidential content may be introduced into prompts, uploaded into assistants, or embedded into automated summarization and coding workflows. This does not automatically eliminate trade secret protection, but it raises the proportionality expectation: organizations should show that they anticipated foreseeable disclosure pathways and implemented rules and controls aligned with their risk environment, consistent with WIPO's emphasis on practical "reasonable steps" (World Intellectual Property Organization, 2019). From a governance standpoint, the NIST CSF 2.0 model is helpful because it frames tool usage as part of organizational risk governance, including policy, roles, oversight, and response preparedness (National Institute of Standards and Technology, 2024).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 1.9. AI-enabled leakage controls as part of trade secret "reasonable steps"

AI-related risk	Typical workflow pattern	Proportionate controls	Evidence artifacts
Prompt disclosure	Employees paste confidential text into prompts	Restricted-data policy; approved tools; training	Policy acknowledgements; tool approvals list
File ingestion	Uploading internal documents for summarization	Blocking sensitive classifications; DLP integration	DLP logs; classification-based blocking records
Automated code assistance	Code and secrets exposed to external services	Secure IDE policies; secret scanning; access segmentation	Scan reports; repository rules; exception approvals
Model output reuse	AI-generated text reintroduces proprietary content	Review workflow; citation and provenance rules	Review logs; publication checks
Vendor boundary risk	Third-party AI terms allow retention or reuse	Contractual clauses; data processing restrictions	Contract addenda; vendor risk assessments

Sources: (World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024).

Table 1.9 highlights that AI governance becomes part of trade secret governance when it affects the practical boundary of secrecy and the demonstrability of protective measures.

"Reasonable steps" should be treated as a flow-based, auditable control system that aligns legal requirements with lifecycle continuity, measurable governance performance, and evidence production. This approach strengthens trade secret defensibility under TRIPS and EU standards because it enables an organization to prove secrecy maintenance, proportional protection, and disciplined response, while using recognized governance frameworks as structuring devices for accountability and documentation (World Trade Organization, 1994; European Parliament & Council, 2016; World Intellectual Property Organization, 2019; National Institute of Standards and Technology, 2024; International Organization for Standardization, 2022a).

4. Remedies and evidence readiness: from containment to enforceable relief. Remedies in trade secret and mixed IP disputes depend less on the abstract availability of legal tools and more on whether the right holder can act quickly without destroying the confidentiality it seeks to protect. EU law addresses this tension through two complementary instruments. Directive 2004/48/EC establishes a baseline toolkit of civil enforcement measures, procedures, and remedies for intellectual property rights, including proportionality requirements and procedural mechanisms aimed at effectiveness (European Parliament and Council, 2004).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Directive (EU) 2016/943 builds a trade secret specific remedial architecture and explicitly requires mechanisms to preserve confidentiality of trade secrets during legal proceedings, which is critical because litigation can otherwise convert a secrecy asset into a public disclosure event (European Parliament and Council, 2016).

In parallel, the international baseline in TRIPS frames the protected interest as the ability to prevent disclosure, acquisition, or use of information contrary to honest commercial practices when secrecy, value, and reasonable protective efforts are present (World Trade Organization, 1994).

From an operational perspective, the decisive factor is sequencing. When an incident occurs, delay increases diffusion and complicates attribution, while premature disclosure can undermine secrecy status. Evidence readiness therefore functions as a standing corporate capability rather than an exceptional response task. It includes a precise definition of the protected information, traceable access governance, documented dissemination controls, enforceable third-party duties, and incident documentation that preserves chain of custody and supports proportional remedies (European Parliament and Council, 2016; World Trade Organization, 1994).

Table 1.10 summarizes the remedy toolbox and clarifies which remedies are realistically actionable depending on the type of breach and the proof posture.

Table 1.10 indicates that the same incident can yield very different legal outcomes depending on whether the organization can demonstrate both pre-incident control and post-incident discipline. This is especially true in trade secret cases because protection presupposes secrecy and reasonable efforts, and the remedial pathway often requires the claimant to define the secret with enough precision to enable adjudication without over-disclosure (World Trade Organization, 1994; European Parliament and Council, 2016).

A second issue is the interface between containment and legal action. Containment is not merely a cybersecurity task. It is a legal risk control because it limits the period in which information is accessible and it prevents additional dissemination that could be framed as “readily accessible” in practice. Legal hold procedures serve the same dual function. They prevent evidence loss and support later requests for measures that depend on credible proof, including injunctions and damages claims (European Parliament and Council, 2004).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 1.10. Remedy toolbox for trade secret and mixed IP disputes and its evidentiary prerequisites

Remedy category	Practical function	Typical legal basis in EU context	Proof posture required for effectiveness
Provisional and precautionary measures	Stop ongoing use or dissemination quickly	Enforcement framework for IP remedies (European Parliament and Council, 2004) and trade secret measures (European Parliament and Council, 2016)	Rapid evidence preservation, credible claim narrative, limited disclosure strategy
Injunctions and cessation orders	Prevent continued unlawful use or disclosure	Trade secrets: civil redress for unlawful use or disclosure (European Parliament and Council, 2016)	Defined secret scope, secrecy governance, attribution and timeline evidence
Corrective measures	Remove infringing or misappropriated materials from circulation	IP enforcement measures (European Parliament and Council, 2004); trade secret corrective measures (European Parliament and Council, 2016)	Demonstrable link between defendant materials and protected assets
Damages	Compensate for economic harm and sometimes broader prejudice	IP enforcement baseline (European Parliament and Council, 2004); trade secret damages logic (European Parliament and Council, 2016)	Harm narrative supported by financial evidence, causality, and incident records
Evidence measures and access to information	Secure proof and identify distribution or supply pathways	Procedural tools under IP enforcement (European Parliament and Council, 2004)	Early legal hold, forensic readiness, clean chain of custody
Confidentiality preservation in proceedings	Prevent court process from exposing trade secrets	Explicit confidentiality protections (European Parliament and Council, 2016)	Structured secret definition, redacted filings, controlled disclosure plan

Sources: (European Parliament and Council, 2004; European Parliament and Council, 2016; World Trade Organization, 1994).

Table 1.11 translates evidence readiness into an enforceable "proof package" that can be assembled quickly without expanding internal disclosure.

Table 11 shows that evidence readiness is primarily a governance discipline. It reduces response time and increases the feasibility of confidentiality-preserving enforcement, because the organization can file targeted claims supported by structured artifacts rather than by broad disclosures of sensitive material (European Parliament and Council, 2016).

Confidentiality preservation is the third pillar of enforceable relief. Directive (EU) 2016/943 explicitly requires Member States to ensure that parties, legal representatives, court officials, witnesses, experts, and other participants in proceedings do not use or disclose trade secrets or alleged trade secrets that they have learned as a result of participation, and it enables

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

confidentiality-preserving measures such as restricted access to documents or hearings (European Parliament and Council, 2016).

Table 1.11. Evidence readiness pack for trade secret and mixed IP incidents in corporate information flows

Evidence component	What it contains	Why it matters legally	Typical failure if missing
Secret definition file	Precise scope statement, component list, examples and exclusions	Enables the court to assess secrecy without ambiguity	Claim fails due to vague identification
Secrecy governance record	Classification policy, trade secret register entries, access matrices	Demonstrates secrecy and reasonable steps	Opponent argues lack of real protection
Access and activity logs	Authentication logs, file access history, privileged changes	Supports attribution and timeline	Unclear who accessed or when
Dissemination trail	Distribution registers, watermark identifiers, link sharing records	Proves unauthorized spread and breach scope	Diffusion cannot be reconstructed
Third-party duty documents	NDAs, use limitation clauses, audit rights, offboarding clauses	Establishes breach of confidentiality or use-limitation duties	Claim weakens against vendors and contractors
Incident record and legal hold	Incident timeline, containment actions, preserved images and snapshots	Preserves admissible proof and supports proportional relief	Evidence spoliation risk and delayed remedies

Sources: (European Parliament and Council, 2004; European Parliament and Council, 2016; World Trade Organization, 1994).

This legal design enables a practical strategy in which the claimant discloses only what is necessary to establish the protected nature of the information and the defendant's unlawful conduct, while requesting procedural safeguards to avoid collateral disclosure.

Table 1.12 summarizes the confidentiality-preserving litigation posture as a sequence of actions that align with the directive's logic.

Table 12 indicates that enforceable relief is more likely when confidentiality is treated as a procedural requirement and as a strategic constraint at every stage. This reduces the probability that enforcement actions themselves compromise secrecy, which would be legally and commercially self-defeating (European Parliament and Council, 2016).

Remedies in corporate information flow disputes are most effective when the organization combines early containment, legal hold, and structured evidence readiness with confidentiality-preserving escalation.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 1.12. Confidentiality-preserving escalation model for trade secret enforcement

Escalation step	Operational objective	Confidentiality technique	Expected legal alignment
Containment and internal segregation	Stop spread and limit internal exposure	Need-to-know incident cell, restricted repositories	Supports proportionality and secrecy discipline
Evidence preservation	Freeze facts without revealing secret broadly	Sealed evidence bundle, controlled access	Supports evidence measures and credible claims (European Parliament and Council, 2004)
Structured notice to the counterparty	Seek cessation with minimal disclosure	Describe categories and identifiers, avoid full disclosure	Reduces risk of widening dissemination
Filing with protective measures request	Enable adjudication without public exposure	Redactions, confidential annexes, limited access requests	Mirrors confidentiality preservation requirements (European Parliament and Council, 2016)
Remedy calibration	Match relief to harm and diffusion risk	Narrowly tailored injunction scope	Aligns with proportionality in enforcement (European Parliament and Council, 2004)

Sources: (European Parliament and Council, 2004; European Parliament and Council, 2016).

EU enforcement measures and trade secret specific protections provide a credible legal pathway, but outcomes depend on whether secrecy governance and proof artifacts already exist at the time of the incident, consistent with TRIPS and EU definitional requirements for undisclosed information (World Trade Organization, 1994; European Parliament and Council, 2004; European Parliament and Council, 2016).

Conclusion. Intellectual property protection in corporate information flows should be understood as a governance and control problem, not as a set of isolated legal declarations. In most corporations, the most valuable knowledge assets gain their value from controlled accessibility, timing, and contextual integrity, which means that protection success depends on how information is handled in daily operations rather than on whether a right can be registered. When sensitive knowledge moves across functions, platforms, and partners, the organization's ability to preserve confidentiality becomes the decisive condition for maintaining competitive advantage and legal enforceability. This is why classification discipline, access governance, and third-party boundary management must be treated as core IP controls that determine whether confidential information remains protectable or becomes practically reachable and therefore commercially degraded.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Digital transformation intensifies the exposure surface of confidential assets because modern work multiplies the number of flow points where disclosure can occur. Collaboration tools, cloud storage, remote work patterns, and AI-enabled productivity systems increase both the speed of dissemination and the difficulty of reconstructing where information traveled after a breach. In this environment, even small policy inconsistencies or operational shortcuts can accumulate into a pattern of permissive handling that undermines defensibility. Effective protection therefore requires continuity across the information lifecycle, beginning with creation and internal use, extending through collaboration and transfer, and ending with retention discipline and secure disposal. The strongest approach is to design "safe pathways" for necessary sharing, so that legitimate collaboration can proceed without forcing employees and partners into ad hoc practices that create uncontrolled copies.

A portfolio posture is more resilient than reliance on any single legal mechanism. Confidential information controls should be combined with protection of authored expression, enforceable contracts that define duties and use limitations, and brand or identity protections where confusion and impersonation risks exist. The practical objective is coherence: each instrument should reinforce the same boundary logic and produce compatible evidence artifacts. Evidence readiness is therefore not an afterthought but a continuous capability. Organizations that maintain precise asset definitions, traceable access records, controlled dissemination trails, and incident-ready evidence packs can respond faster, contain harm earlier, and pursue proportionate remedies without expanding exposure through unnecessary disclosure.

Ultimately, corporate information flow protection succeeds when confidentiality is operationalized as measurable behavior, supported by repeatable controls, and embedded into organizational accountability. This makes protection scalable across business units and jurisdictions, improves trust with partners and regulators, and reduces both the frequency and the impact of events that would otherwise convert intangible value into unrecoverable loss.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048
2. European Parliament and Council of the European Union. (2016). *Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance).* https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
3. International Organization for Standardization, & International Electrotechnical Commission. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements.* ISO. https://www.iso.org/standard/27001
4. International Organization for Standardization, & International Electrotechnical Commission. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: Information security controls.* ISO. https://www.iso.org/standard/75652.html
5. Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Papers, NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
6. Shakhatreh, H. (2024). Comparison of Commercial Dispute Resolution Mechanisms in Jordan and the Middle East. *Public Administration and Law Review*, (2(18), 51–66. https://doi.org/10.36690/2674-5216-2024-2-51-66
7. Shakhatreh, H. J. M. (2023). Development of E-Commerce within the Framework of Compliance with Financial Law. *Financial and Credit Activity Problems of Theory and Practice*, *4*(51), 429–439. https://doi.org/10.55643/fcaptp.4.51.2023.4123
8. Shakhatreh, H., & Ababneh, E. M. (2023). The main ways of leaking commercial secrets and measures to protect them. *Economics, Finance and Management Review*, (2), 76–82. https://doi.org/10.36690/2674-5208-2023-2-76-82
9. World Intellectual Property Organization. (2019). *Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps". WIPO Magazine.* https://www.wipo.int/en/web/wipo-magazine/articles/protecting-trade-secrets-how-organizations-can-meet-the-challenge-of-taking-reasonable-steps-41043
10. World Trade Organization. (1994). *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization).*https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Chapter 2
Legal and Technological Transformation of Intellectual Property Protection in the Digital Environment

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Section 2.1. Contemporary Challenges in Intellectual Property Protection: Legal Transformations and Technological Disruptions

Inna Kilimnik[1]

[1]*Ph.D. (Law), Associate Professor, Associate Professor of the Department of Patent Science and Fundamentals of Law Enforcement Activities, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-3225-6257*

Citation:
Kilimnik, I. (2025). Contemporary Challenges in Intellectual Property Protection: Legal Transformations and Technological Disruptions. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 45-67). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-45-67

Abstract. *The accelerated digitalisation of economic and cultural activity has fundamentally altered the conditions under which intellectual property (IP) is created, exploited, and protected. The expansion of platform-based markets, the growing role of data as an economic asset, and the deployment of artificial intelligence and distributed technologies have generated new legal risks while simultaneously challenging the conceptual foundations of traditional IP law. These processes are particularly relevant for states undergoing legal modernisation and European integration, including Ukraine, where intellectual property protection increasingly intersects with cybersecurity, digital governance, and technological innovation. The aim of this study is to analyse the contemporary challenges of intellectual property protection in the digital environment, to identify structural contradictions between technological development and existing legal frameworks, and to assess the potential of emerging technologies for strengthening legal guarantees of IP protection. The research seeks to substantiate the need for an integrated legal-technological approach to IP governance aligned with international and European standards. The study is based on a combination of general scientific, special legal, comparative-legal, and interdisciplinary methods. Formal-legal analysis is applied to national and international IP norms, while comparative methods are used to examine EU, US, and selected Asian regulatory models. System-structural analysis, case studies, and elements of technological and risk assessment are employed to evaluate the impact of artificial intelligence, blockchain, digital platforms, and cybersecurity threats on IP protection. The main results demonstrate that contemporary IP protection can no longer rely solely on classical legal doctrines. Digital transformation exposes territorial limitations of IP rights, increases vulnerability to cyber-espionage and automated infringement, and challenges concepts of authorship and originality. At the same time, technologies such as blockchain, smart contracts, digital watermarking, and AI-based enforcement tools offer significant opportunities to enhance transparency, authenticity, and rights management, provided they are supported by coherent legal regulation and institutional capacity. The findings confirm the necessity of a hybrid model of intellectual property governance combining legal harmonisation, technological safeguards, and international cooperation.*

Keywords: *intellectual property; digital transformation; copyright; patents; artificial intelligence; blockchain; cybersecurity; digital platforms; data as an asset; IP enforcement; EU harmonization; technological innovation; electronic evidence; smart contracts; legal regulation.*

ISBN 978-9916-9389-5-9 (pdf)

1. Intellectual Property Protection in the Digital Environment: Theoretical Foundations, Technological Challenges, and Contemporary Scholarly Discourse. The rapid development of digital technologies and the pervasive expansion of information and communication infrastructures have fundamentally transformed the mechanisms through which creative, scientific, and technological outputs are produced, distributed, and used. Intellectual property (IP) – historically associated with the protection of tangible artifacts and clearly identifiable authorship – has undergone profound conceptual and practical reconfiguration. In the contemporary global knowledge economy, intangible assets constitute a substantial share of national wealth, and the effectiveness of IP protection frameworks increasingly determines the competitiveness of states, industries, and individual creators. As a result, the legal discourse surrounding intellectual property has acquired heightened relevance, necessitating rigorous interdisciplinary examination that integrates jurisprudence, information technology, and cybersecurity studies.

Despite unprecedented opportunities introduced by digitalization, the modern IP landscape is characterized by complex contradictions and systemic challenges. The dematerialization of creative content, the emergence of decentralized distribution platforms, and the near-zero cost of digital reproduction have undermined the traditional assumptions underpinning IP law. Territoriality – the cornerstone of classical IP protection – has become increasingly incompatible with the global circulation of digital goods, raising questions about jurisdiction, enforcement, and harmonization of legal standards. Simultaneously, new modalities of infringement, such as unauthorized streaming, large-scale data scraping, industrial cyber-espionage, and AI-assisted content replication, require legal solutions that extend far beyond the scope of conventional doctrines.

Particular attention must be paid to the growing influence of artificial intelligence and machine learning technologies, which challenge the foundational legal categories of authorship, originality, and liability. The emergence of AI-generated works raises previously unarticulated questions concerning the boundaries of copyright protection, the legitimacy of training datasets, and the allocation of responsibility in autonomous decision-making environments. These issues underscore the need for a comprehensive reassessment of existing legal frameworks to ensure their adaptability to technological realities.

Simultaneously, the integration of digital governance instruments – blockchain registries, smart contracts, digital watermarking, and tokenized

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

asset systems – offers new opportunities for strengthening IP protection but also introduces additional regulatory dilemmas. The legal status of blockchain records, the evidentiary value of smart contracts, and the enforceability of decentralized mechanisms remain insufficiently clarified in most jurisdictions. Without a coherent and technologically informed legal framework, such mechanisms cannot fully realize their potential to enhance transparency, authenticity, and traceability of intellectual property assets.

International organizations, including WIPO, the WTO, and the European Union, have undertaken extensive efforts to modernize the global regulatory architecture. Yet the speed of technological innovation outpaces legal adaptation, resulting in persistent discrepancies between national and international standards. This is particularly relevant for countries undergoing digital transformation, where legal systems must simultaneously comply with international obligations and respond to domestic technological challenges. For states such as Ukraine, seeking integration with European normative frameworks, the modernization of IP legislation becomes a strategic imperative for economic resilience, innovation development, and harmonization with EU acquis.

Given these circumstances, the present study seeks to provide a comprehensive, legally oriented examination of the contemporary challenges facing intellectual property protection in the digital environment. The research places particular emphasis on identifying the legal contradictions arising from technological innovation, evaluating the effectiveness of existing regulatory instruments, and exploring the potential of emerging technologies for strengthening legal guarantees of IP protection. Through a combination of comparative-legal, formal-legal, and interdisciplinary methodological approaches, the study addresses both theoretical foundations and practical dimensions of modern IP governance.

By analyzing the intersections between law and technology, this research contributes to the broader academic discussion on the future of intellectual property and outlines pathways for developing a robust, adaptive, and internationally harmonized legal framework capable of responding to the complex realities of the digital age.

The study of intellectual property (IP) in the contemporary digital environment is rooted in broader theoretical reflections on the evolution of information societies. Foundational contributions by Manuel Castells (1996; 1998; 2010) introduced the notion of a “network society,” emphasizing how digital communication infrastructures reshape economic relations, governance models, and regulatory priorities. Castells’ work, together with analyses by Frank Webster (2002) and Herbert Schiller (1999), established

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

a conceptual basis for understanding how the shift toward digitized knowledge production generates new legal and institutional challenges, particularly in the domain of intellectual property protection.

Within legal scholarship, the digital transformation of IP has been examined extensively by authors who analyze the erosion of traditional enforcement mechanisms under conditions of technological acceleration. Peter Drahos (1996; 2010) and John Braithwaite (2000) highlight the global restructuring of IP governance through treaties and bilateral agreements, arguing that digital technologies simultaneously strengthen and destabilize institutional control over intangible assets. Their work demonstrates that conventional IP frameworks – largely developed for physical, territorially anchored markets –struggle to accommodate instant, cross-border dissemination of digital content.

A parallel stream of literature examines the relationship between information technologies and copyright enforcement. Ian Hargreaves' review (2011) for the UK government, along with scholarly contributions by Lionel Bently and Brad Sherman (2014), underscores the need to modernize copyright doctrines to reflect digital reproduction, platform-based distribution, and algorithmic content management. Scholars such as Rebecca Tushnet (2018) and Glynn Lunney (2001; 2018) argue that overexpansion of exclusive rights may stifle innovation, calling for balanced frameworks that incorporate public-interest safeguards and technological realities.

Further contributions in the field of digital governance and cybersecurity – particularly works by Bruce Schneier (2015), Helen Nissenbaum (2004; 2010), and Jack Balkin (2017) – demonstrate how vulnerabilities in digital infrastructures complicate the protection of IP assets. These authors note that as governments and businesses increasingly depend on electronic archives, cloud-based systems, and algorithmic management tools, risks of unauthorized access, data manipulation, and cyber-theft become central to broader legal debates. In this context, IP is not merely an economic category but a component of national information security.

The literature examining long-term preservation of electronic documents and digital evidence also demonstrates significant legal uncertainty. Studies by Anne Gilliland (2014), Luciana Duranti (2010; 2016), and Victoria Lemieux (2016) identify systemic vulnerabilities in digital archiving, stressing the difficulties posed by format obsolescence, metadata degradation, and verification of authenticity over extended periods. In recent years, Duranti and Lemieux have also examined how distributed ledger technologies may improve provenance tracking, though they

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

emphasize that such solutions require robust legal frameworks to ensure admissibility and evidentiary reliability.

In the context of technological innovation, a growing body of scholarship addresses the implications of artificial intelligence (AI) for authorship, ownership, and originality. Authors such as Ryan Abbott (2020), Andres Guadamuz (2017; 2021), and Mauritz Kop (2021) discuss how generative AI systems challenge core assumptions of IP law. They highlight unresolved issues surrounding machine-produced content, algorithmic creativity, and the legality of using copyrighted data to train models. These debates reveal deeper structural tensions between emerging technologies and doctrinal constructs originally developed to regulate human creative labor.

Recent discussions on global harmonization of IP standards also draw on the work of international law scholars such as Graeme Dinwoodie (2006; 2018), Rochelle Cooper Dreyfuss (2009), and Thomas Dreier (2017). Their analyses focus on fragmentation of digital regulation, divergence in enforcement mechanisms, and inconsistencies between national laws and multilateral agreements. They emphasize that IP protection in the digital environment increasingly relies on convergence between cybersecurity policies, data governance standards, and cross-border cooperation mechanisms.

In the Ukrainian and broader Central and Eastern European context, researchers such as Volodymyr Prylutskyi, Oksana Kachur, and Andriy Semenchenko have studied legislative adaptation processes in light of European integration. Their studies highlight gaps in digital governance, inconsistencies in national IP legislation, and the need for improved regulatory tools for managing electronic resources, digital archives, and state information systems. These works emphasize that ensuring authenticity, integrity, and long-term accessibility of electronic documents requires the simultaneous development of legal norms, technical standards, and institutional capacities.

Despite substantial contributions across disciplines, several gaps remain evident in the existing literature. First, research integrating IP law with digital archiving, blockchain-based verification, and cybersecurity remains limited, and empirical studies on state-level implementation are particularly scarce. Second, the legal implications of emerging technologies – especially automated content creation, decentralized storage architectures, and smart-contract licensing – remain under-theorized in scholarly debates. Finally, many authors note a persistent misalignment between technological innovation cycles and the pace at which regulatory frameworks adapt, resulting in persistent legal uncertainty.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Overall, the reviewed literature underscores the complexity of intellectual property protection in the digital age, revealing the need for holistic, interdisciplinary research that addresses not only doctrinal transformations but also the technical, institutional, and security dimensions shaping the contemporary IP landscape.

Intellectual property (IP) rights protect creative and technical "creations of the mind" (inventions, literary/artistic works, brands, etc.). Philosophically, IP is justified on utilitarian grounds (encouraging innovation and social progress) and on natural-rights (Lockean labor) grounds (granting creators a just reward for their work) (Stanford Encyclopedia, 2022). Personality theorists also view IP as an extension of individual character and expression. By balancing creators' rights and the public interest, IP systems aim to foster creativity and economic growth.

Below is a structured overview of the main types of intellectual property, showing what each category protects and the practical conditions that shape protection and enforcement in digital and offline environments (Table 2.1).

The each IP category protects a different asset type and therefore relies on distinct legal tests, evidence, and enforcement routes. The most important practical implication is that protection is strongest when legal instruments are matched with operational measures, such as documentation, access control, and compliance routines, especially in digitally mediated markets where infringement can scale quickly.

The international framework for intellectual property protection is built on a multilayer system of treaties and regional legal instruments that jointly define minimum standards, procedural guarantees, and enforcement expectations. At the global level, intellectual property protection is codified through multilateral agreements administered by international organizations, with the World Intellectual Property Organization serving as a key institutional platform for harmonizing basic concepts and facilitating cooperation among states. Within this architecture, Ukraine participates in core WIPO administered conventions, including instruments that structure copyright protection and related rights, and it has also joined specialized treaties that address modern requirements of copyright in the digital environment and the procedural aspects of patent law. In parallel, Ukraine's accession to the World Trade Organization in 2008 created binding commitments under the Agreement on Trade Related Aspects of Intellectual Property Rights, which functions as a baseline regime for minimum levels of protection, non discrimination principles, and enforcement standards across WTO members. As a result, Ukraine's national intellectual property system is not only a matter of domestic policy, but also an internationally

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

accountable legal field in which compliance is assessed against globally accepted benchmarks.

Table 2.1. Main Types of Intellectual Property: Scope, Protection Conditions, and Practical Enforcement Considerations

Type of IP	What it protects	Core eligibility or legal basis	Registration requirement	Typical duration (general)	Common risks in practice	Typical remedies
Patents	Technical inventions, products, processes, technical solutions	Novelty, inventive step, industrial applicability	Usually required (grant by patent office)	Often about 20 years from filing (jurisdiction specific)	Reverse engineering; invalidity challenges	Injunctions; damages; border measures; licensing
Copyrights	Literary, artistic, scientific works; software; audiovisual content	Protects original expression once fixed in a tangible form	Not required in many systems, but registration may help evidence	Often life of author plus a term (varies)	Online piracy; unauthorized adaptation; AI assisted copying	Takedowns; injunctions; damages; attribution claims
Trademarks	Brand identifiers that distinguish goods or services	Distinctiveness; non descriptiveness; likelihood of confusion analysis	Usually required (registration strengthens rights)	Renewable in many systems as long as used	Counterfeiting; cybersquatting; dilution	Opposition/ cancellation; injunctions; seizures; damages
Industrial designs	Appearance, aesthetic features of a product	Novelty or individual character (varies by regime)	Often required (design registration)	Often 5 years renewable up to a cap (varies)	Copying in fast moving markets; look alike products	Injunctions; damages; customs enforcement
Geographical indications	Origin linked quality, reputation, or characteristics	Demonstrated link between product qualities and territory	Protected via specific national or regional systems	Often indefinite while conditions are met	Misuse of names; misleading labeling	Administrative enforcement; injunctions; market withdrawal
Trade secrets	Confidential business information with commercial value	Secrecy, economic value, and reasonable protection measures	No registration, protection is practice based	Potentially indefinite while secret is preserved	Insider leakage; cyber theft; weak access control	Injunctions; damages; confidentiality orders; internal controls

Sources: (World Trade Organization, 1994; World Intellectual Property Organization, 2004; European Parliament and Council, 2004).

At the regional level, intellectual property rules are significantly influenced by European Union directives and regulations, which develop more detailed standards for the internal market and provide a high degree of normative specificity in areas such as digital use of content, intermediary responsibility, and enforcement mechanisms. For Ukraine, this regional layer has become particularly important because EU alignment is a strategic legal and institutional priority connected to the broader accession process. Harmonization in this context should be understood not as a formal copying of norms, but as a systematic process of adjusting definitions, rights scopes, limitations and exceptions, collective management rules, and procedural

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

instruments so that they operate coherently with European legal logic. A concrete illustration is the modernization of copyright regulation, where the 2022 legislative updates are oriented toward incorporating significant elements of the EU acquis and ensuring that rights protection corresponds to contemporary digital distribution models. Beyond legislation, ongoing policy dialogue with European partners focuses on further approximation to EU rules, including those governing digital content markets and the enforcement environment, which underscores that harmonization is continuous and requires consistent implementation capacity.

Taken together, these global and regional layers create the practical meaning of the "international framework" for Ukraine's intellectual property protection. The WIPO and TRIPS pillars establish the general obligations and minimum standards, while the EU dimension adds detailed regulatory solutions and institutional expectations that are particularly relevant for digital platforms, online uses of protected works, and cross border enforcement. Consequently, Ukraine's intellectual property policy operates within a structured corridor of international commitments, where reform priorities are shaped not only by domestic needs but also by the requirement to maintain compatibility with treaty obligations and regional integration goals. This configuration increases legal predictability for right holders and market participants, yet it also raises the institutional demands placed on national authorities, courts, and enforcement bodies, because harmonization must be supported by evidence standards, administrative procedures, and effective remedies. In this sense, the international framework is both a source of legal guidance and a governance mechanism that drives modernization, aligns national standards with external benchmarks, and sets measurable expectations for the effectiveness of protection in practice.

2. Digital Transformation of Intellectual Property: Platformization, Artificial Intelligence, and Emerging Legal Challenges. The Internet and new technologies have dramatically reshaped IP. Digital platforms (streaming, e-commerce, social media) enable global distribution of creative works and brands, but also raise novel legal and economic issues.

Digital markets are increasingly defined by platformization, which has structurally changed the circulation of creative content and the practical meaning of territorial rights. In many creative industries, consumption has shifted from ownership based models to continuous access through streaming and on demand services, where the same work is simultaneously exploited in multiple jurisdictions through a dense network of intermediaries. As a result, right holders must negotiate and manage licensing portfolios across dozens of platforms, each with distinct

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

contractual standards, reporting formats, remuneration rules, and content governance policies. This multiplies transaction costs and weakens the traditional assumption that distribution channels can be controlled through a limited number of local partners. It also increases legal complexity because the applicable rules for communication to the public, reproduction, and availability may be interpreted differently across jurisdictions, while the technical act that triggers use can be executed on servers located in yet another country. At the enforcement level, the platform environment introduces new asymmetries of power, since platforms may control discoverability, monetization tools, and takedown procedures. For copyright owners, the operational challenge is therefore twofold: to secure lawful access and remuneration through scalable licensing, and to preserve enforceability when unauthorized uses can be replicated and redistributed instantly. In this sense, platformization transforms copyright management from a relatively stable territorial practice into a dynamic, data dependent governance process that relies on reliable identifiers, usage analytics, and standardized contractual frameworks.

Cloud computing and virtualization further deepen this transformation by enabling intangible goods such as software, music, and datasets to be delivered as services rather than as one time transfers. When products are accessed through Software as a Service models, licensing becomes continuous and conditional, often tied to subscription parameters, user accounts, geolocation rules, and technical access controls. This changes how rights are priced, how royalties are calculated, and how compliance is monitored, because value is extracted through ongoing use rather than discrete distribution events. Cloud infrastructures also promote collaboration and co creation across borders, which can accelerate innovation but can complicate ownership allocation, version control, and evidence of authorship or contribution. At the same time, the cloud environment concentrates risk because a single breach, misconfiguration, or insider misuse may expose large volumes of proprietary information and compromise trade secrets or confidential know how. For this reason, secure delivery, access governance, auditability, and contractual safeguards become integral components of IP strategy, not merely IT concerns. In practice, rights management in cloud settings depends on the alignment of legal entitlements with technical enforcement mechanisms such as authentication, encryption, logging, and robust incident response. Consequently, the boundary between legal protection and information security becomes increasingly porous, because effective IP protection requires that digital delivery pipelines are designed to preserve both confidentiality and integrity.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Decentralized digital models, often associated with Web3 architectures and non fungible tokens, introduce an additional layer of commercialization logic focused on provenance, authenticity, and verifiable transaction histories. Tokenization enables creators and firms to attach a unique digital marker to a digital object or a representation of an asset, which can support market narratives about originality and facilitate new forms of monetization through direct to consumer distribution. However, the legal meaning of such tokens should be treated with precision: a token can function as a signal of authenticity or as a record of a transaction, but it does not automatically confer copyright or replace the underlying legal rules governing exclusive rights and permitted uses. This gap between technological representation and legal entitlement creates practical risks, including misleading claims about ownership, unauthorized tokenization of works by third parties, and disputes about what exactly is being transferred. In parallel, the rise of data driven business models has redefined data itself as a strategic intangible asset, even when raw data may not qualify for copyright protection in a straightforward manner. Curated datasets, structured databases, customer lists, and analytically valuable aggregations can be protected through a combination of intellectual property instruments, contractual arrangements, and trade secret safeguards, depending on the jurisdiction and the specific characteristics of the compilation. This makes data collection, governance, and lawful reuse central elements of IP planning, especially when datasets are used for analytics, personalization, and the training of AI systems. Overall, digitalization shifts IP management toward an integrated approach where markets, infrastructures, decentralized tools, and data governance interact, and where legal protection is effective only when it is operationally supported by scalable licensing, security controls, and credible evidence mechanisms.

Ukraine's own digital transformation aligns with these trends. The government is building AI and e-governance capabilities (e.g. an AI-driven public large language model and ePermit system) to digitize services (UANIPIO, 2025). UANIPIO (the Ukrainian IP Office) is digitizing records and integrating with international platforms (see below). These moves aim to support Ukraine's creative/innovation sectors under wartime pressures and beyond.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 2.2. Digital Transformation Trends

Trend	Legal Impact
Platformization	Cross-border licensing complexity
Cloud Technologies	Transformation of IP into service-based licensing
Web3 / NFTs	Issues of authenticity, provenance, and ownership
Data as an Asset	Expansion of database rights & trade-secret protection

Source: systematized by the author

Modern technology strains traditional IP laws. Key legal challenges include:

–*Territoriality and jurisdiction:* IP rights are inherently territorial (each country's laws apply within its borders). The Internet, however, is global. This mismatch causes conflicts: for example, an online work may infringe in one country but not another, raising thorny questions of which law applies (Xalabarder, 2002). No single global IP right exists, so creators and platforms must navigate multiple national laws. Enforcement (e.g. taking down infringing content) often requires cross-border cooperation, which is legally complex.

– *Copyright in streaming ecosystems:* The rise of streaming and on-demand services means copyright owners now license to many digital intermediaries. For instance, the music industry reports that streaming grew to ~46% of global revenues by 2014 (Rechardt, 2015). While consumers benefit from legal access, this model pressures creators to secure licensing across numerous platforms and jurisdictions. Geoblocking (restricting content by country) is common to respect territorial rights. Copyright exceptions (e.g. for "making available" in EU law) have been updated (see EU DSM Directive), but enforcement remains challenging.

– *Software and algorithm patents:* The patentability of software and algorithms is disputed worldwide. In line with EU law, Ukraine generally requires that software must produce a "technical effect" beyond a mere abstract algorithm to be patentable. (In contrast, the US historically has been more permissive, though its courts have tightened standards recently.) As digital innovation grows, countries are reconsidering how strictly to allow software patents.

–*Trademarks in online marketplaces:* Online shopping sites (Amazon, eBay, etc.) have amplified trademark issues. Counterfeit or infringing products can be sold across borders with impunity. IP owners often rely on notice-and-takedown systems or "brand registry" programs to police listings, but these can be slow or imperfect. As Ukraine integrates into global

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

commerce, ensuring trademark protection on international platforms is a growing concern.

– *AI-generated content:* AI tools (art generators, text bots) blur the line between human and machine authorship. Ukraine's 2022 Copyright Law (No. 2811-IX) addresses this by excluding purely AI-generated works from copyright. Instead, it creates a 25-year sui generis right for "non-original computer-generated" works, vested in the software's author or user (Kyrylenko, 2024). In practice, the Ukrainian IP Office has noted that only human-created parts of a work are protected by copyright (UIPO, 2024), and that AI-generated elements fall under this new right. However, the law is ambiguous (it does not clearly define who exactly holds the AI right) and differs from EU law (which has no analogous sui generis right). This creates uncertainty that Ukraine may need to resolve as it harmonizes with EU norms (Kyrylenko, 2024).

– *Digital exhaustion vs. licensing:* The traditional "first sale" (exhaustion) doctrine lets purchasers resell physical goods freely. Digital goods, however, are often licensed rather than sold. The EU holds that exhaustion applies only to copies first sold in the EEA, and courts have balked at applying exhaustion to purely digital transfers. This means consumers typically cannot legally resell digital ebooks, software licenses or streamed media. Ukraine has yet to fully tackle this debate, but as a candidate country it is closely watching EU practice (which for now favors perpetual licenses for digital content).

New technologies also introduce major risks to IP assets:

– *Cyber espionage and trade secret theft:* Industrial and military secrets are increasingly targeted by cyberattacks. Trade secrets (manufacturing processes, software code, R&D data) are especially vulnerable because their value lies in secrecy. Experts warn that cyber espionage (through phishing, malware, supply-chain hacks, etc.) is a growing threat to businesses' IP (Somal, 2025). Loss of trade secrets can erode a company's competitive advantage and trust with partners (Somal, 2025). Ukraine's wartime context makes this acute: Ukrainian defense and tech R&D must be protected from sophisticated intrusion.

– *Data breaches and IP leaks:* Large-scale data breaches (whether corporate or governmental) often expose IP assets (customer lists, prototype designs, software). For example, recent high-profile hacks (e.g. SolarWinds, Equifax) have included theft of proprietary information (Somal, 2025). Such breaches can devastate innovation-intensive industries. Strengthening cybersecurity (firewalls, encryption, employee training, etc.) is now integral to IP protection.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

– *Unauthorized copying and AI training:* The rise of web scraping and AI training has led to massive, often unauthorized copying of copyrighted works. Generative AI models today are trained on "vast troves" of data scraped from the Internet (Levi, & Ghaemmaghami, 2025). U.S. authorities have explicitly warned that using copyrighted works to train AI may be prima facie infringement (Levi, & Ghaemmaghami, 2025). Many copyright owners have launched lawsuits against AI companies for such unauthorized use. This highlights a new digital risk: automated extraction of IP for algorithmic use, potentially on a scale beyond any manual infringement.

– *Deepfakes and authenticity attacks:* Advances in AI allow creation of highly realistic synthetic media ("deepfakes"), where faces, voices or entire scenes can be fabricated. This technology threatens the authenticity of audiovisual IP. KPMG reports that deepfakes are becoming easy to produce, enabling fraud and disinformation (McGowan, 2025). For IP, a deepfake could be an unauthorized imitation of an artist's style, or a fake advertisement misusing a trademark. Defenses (digital watermarking, blockchain provenance, strict verification) are being developed, but the threat to brand integrity and media trust is real.

– *Digital archives and DRM weaknesses:* Archival and preservation systems must cope with format obsolescence, data decay, and even war-related destruction. Ukraine's libraries and archives, like others, face challenges keeping digital collections accessible long-term. Additionally, existing DRM (digital rights management) technologies, used to prevent copying, have limitations: they can often be cracked or bypassed by determined users. Thus, creators cannot rely solely on DRM; they need legal and institutional safeguards as well.

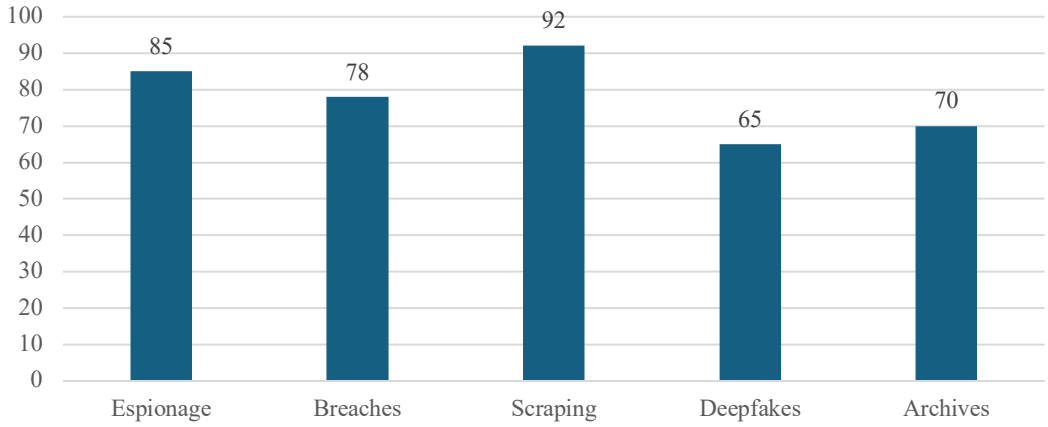

Figure 2.1. Illustrative Severity of Digital IP Threats

Source: systematized by the author

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Artificial intelligence simultaneously disrupts and empowers intellectual property systems because it changes both the production of creative outputs and the institutional routines through which rights are attributed, managed, and enforced. The most visible disruption concerns originality and authorship, since generative models can produce text, images, music, and code that resemble human created works while blurring the boundary between human contribution and automated generation. This situation forces legal systems to clarify whether originality is anchored in the final expression, in the human decision making embedded in prompts and curation, or in demonstrable authorial control during editing and selection. In Ukraine, the current approach treats purely AI generated outputs as non copyrightable and relies instead on a sui generis solution that links protection to the software author or user, reflecting a cautious position grounded in the requirement of human originality (Kyrylenko, 2024). Comparable controversies persist internationally, including debates about whether and when model training on copyrighted works constitutes infringement, and how courts should treat AI assisted outputs that contain varying degrees of human involvement (Levi & Ghaemmaghami, 2025). For Ukraine, the EU integration trajectory intensifies the practical significance of these questions because doctrinal compatibility with European principles, including the emphasis on a human author, must be aligned with workable rules for hybrid creative workflows that are already standard in digital markets (Kyrylenko, 2024).

A second cluster of issues relates to bias, transparency, and ownership in AI mediated creativity and innovation. Because models learn from large scale datasets, they may reproduce embedded biases, which can affect creative recommendations and cultural representation, raising concerns about fairness and the distribution of visibility in digital cultural markets (UNESCO, 2021). At the same time, explainability constraints complicate IP governance because it can be difficult to reconstruct how a specific output was generated, to distinguish lawful influence from unlawful reproduction, or to assess whether protected elements were reproduced in legally relevant ways (UNESCO, 2021). Ownership questions remain unsettled as well, since AI outputs emerge from interactions among developers, data providers, users, and platforms, while traditional IP categories were designed for more linear production chains. Within this context, the legality of upstream data practices becomes a central compliance issue, since the legitimacy of downstream outputs cannot be separated from whether training and input materials were lawfully acquired and used. This principle is also reflected in Ukrainian institutional positions that emphasize compliance with

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

international IP standards and the use of authorized training data in national level AI development (UANIPIO, 2025).

At the enforcement level, AI strengthens institutional capacity by enabling scalable monitoring and detection tools in environments where infringements can occur at high volume and speed. Content recognition techniques, including audio fingerprinting, image hashing, and automated similarity detection, support the identification of unauthorized copies and trademark misuse, and they increasingly inform platform level screening and administrative workflows. However, AI assisted enforcement also introduces governance risks, particularly regarding accuracy, proportionality, and procedural fairness, because automated takedowns can generate false positives and may restrict lawful uses if appeal mechanisms and transparency are insufficient (UNESCO, 2023). These tensions motivate the gradual development of standards and regulation at international and regional levels, including ethical guidance that stresses respect for IP and transparency regarding AI generated content (UNESCO, 2021, 2023). In the European context, the emerging AI regulatory framework increasingly intersects with IP through transparency and documentation expectations, which affects how right holders may identify and assert interests in datasets used for training (European Union, 2025). In Ukraine, professional guidance similarly emphasizes that AI deployment should be organized in a manner consistent with copyright compliance and responsible data practices, especially for organizations integrating AI into content production and digital services (IT Ukraine Association, 2025). Overall, the direction of change suggests that effective IP governance under AI will depend on combining doctrinal rules with auditable data governance, transparent workflows, and due process safeguards that preserve enforceability while protecting rights and legitimate uses (Kyrylenko, 2024; UNESCO, 2023).

3. Technological Instruments, Comparative Regulatory Models, and Strategic Directions for Strengthening Intellectual Property Protection in the Digital Age. To protect intellectual property in the digital era, rights holders and public institutions increasingly combine legal instruments with technical methods that strengthen evidence, automate transactions, and enable scalable monitoring. A central direction is blockchain based authorship verification, where the work itself is not published on chain, but a cryptographic hash is recorded together with a time stamp. This approach creates a durable proof that a specific digital object existed at a certain time, and it supports priority claims without disclosing confidential content, which is especially valuable for early stage designs, drafts, and other sensitive materials (Rose, 2020). In practical terms, a

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

designer can generate a hash of a design file and anchor it in a blockchain record, thereby obtaining an immutable reference that can later be compared to the original file if a dispute arises. Such mechanisms are conceptually aligned with institutional solutions that provide trusted time stamping services for digital evidence, including WIPO initiatives oriented toward proof of existence and integrity.

A second direction concerns smart contracts as a licensing and royalty administration instrument. Smart contracts can execute predefined conditions automatically, which allows licensing terms to be embedded into a transaction logic rather than enforced only through ex post monitoring. In theory and in limited practice, this can support automated royalty distribution, time stamped proof of use, and standardized recording of licensing events across multiple market participants. Importantly, the legal value of smart contract records depends on the quality of governance around them, including the reliability of identifiers, the legal recognition of digital evidence, and the ability of courts or registries to interpret blockchain based logs as meaningful proof. WIPO oriented expert discussions emphasize that time stamped blockchain evidence can help demonstrate trademark or copyright use and reduce evidentiary friction, although it does not eliminate the need for legal qualification and procedural safeguards (Rose, 2020). Therefore, smart contracts should be treated as an operational tool that can strengthen compliance and documentation, not as a replacement for substantive legal rules.

Digital watermarking and fingerprinting represent another major group of technical methods, especially relevant for platforms that distribute audio visual content at scale. Watermarking embeds hidden identifiers into media files, enabling tracing of copies back to a source or a licensing origin, while fingerprinting derives a unique signature from the content itself and can recognize the same work even after certain transformations. Together with structured metadata and content identification systems, these techniques allow automated detection of unauthorized uploads, impersonation, and some forms of derivative misuse. Their value is practical rather than purely doctrinal, because they translate a legal right into a measurable signal that can be monitored across platforms and jurisdictions. At the same time, the governance challenge lies in accuracy and dispute handling, since automated matching may generate false positives and requires transparent procedures for contesting claims and restoring lawful uses.

Tokenization of IP assets, including NFTs and other blockchain tokens, has introduced an additional commercialization layer focused on provenance, authenticity narratives, and new trading formats. In this model,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

a token linked to a digital artwork can function as a certificate of authenticity or as a market instrument enabling new forms of monetization, including experiments with fractional participation in revenue streams. However, tokenization does not itself create intellectual property rights, and it does not automatically transfer copyright or trademark ownership. The underlying rights remain governed by applicable IP law and by the contractual terms between the creator, the platform, and the buyer. Consequently, tokenization is best understood as a mechanism for organizing transactions and signaling authenticity, while legal certainty still requires explicit licensing terms, clear scope of permitted uses, and enforceable identification of the right holder.

Finally, long term protection in digital environments requires interoperability and preservation as strategic priorities. Digital works, registries, and evidence files are vulnerable to format obsolescence and platform lock in, which can undermine both cultural preservation and enforceability if records cannot be accessed or verified over time. Therefore, IP systems increasingly depend on open standards, cross platform access, and the ability to exchange records between national and international databases. Interoperability is not only a technical concern, because it affects administrative reliability, evidentiary continuity, and the capacity to support cross border enforcement. From this perspective, initiatives that integrate national IP data infrastructures with global databases respond to a structural need: without interoperable standards and preservation planning, registries face cumulative risks of fragmentation, loss of auditability, and reduced trust in the integrity of rights records.

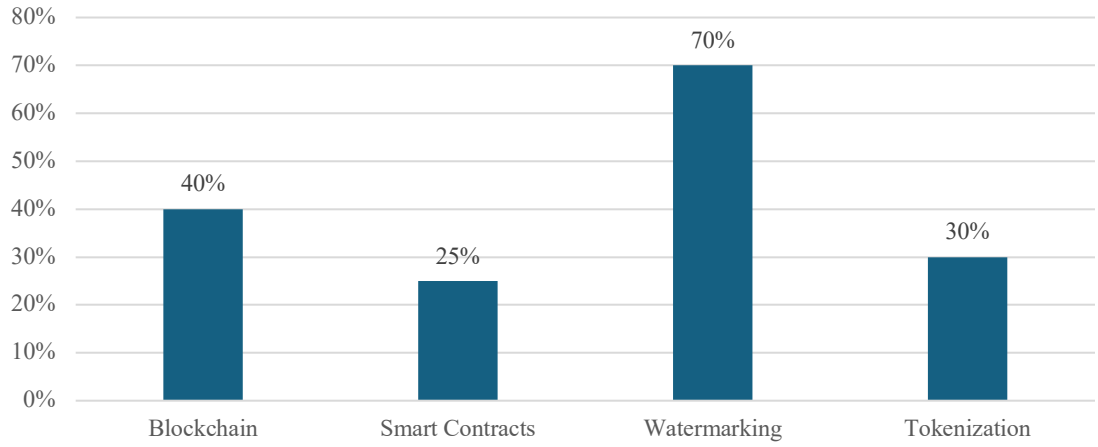

Figure 2.2. Illustrative Adoption of Technical Methods for IP Protection in the Digital Era

Source: systematized by the author

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Different jurisdictions approach digital intellectual property through distinct legal philosophies and institutional designs, which shape how rights are created, limited, and enforced in platform mediated markets. In the European Union, digital IP governance is anchored in a comprehensive acquis that combines harmonized substantive rules with sector specific enforcement instruments. Contemporary EU copyright policy has expanded both regulatory expectations for online intermediaries and the architecture of exceptions, including mechanisms relevant to text and data mining and to new neighboring rights constructs, while enforcement policy is supported by dedicated instruments that structure remedies and cross border coordination in the internal market (European Parliament & Council, 2019; European Parliament & Council, 2004). In parallel, platform governance reforms have increased the practical significance of notice and action systems, transparency duties, and accountability expectations for online services, which affects the operational environment in which IP enforcement occurs (European Parliament & Council, 2022). Because Ukraine has defined EU accession as a strategic trajectory, approximation to these rules is not only a matter of policy preference, but also a pathway toward compatibility with EU market standards, institutional routines, and enforcement expectations (Savchuk & Tsurkan, 2025).

The United States relies on a different balancing mechanism, where the flexible doctrine of fair use functions as a central tool for resolving conflicts between exclusive rights and socially valuable uses, including research, commentary, and certain transformative practices. This approach differs from the EU model, which generally uses a more enumerated system of exceptions and limitations, and it tends to produce greater legal adaptability to new technological contexts, although with higher uncertainty because outcomes are often case specific. In digital markets, this flexibility is frequently invoked in debates about AI development, training practices, and innovative reuse, where actors argue that certain unlicensed uses can be justified as transformative or necessary for technological progress (Levi & Ghaemmaghami, 2025). For Ukraine, the comparative lesson is not that one model should be replicated wholesale, but that harmonization choices involve trade offs between predictability and flexibility, as well as between ex ante clarity and ex post adjudication. Since the EU vector remains central for Ukraine, the practical challenge is to align with EU standards while preserving workable space for innovation and research within the boundaries of European legal logic (Kyrylenko, 2024).

In several Asian jurisdictions, policy strategies have been explicitly framed around innovation capacity, cultural industries, and global

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

competitiveness, with strong state supported institutional infrastructures. Japan's strategic emphasis on legal frameworks suited to the AI and digital era, alongside active promotion of cultural exports such as gaming and animation, illustrates a model where IP policy is closely linked to industrial strategy and international market positioning (Li, 2025). South Korea's institutional focus on technology transfer and a patent intensive ecosystem demonstrates how procedural efficiency and strong linkages between R&D, commercialization, and rights management can create a competitive advantage, particularly in technology dense sectors. Singapore, as an IP services hub, exemplifies another variant: a highly efficient enforcement environment combined with support instruments that treat IP as a financeable asset and a component of investment attractiveness. These approaches share a common emphasis on rapid adjudication, institutional specialization, and globally oriented IP services, which can inform Ukraine's reconstruction and modernization goals by highlighting the value of procedural capacity, sectoral targeting, and support for creative and high technology ecosystems (Savchuk & Tsurkan, 2025).

For Ukraine, the overarching strategic lesson is that digital IP governance must combine international integration with national resilience priorities and innovation needs. Recent reforms already reflect convergence with international best practices and EU alignment, yet the next phase requires moving from formal transposition to consistent implementation, institutional capability, and operational tools that function under real enforcement constraints (Savchuk & Tsurkan, 2025). A particularly sensitive domain is AI generated and AI assisted creation, where Ukraine's current sui generis approach to AI outputs may require further refinement as EU harmonization deepens and as the legal meaning of "human authorship" becomes a practical determinant of copyrightability across jurisdictions (Kyrylenko, 2024). At the same time, Ukraine's policy agenda must reflect reconstruction realities, including protection of dual use innovation, safeguarding of sensitive R&D, and support for displaced creators, which makes IP policy a component of economic security and continuity planning rather than a narrowly specialized legal field (UANIPIO, 2025).

Building on these comparative insights, a coherent roadmap for Ukraine can be described across five interdependent dimensions. First, legal reforms should prioritize full and technically accurate approximation to EU digital IP standards, including the refinement of exceptions, intermediary related obligations, and enforcement remedies, while also clarifying the national position on AI generated outputs to ensure doctrinal coherence and predictable market practice (Kyrylenko, 2024; Savchuk & Tsurkan, 2025).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Second, institutional strengthening should focus on capacity building for the IP office, courts, customs, and law enforcement units that handle complex digital cases, supported by training and specialized expertise capable of evaluating technical evidence and platform based infringement patterns (UANIPIO, 2025). Third, digital registries and tools should be developed as a governance infrastructure, meaning secure digitization, international interoperability, and trusted evidence services that reduce duplication, improve transparency, and strengthen evidentiary readiness for cross border enforcement (UANIPIO, 2025). Fourth, cybersecurity should be embedded into IP strategy, because digital IP is increasingly compromised through hacking, scraping, insider misuse, and synthetic media threats, which requires risk assessment, secure architectures, and practical guidance for firms on safe AI use and data governance (McGowan, 2025). Fifth, sustained international collaboration with WIPO, EUIPO, and peer offices should function as an implementation accelerator through shared platforms, capacity programs, and coordinated policy dialogue, ensuring that Ukraine's reforms remain aligned with evolving global standards while supporting innovation and cultural recovery during reconstruction (UANIPIO, 2025).

Conclusions. The analysis conducted in this study demonstrates that the contemporary intellectual property (IP) landscape – globally and in Ukraine – is undergoing a profound structural transformation driven by digitalization, the proliferation of data-centric business models, and the rapid deployment of artificial intelligence and distributed technologies. Theoretical and doctrinal foundations of IP, although still anchored in classical utilitarian, natural-rights, and personality-based justifications, increasingly interact with technological realities that challenge traditional assumptions regarding authorship, originality, territoriality, infringement detection, and long-term preservation of IP assets. The global shift toward platformized, highly interoperable digital markets intensifies these challenges by exposing IP frameworks to cross-border legal conflicts, heightened cybersecurity risks, and unprecedented levels of unauthorized data extraction and content replication.

For Ukraine, which is simultaneously modernizing its legal system and aligning with the EU acquis, these findings underscore the need for a hybrid legal-technological model of IP governance. Legal reforms alone – however comprehensive – cannot ensure the integrity, authenticity, or enforceability of rights without equally strong technological infrastructures. Likewise, purely technological tools such as blockchain, watermarking, smart contracts, or AI-based enforcement systems cannot operate effectively without clear statutory authority, harmonized exceptions and limitations, and

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

robust institutional oversight. Therefore, a balanced, hybrid approach – integrating doctrinal clarity, well-designed enforcement mechanisms, cybersecurity standards, and interoperable digital registries – is essential for strengthening Ukraine's IP ecosystem and ensuring its compatibility with international practices.

The study's findings also indicate that emerging technologies not only produce new risks (e.g., AI-generated content, unauthorized scraping, deepfakes, or quantum-threatened cryptography) but also offer new opportunities for reforming IP administration. Blockchain-based provenance, tokenization of rights, automated licensing, and algorithmic infringement detection can significantly modernize rights management, provided that appropriate safeguards, auditability, and dispute-resolution frameworks accompany them. Ukraine's current trajectory – digitizing UANIPIO systems, integrating with WIPO databases, adopting EU-oriented copyright reforms, and embracing AI-assisted governance – illustrates promising steps in this direction. Nevertheless, the persistence of regulatory gaps, the complexity of litigation involving digital evidence, and the vulnerability of digital registries during wartime conditions necessitate further systemic improvements.

Future research directions should extend in several complementary domains. First, deeper empirical studies are required to assess how Ukrainian creators and technology firms actually interact with the new legal changes, particularly regarding AI-generated works, digital exhaustion, and cross-border licensing. Second, further comparative analysis is needed to evaluate how leading innovation economies (EU, United States, Japan, South Korea, Singapore) integrate AI ethics, cybersecurity standards, and data-governance rules into their IP frameworks – and how these models could be adapted to post-war Ukrainian reconstruction. Third, technological research should explore the long-term viability of blockchain and related distributed systems for archival preservation, considering issues such as cryptographic obsolescence, interoperability with existing registries, and compliance with data-protection principles, including the right to be forgotten. Finally, interdisciplinary scholarship – linking IP law, information science, cybersecurity, and computational linguistics – is necessary to design governance systems capable of addressing the complex interaction between creators, machines, and markets.

In sum, transitioning to a resilient, innovation-oriented IP regime requires Ukraine to combine legal harmonization, institutional strengthening, and technological modernization. Only an integrated model – capable of balancing rights protection with digital openness – can support

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Ukraine's creative economy, reinforce its position in the global IP system, and ensure that intellectual property continues to serve as a foundation for economic competitiveness, cultural development, and democratic resilience in the digital age.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Berne Notification No. 169. [Berne Convention for the Protection of Literary and Artistic Works]. Accession by Ukraine. URL: https://surl.li/cwovek
2. Data as an IP Asset. (2023). URL: https://surl.li/ogsheh
3. For the first time in ukraine, copyright is registered for works that include AI-generated images. (2024). URL: https://surl.li/cvslic
4. Intellectual Property (Stanford Encyclopedia of Philosophy). URL: https://plato.stanford.edu/entries/intellectual-property/
5. Kyrylenko, A. (2024). Ukrainian IP Office registers works incorporating AI-generated content protected under new sui generis right - The IPKat. URL: https://surl.li/gzujju
6. Levi, S. D., & Ghaemmaghami, M. (2025). Copyright Office Weighs In on AI Training and Fair Use | Skadden, Arps, Slate, Meagher & Flom LLP. URL: https://surl.li/hztxut
7. Li, C. (2025). Japan unveils 2025 IP strategy to climb global innovation rankings | Asia IP. URL: https://surl.lt/eienqg
8. Ministry of Economy and WIPO sign Memorandum of Cooperation. URL:https://surl.li/plmgvj
9. McGowan, B. (2025). Deepfake threats to companies. URL: https://surl.li/aygtyg
10. Preparing for the Ukraine-European Commission negotiating: copyright. URL: https://nipo.gov.ua/en/ua-mock-session-7-d2-en/
11. Ramos, A. (2022). The metaverse, NFTs and IP rights: to regulate or not to regulate? URL: https://surl.li/ycypcv
12. Rechardt, L. (2015). Streaming and Copyright: a Recording Industry Perspective. URL: https://surl.lu/vdwavt
13. Rose, A. (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. URL: https://surl.li/inkqba

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

14. Savchuk, V., & Tsurkan, O. (2025). Legal Landscapes: Ukraine – Intellectual Property. URL: https://surl.li/crdlvh
15. Somal, S. (2025). The Increasing Threat of Cyber Espionage and Its Impact on Trade Secret Protection. URL: https://surl.li/zgdecf
16. UANIPIO is in the process of integration with WIPO digital platforms. URL: https://nipo.gov.ua/en/integration-wipo-digital-platforms-ga-2025/
17. WCT Notification No. 30. [WIPO Copyright Treaty]. Accession by Ukraine. URL: https://surl.lt/hbopek
18. What is Intellectual Property? URL: https://surl.li/vgmkpj
19. Xalabarder, R. (2002). Copyright: Choice of Law and Jurisdiction in the Digital Age. URL: https://surl.li/krkbzb

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Section 2.2. Operational intellectual property management for EU game developers: from harmonization to scalable enforcement

Oleksandr Mihus[1]

[1]*Bachelor's student of the Management program, WSHIU University, Poznan, Poland; Junior Researcher, Scientific Center of Innovative Research, Pussi, Estonia, ORCID: https://orcid.org/0009-0007-7856-8199*

Citation:
Mihus, O. (2025). Operational intellectual property management for EU game developers: from harmonization to scalable enforcement. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 68-88). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-68-88

Abstract. *The EU games sector is moving from discrete packaged releases to live service ecosystems in which value is produced through code, audiovisual assets, narrative worlds, brands, continuous updates, and community mediated creativity, while infringement and impersonation can propagate across borders in real time. The study formulates an operational approach to intellectual property protection for EU game developers, particularly SMEs, by treating IP protection as a measurable governance capability rather than a static portfolio of registrations. The analysis applies a doctrinal and operational synthesis that maps protected game assets to the relevant EU legal stack, then translates these norms into a control and documentation system oriented toward incident routing, evidence readiness, and scalable platform engagement. The study demonstrates that effective protection requires multi object asset mapping, since a single title simultaneously activates software and copyright rules, database related protections where applicable, trademark and design instruments for franchise identity, and trade secrets for internal pipelines and security heuristics. The decisive operational variable is evidence readiness, implemented through provenance logs, licensing and notice records, brand clearance artefacts, trade secret access controls, and standardized enforcement evidence packs that enable rapid response across courts and intermediaries. Cross border brand governance converts IP from a purely legal asset into a continuous compliance obligation, so studios should prioritize standardized documentation, fast institutional routing, and proportionate measures that remain publicly defensible in high visibility disputes. Future studies should operationalize metrics for rights clarity, control effectiveness, and response speed, and empirically test how evidence readiness and platform procedures affect enforcement outcomes, consumer trust, and long-term franchise value in different EU jurisdictions.*

Keywords: *EU games industry; intellectual property governance; operational IP management; evidence readiness; cross border enforcement; user generated content; trademark protection; trade secrets; copyright compliance; Digital Services Act; Digital Single Market; reputation and trust.*

1. Context and rationale. The contemporary EU games sector operates within a structural transition from a discrete, packaged product economy to a continuous service and ecosystem economy in which value is produced, distributed, and contested across borders in real time. This transition changes the practical meaning of intellectual property protection because the core object of protection is no longer only a finished game build, but an evolving portfolio of code, audiovisual assets, narrative worlds, brands, live updates, and community mediated creativity. A single successful title typically becomes a franchise that extends into merchandising, esports, streaming cultures, and licensing arrangements, which amplifies the reputational and economic consequences of infringement, impersonation, and uncontrolled brand dilution. The logic is visible in globally recognised games such as Fortnite, where cosmetics, live events, and rapid content cycles make brand integrity and licensing discipline central to business stability, and in Minecraft, where extensive modding communities increase both innovation potential and the need for clear boundaries for lawful reuse. The same governance tension appears in Roblox and similar platforms, where user generated content is not peripheral but foundational to the business model, so IP risk management must incorporate platform rules, scalable licensing, and structured notice and redress procedures rather than relying on case by case litigation.

Cross border distribution intensifies these challenges because legal rights remain territorially grounded while consumer perception and digital circulation are transnational. In practice, the EU internal market reduces some barriers, yet enforcement outcomes may still vary due to procedural differences, resource asymmetries, and the speed at which infringement can propagate through online channels. This problem is compounded by the fact that game related infringements are rarely confined to classic piracy. They increasingly include account fraud, deceptive clone apps, counterfeit digital goods markets, domain based impersonation during releases, and unauthorised exploitation of characters and symbols in adjacent markets. The live service structure also makes data governance inseparable from IP governance, because online play, analytics, personalization, and anti cheat systems require personal data processing that can affect trust and compliance exposure. Well known controversies around aggressive anti cheat tooling illustrate that technical protection choices can create legitimacy and transparency challenges, meaning that protection must be effective but also proportionate and publicly defensible.

The rationale for this chapter is therefore twofold. First, it aims to explain how harmonised EU rules can be translated into operational routines

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

that protect creators' incentives while maintaining user trust, lawful community creativity, and competitive fairness. Second, it treats IP protection as a governance capability that can be measured through rights clarity, technical and contractual controls, monitoring, evidence readiness, and enforcement execution speed, rather than as a static set of registrations. This approach is particularly relevant for SMEs and independent studios, including those producing culturally significant EU titles, because limited legal budgets increase the value of preventive design, standardised contracting, and scalable response playbooks. In short, the chapter positions IP protection in gaming as an applied system of legal, technical, and organisational controls that must function continuously, across jurisdictions, and under high public visibility.

The EU games industry requires an IP protection model that is operational, cross border, and trust sensitive, because live service production, platform intermediation, and user participation transform infringement from an episodic legal problem into a continuous governance and reputational risk.

2. Normative and institutional foundations for EU IP protection in gaming. IP protection in the EU games sector rests on a harmonised architecture that aligns substantive rights, enforcement tools, and market governance across Member States. The core legal premise is that games are multi component digital works, so protection must address several legal objects at once, including software code, audiovisual content, databases, brands, and confidential know how. Copyright harmonisation for the digital environment is anchored in the Information Society framework, which also requires Member States to provide legal protection against circumvention of effective technological measures. (European Parliament & Council, 2001). The Digital Single Market framework modernises copyright rules in platform mediated environments and reshapes the compliance expectations for services that host user uploads, while the Commission's guidance on Article 17 clarifies the intended balancing of licensing, platform responsibilities, and user safeguards. (European Parliament & Council, 2019; European Commission, 2021). In parallel, the software specific copyright regime remains relevant because it frames protection of computer programs as literary works and recognises limited exceptions linked to interoperability, which is practically important for engines, middleware, and modding interfaces. (European Parliament & Council, 2009). Database protection also matters for games that rely on structured compilations, including live service content libraries, item tables, telemetry repositories, or curated datasets, because the EU database regime defines the scope of legal

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

protection for databases as such, distinct from the software used to operate them. (European Parliament & Council, 1996).

Beyond copyright, trade mark protection is central to franchise economics because titles, logos, character marks, and merchandising identifiers operate as reputation carriers across markets and languages. (European Parliament & Council, 2017; European Parliament & Council, 2015). Design protection can also be relevant when distinctive visual appearance is industrially reproduced, for example in collectible items and branded products, and EU design law provides both national harmonisation and an EU wide design regime. (European Parliament & Council, 1998; Council, 2002). Trade secrets law supports protection of confidential business information and reduces the burden of proving unfair conduct when secret assets are unlawfully acquired, used, or disclosed. (European Parliament & Council, 2016a). Finally, GDPR shapes game operations because identity systems, behavioural analytics, anti cheat tooling, and live operations increasingly rely on personal data processing, which makes privacy compliance part of the trust and reputation baseline. (European Parliament & Council, 2016b).

Table 2.3 consolidates the primary EU legal instruments as an applied stack, emphasising what each instrument contributes to enforceable protection in gaming.

Table 2.3 indicates that EU protection functions as a layered system, where copyright and software rules secure core creation, brand and design instruments protect market identity, trade secrets protect competitive advantage, and enforcement and platform regulation determine practical effectiveness. The key methodological implication is that compliance should be managed as an integrated portfolio of artefacts, rather than as isolated legal checklists.

The EU normative baseline is broad because games combine multiple protected objects, and practical protection depends on translating this legal stack into operational documentation and platform ready procedures.

A deeper understanding of “what is protected” is necessary because games do not correspond to a single legal category. The same title includes software protected under the computer program framework, audiovisual and literary components protected by copyright, and brand identifiers protected by trade mark law. (European Parliament & Council, 2009; European Parliament & Council, 2001; European Parliament & Council, 2017).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 2.3. EU normative stack relevant to the games industry

Legal instrument	Regulatory domain	Practical object in games	Typical compliance deliverable
Directive 2001/29/EC	Digital copyright and TPM protection	Distribution of protected works; anti circumvention for effective technological measures	TPM rationale, anti circumvention policy, takedown evidence package
Directive (EU) 2019/790	DSM copyright modernisation	Platform mediated distribution; UGC governance; licensing markets	Licensing logs, notice and complaint workflow, user safeguards documentation
Commission Guidance COM/2021/288	Article 17 interpretation	Operationalisation of platform duties and user protection	Best efforts protocol, transparency reporting structure
Directive 2009/24/EC	Legal protection of computer programs	Engine code; middleware integration; interoperability considerations	Source control provenance, third party code registers, interoperability assessments
Directive 96/9/EC	Database protection	Structured collections used in live ops and content systems	Database rights assessment, extraction and reuse risk controls
Regulation (EU) 2017/1001; Directive (EU) 2015/2436	EU and national trade marks	Franchise signs; game titles; logos; merchandising identifiers	Clearance and filing strategy, brand use guidelines, enforcement triage
Regulation (EC) No 6/2002; Directive 98/71/EC	EU and national designs	Industrially reproduced visual appearance in products and collectibles	Design audit for eligible assets, filing decision log
Directive (EU) 2016/943	Trade secrets	Build pipelines; anti cheat heuristics; unreleased roadmaps; security tooling	NDA architecture, access segmentation, incident response playbook
Directive 2004/48/EC	Civil enforcement remedies	Injunctions; evidence measures; damages; cross border litigation	Evidence readiness package, interim relief checklist
Regulation (EU) 2016/679	Data protection	Accounts; analytics; profiling; online safety and security tooling	DPIA triggers, vendor governance, breach response documentation
Regulation (EU) 2022/2065	Platform governance	Notice action systems; systemic risk management for platforms hosting illegal content	Notice and action procedures, transparency reporting where applicable
Directive (EU) 2019/770	Digital content contracts	Consumer rights for digital content and services	Contract and update policy alignment, conformity and remedies approach
Regulation (EU) 2024/1689	AI governance	AI systems in moderation, detection, or enforcement workflows	AI compliance screening for relevant use cases

Sources: (World Trade Organization, 1994; European Parliament and Council, 2004)

This multi object structure becomes more complex in live service models because updates create continuous authorship and licensing flows,

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

and the practical evidence of creation and ownership must be preserved across versions. Modding ecosystems introduce a governance challenge because they blur the boundary between community creativity and derivative works, which makes the DSM platform and licensing logic relevant even for companies that are not classic "platforms" but operate UGC features. (European Parliament & Council, 2019; European Commission, 2021).

Trade secrets complement these regimes by protecting confidential know how that is not disclosed in the game build but is crucial for competitive performance, such as proprietary tooling, telemetry methods, detection heuristics, or unreleased content pipelines. (European Parliament & Council, 2016a). Database rights can be relevant where substantial investment is made in obtaining, verifying, or presenting content collections, and they can become strategically important for games that rely on curated content libraries or sophisticated item and world state tables. (European Parliament & Council, 1996). This mapping also clarifies why brand governance is inseparable from reputation management, since in markets where players purchase skins, season passes, or expansions, brand confusion caused by clones or impersonation directly translates into consumer harm and loss of trust.

Table 2.4 systematises the asset level mapping and connects each asset type to the EU legal regimes that typically apply.

Table 2.4. Game asset layers and corresponding EU protection regimes

Asset layer in a game	Typical legal characterisation	Primary EU legal basis
Engine and gameplay code	Computer program protected under copyright	Directive 2009/24/EC
Art, music, dialogue, cutscenes	Copyright protected works in digital form	Directive 2001/29/EC
Online distribution and UGC features	Licensing and platform responsibility logic	Directive (EU) 2019/790; COM/2021/288
Item tables, content libraries, structured collections	Database protection where criteria are met	Directive 96/9/EC
Title, logo, key franchise signs	Trade mark protection across the internal market	Regulation (EU) 2017/1001; Directive (EU) 2015/2436
Product and collectible appearance	Design protection where industrial reproduction applies	Regulation (EC) No 6/2002; Directive 98/71/EC
Build pipeline, anti cheat heuristics, internal tools	Confidential know how protected as trade secrets	Directive (EU) 2016/943
Player accounts and behavioural telemetry	Personal data processing compliance baseline	GDPR (EU) 2016/679

Sources: (European Parliament and Council, 2016; European Union Intellectual Property Office, 2019)

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 2.4 shows that protection is strongest when asset classification is explicit, because each asset type implies different evidentiary needs and different enforcement levers. It also supports a practical governance rule: the studio should maintain a living "asset registry" that links each major asset to ownership, licence terms, and the applicable legal regime, with version control over time.

Asset level mapping prevents category errors, reduces licensing gaps, and enables faster enforcement because it aligns each infringement scenario with the correct legal tool.

Norms alone do not secure IP in practice, because enforcement is executed through institutions and procedural mechanisms. Civil enforcement in the EU is supported by a minimum set of measures and remedies intended to allow effective enforcement across the internal market, but operational realities still depend on national courts and procedural practice. (European Parliament & Council, 2004). The EUIPO provides institutional infrastructure for EU trade marks and designs and also hosts enforcement related tasks through the Observatory framework, which is relevant for monitoring and coordination against infringements. (European Parliament & Council, 2012). Platform regulation adds another institutional layer because the Digital Services Act introduces governance expectations for online intermediaries, including procedural systems around illegal content, which can include IP infringing content in practice. (European Parliament & Council, 2022). Data protection authorities and the European Data Protection Board ecosystem influence game operations by shaping compliance expectations for processing practices, which can affect anti fraud and anti cheat tools that rely on behavioural signals. (European Parliament & Council, 2016b).

From a governance perspective, the institutional map should be read as a set of channels that must be coordinated rather than as separate regulators. A trade mark infringement that emerges through counterfeit digital marketplaces may require EUIPO linked intelligence and national enforcement cooperation, while a UGC infringement problem may require platform procedures aligned with DSM expectations and DSA style operational clarity. The practical effect is that studios should design an internal escalation model that routes incidents by their legal nature and by the institution that can act fastest.

Table 2.5 provides an applied institutional map oriented toward response speed and evidence flows.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 2.5. Key EU and national actors relevant to IP protection in games

Actor or institutional channel	Primary role	What it means for game studios
National courts and authorities	Procedural enforcement and remedies under civil enforcement baseline	Evidence readiness determines speed and outcome in injunction and damages pathways
EUIPO	EU trade marks and designs; enforcement related coordination tasks via Observatory mandate	Centralised brand and design strategy, plus access to enforcement oriented resources and coordination
European Commission	Guidance and policy shaping for DSM implementation	Need for documented compliance processes aligned with Article 17 guidance logic
Platform governance under DSA	Operational systems for illegal content procedures	Importance of structured notices and traceable complaint handling for scalable online enforcement
Data protection supervisory authorities	Oversight of GDPR compliance	Privacy by design choices affect trust and legal risk, including in security tooling

Sources: (European Parliament and Council, 2016; European Parliament and Council, 2022; European Parliament and Council, 2024)

Table 2.5 indicates that enforceability is partly a function of institutional fit, meaning that the same harmful behaviour must be framed correctly to engage the right channel with the right evidence standard. This observation strengthens the case for standardised evidence packages and clearly assigned responsibilities inside the organisation.

Institutional effectiveness depends on routing decisions and evidence quality, so studios need a structured incident governance model that connects legal characterisation to the competent enforcement channel.

In games, reputational damage can occur faster than legal resolution, so governance should prioritise documentation that enables rapid action and credible public communication. Evidence readiness is particularly important because digital infringement often involves transient online traces, multiple intermediaries, and rapid replication across jurisdictions. The civil enforcement baseline supports measures that rely on proof and documentation, so the practical question becomes whether the studio can demonstrate ownership, infringement, and harm in a manner that courts and platforms can process quickly. (European Parliament & Council, 2004). For DSM related governance, evidence of licensing efforts and the functioning of complaint and redress processes can become equally important, since compliance is assessed through demonstrable procedures rather than through statements of intention. (European Commission, 2021). For trade secrets, the ability to show that reasonable steps were taken to keep information secret is often decisive in practice, which makes access control logs, NDA regimes,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

and policy enforcement integral to protectability. (European Parliament & Council, 2016a). In data governance, DPIA style assessments and vendor contracts support accountability and reduce the risk that enforcement tooling becomes legally vulnerable. (European Parliament & Council, 2016b).

Table 2.6 translates these needs into a concrete set of artefacts that can be maintained throughout the game lifecycle.

Table 2.6. Evidence and documentation artefacts that support enforceable IP governance

Governance domain	Core artefact	Why it matters for enforcement and reputation
Copyright and software	Authorship and provenance logs, version control history, third party component register	Establishes ownership and scope of rights under software and copyright rules
UGC and platform compliance	Licensing records, notice handling logs, complaint and redress records	Demonstrates procedural compliance under DSM governance expectations
Trade marks and brand	Clearance evidence, filing portfolio, brand use guidelines, enforcement triage	Supports consistent market identity and reduces confusion risk
Trade secrets	NDA library, access controls, incident response, classification schema	Shows reasonable protection steps for confidential assets
Civil enforcement	Standard evidence pack templates, preservation checklist, chain of custody	Enables faster injunction and damages pathways under EU enforcement baseline
Data governance	DPIA triggers, vendor governance pack, breach response plan	Strengthens trust and reduces legal vulnerability of operational systems
Platform and intermediary engagement	Structured notices and traceability records	Aligns with procedural expectations for handling illegal content at scale

Sources: (International Organization for Standardization, 2010; International Organization for Standardization, 2020; World Intellectual Property Organization, 2019)

Table 2.6 indicates that "protectability" is partly produced by organisational behaviour that can be evidenced, audited, and repeated. This is the point where legal protection becomes a management system, and where SMEs can compensate for limited litigation capacity through disciplined documentation and fast incident workflows.

Evidence readiness is the operational centre of IP governance in games because it converts legal rights into actionable remedies, accelerates response, and supports trust preserving communication.

Normative and institutional foundations for EU IP protection in gaming can be understood as a layered governance architecture that combines harmonised rights, procedural enforcement tools, and institutional channels for market and platform governance. The most effective approach treats

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

these rules as a single operational system implemented through asset mapping, institutional routing, and evidence ready documentation.

3. Cross border use of IP in branding and compliance: risks and responsibility. Cross border branding in the games sector transforms IP from a legal asset into a continuous compliance obligation because distribution, marketing, community activity, and merchandising operate simultaneously across jurisdictions and platforms. The core difficulty is that the reputation of a game brand is built globally, while rights enforcement is executed through a combination of EU harmonised instruments and national procedures, each with different speed and evidentiary expectations. In parallel, modern infringement is rarely limited to direct copying of a game build. It increasingly includes look alike titles and logos, counterfeit merchandise, impersonation domains, fraudulent in game currency offers, and unauthorised user generated content monetisation, all of which can harm consumers and destabilise trust. The OECD's analysis of trade in fakes indicates that counterfeit and pirated goods remain economically significant, including in the EU import context, which supports the conclusion that brand driven industries such as gaming face persistent cross border exposure even when core products are digital (OECD, 2025). The OECD also documents how illicit networks misuse e commerce and online platforms for counterfeit trade, which is relevant for games because the same channels are used for counterfeit collectibles, branded apparel, and fraudulent digital offers (OECD, 2021). In addition, EUIPO's qualitative evidence on consumer risks posed by counterfeits highlights safety and harm dimensions that can translate directly into reputational losses for brand owners, particularly when counterfeits are perceived by consumers as authentic (EUIPO, 2019).

From a governance standpoint, cross border IP risk in games can be structured into a limited set of recurrent scenarios that differ in legal basis, institutional pathway, and reputational consequences. The EU trade mark framework provides an internal market instrument for protecting franchise signs, including titles, logos, and other brand identifiers, but protection is effective only if it is paired with monitoring and consistent use policies that preserve distinctiveness (European Parliament & Council, 2017). Where user creativity is encouraged, the DSM copyright framework becomes relevant because platform like environments must operationalise licensing, notice handling, and user safeguards in a way that is scalable and auditable (European Parliament & Council, 2019). The cross border dimension is intensified by domain name abuses, because cybersquatting and phishing can emerge around major releases or esports events, and the UDRP offers an expedited administrative path for certain trademark based disputes (WIPO,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

2025; ICANN, 2020). Finally, when disputes escalate, Directive 2004/48/EC anchors the civil enforcement toolkit across the EU, which makes evidence readiness a decisive determinant of speed and outcome (European Parliament & Council, 2004).

Table 2.7. Cross border IP risk taxonomy for games brands and live operations

Risk category	Typical manifestation	Primary legal anchor	Principal reputational harm
Brand confusion and dilution	Look alike titles, logos, fake "official" tournament pages	EU trade mark regime	Loss of distinctiveness, perceived loss of control, consumer confusion
Domain impersonation and phishing	Cybersquatting, fake launch sites, credential harvesting	UDRP processes and registrar obligations	User harm and distrust, support costs, negative press
UGC infringement and monetisation conflict	Unlicensed skins, maps, videos, derivative asset packs	DSM copyright framework and platform governance logic	Perceived unfairness to creators, community backlash, inconsistent moderation risk
Counterfeit merchandise and unsafe products	Fake apparel, toys, collectibles linked to a franchise	Illicit trade evidence base; consumer risk findings	Direct safety concerns, brand association with harm, regulatory attention
Organised piracy and circumvention ecosystem	Tools enabling unauthorised access and distribution	Anti circumvention protection under EU copyright framework	Revenue leakage, perceived weakness of protection, unfair competition narrative
Cross border litigation and remedy delays	Injunction and damages actions across Member States	EU civil enforcement baseline	Prolonged uncertainty, cost escalation, investor confidence decline

Sources: (European Parliament and Council, 2017; European Parliament and Council, 2015)

Table 2.7 supports a practical inference: reputational severity is often highest when consumer harm is plausible, such as phishing or unsafe counterfeits, and when the organisation appears slow or inconsistent in response.

Cross border risk is multi channel and reputationally asymmetric, so the governance priority should be rapid containment of consumer facing harms and consistency of enforcement logic across jurisdictions and platforms.

Cross border branding creates shared responsibility because infringement is frequently mediated by platforms, payment systems, app stores, hosting services, marketplaces, and community tools. A defensible compliance position therefore requires clarity on who is responsible for prevention, detection, evidence preservation, and remedial action. The DSA strengthens procedural expectations for digital intermediaries, including notice and action systems and transparency duties for certain services, which

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

can matter when IP infringements are handled through platform processes (European Parliament & Council, 2022).

At the same time, the rights holder remains responsible for the quality of claims and the proportionality of enforcement choices, especially where lawful user activity and creative expression are implicated under EU copyright balancing. In practice, this means that a studio or publisher should treat responsibility as a governance model, not as a legal afterthought, and should maintain a clear internal routing mechanism that links each incident to an accountable owner (Table 2.8).

Table 2.8. Responsibility matrix for cross border IP incidents in games

Task element	Rights holder	Platform or marketplace	Registrar or host	Community creators	External partners
Brand policy and permitted use rules	Lead, define and publish	Support via tooling and policy alignment	Support via abuse contact points	Follow rules and disclose attribution	Align licensing and marketing
Monitoring and detection	Lead, implement watch systems	Share signals and provide reporting channels	Respond to abuse reports	Flag misuse, community moderation	Provide intelligence where relevant
Evidence preservation	Lead, maintain chain of custody	Provide logs and takedown records where available	Provide registration and hosting records where lawful	Preserve upload context	Support with distribution records
Notice and action execution	Submit substantiated notices	Operate notice, redress, and repeat infringer tools	Act on abuse per policy or law	Comply with outcomes	Implement channel partner actions
Litigation and civil remedies	Lead, instruct counsel	Cooperate as needed	Cooperate as needed	Not applicable	Support where contracts require

Sources: (European Parliament and Council, 2019; World Intellectual Property Organization, 2019)

Table 2.8 indicates that responsibility is distributed, but accountability remains concentrated. The rights holder must be prepared to substantiate claims and coordinate response speed, while intermediaries contribute procedural capacity.

Cross border compliance becomes credible when responsibility is explicit and operational, with clear ownership for evidence quality, notice integrity, and escalation decisions under EU procedural frameworks.

Effective control design balances three goals that often conflict in practice: robust brand protection, community legitimacy, and procedural defensibility. The EU trade mark system supports a unified registration

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

strategy, but brand protection can still fail if franchise signs are used inconsistently or if enforcement is selective in a way that appears arbitrary (European Parliament & Council, 2017).

In UGC heavy environments, legitimacy depends on transparent rules for fan content and monetisation boundaries. This is why leading publishers increasingly issue public guidelines that define acceptable uses, for example Minecraft usage guidelines that explain acceptable ways to use the brand and assets (Mojang Studios, 2025). Epic's fan content policy likewise defines "Fan Content" and limits it to personal, non commercial uses under specified conditions, which illustrates how brand holders can support community creativity while preserving control of commercial exploitation (Epic Games, 2025). On large creator platforms, the same governance logic appears through structured terms and licensing tools. Roblox's Terms of Use define UGC and incorporate creator related terms, and Roblox has introduced licensing tooling for rights holders through its License Manager terms, illustrating a move toward permissioned and auditable IP use at scale (Roblox, 2025).

Table 2.9. Control catalogue for cross border brand and IP governance in games

Control domain	Control objective	Minimum artefact	Operational metric
Brand use governance	Preserve distinctiveness and reduce confusion	Brand guidelines and naming rules aligned with trade mark strategy	Number of confusion reports; enforcement cycle time
UGC and fan content governance	Enable lawful creativity while limiting commercial misuse	Fan content policy, monetisation boundaries, attribution rules	Appeal rate; reversal rate; creator satisfaction indicators
Domain and impersonation protection	Reduce phishing and cybersquatting exposure	Domain watch list, rapid complaint template for UDRP	Time to domain takedown or transfer
Marketplace and counterfeit monitoring	Reduce counterfeit products and unsafe goods association	Marketplace watch and escalation playbook	Volume of delistings; recurrence rate
Evidence readiness	Enable fast civil enforcement and platform actions	Standard evidence pack and chain of custody protocol	Time to assemble evidence package
Partner compliance	Prevent unlicensed cross border exploitation	Licensing register and partner audit rights	Contract compliance findings; remediation time

Sources: (Epic Games, 2025; Mojang Studios, 2025; Nintendo, 2018)

Table 2.9 implies that compliance maturity can be audited through artefacts and metrics. This supports a reputational thesis: stakeholders trust

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

brands that demonstrate consistent rules and predictable procedures, even when enforcement actions are frequent.

Cross border control design is strongest when it is transparent to users, auditable for platforms and courts, and measurable through operational metrics that reveal whether protection is timely and proportionate.

Contractual architecture is the main instrument for allocating rights and responsibilities across publishers, studios, distributors, esports organisers, influencers, and licensing partners. A cross border brand strategy typically requires that contracts define permitted uses, geographic scope, quality control, approval rights, and remedies for misuse. In merchandising, quality control is reputationally decisive because counterfeit goods can be unsafe, and EUIPO research highlights that counterfeits can pose multiple types of consumer risks, which increases the cost of inadequate licensing governance (EUIPO, 2019). Contracts should therefore treat quality control, supply chain transparency, and audit rights as core clauses rather than optional additions. For UGC ecosystems, contracts and terms should also define the licensing grant, user retention of rights, moderation standards, and dispute pathways. Roblox's documentation illustrates how UGC ecosystems are governed through layered terms and creator frameworks, which can be adapted as a model for studios that host creator marketplaces (Roblox, 2025-a).

Table 2.10. Clause set for cross border licensing and brand compliance in the games sector

Clause group	Primary purpose	Typical risk mitigated
Scope, territory, term	Define where and how the IP can be used	Grey market exploitation, territorial overreach
Quality control and approvals	Protect brand integrity and consumer trust	Low quality or unsafe merchandise reputational harm
Anti counterfeiting cooperation	Enable rapid response across channels	Recurrence and distribution network resilience (OECD, 2021; OECD, 2025)
Data and platform compliance	Align marketing and community activity with platform rules	Policy violations, account enforcement, loss of distribution channels
Audit and reporting	Produce evidence and accountability	Disputes over sales, royalties, and misuse
Remedies and termination	Enable proportional enforcement	Delayed action and escalation costs

Sources: (Organisation for Economic Co-operation and Development, 2021; Organisation for Economic Co-operation and Development and European Union Intellectual Property Office, 2021; Organisation for Economic Co-operation and Development, 2025)

Table 2.10 supports a governance conclusion: cross border compliance is implemented primarily through contracts, and weak clause design creates

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

avoidable reputational exposure, especially in merchandising and partner marketing.

Contract models are the enforceable layer of cross border compliance because they define quality control, auditability, and remedy speed, all of which influence reputation outcomes when infringement or misuse becomes public.

Real ecosystems demonstrate that cross border IP governance is not a theoretical concern but a daily operational necessity. Minecraft's public usage guidelines illustrate how a franchise can encourage community creativity while limiting uses that would confuse consumers or suggest official endorsement, which is especially relevant when fan creations are distributed internationally (Mojang Studios, 2025). Epic's fan content policy similarly demonstrates a boundary between non commercial fan activity and commercial exploitation, reflecting a strategic approach to preserve licensing value while supporting community engagement (Epic Games, 2025).

Roblox illustrates the platform scale version of the same issue: the Terms of Use define UGC governance, and the License Manager terms indicate a structured approach for rights holders to license IP for use on platform experiences, which aligns with the broader industry trend toward permissioned UGC monetisation (Roblox, 2025-a; Roblox, 2025-b).

Table 2.11. Scenario mapping from famous game ecosystems to cross border IP controls

Ecosystem example	Typical cross border IP issue	Control pattern that works	Source signal
Minecraft community creations	Brand use in fan products and servers	Public brand usage rules and monetisation boundaries	Usage guidelines (Mojang Studios, 2025)
Epic fan creations	Fan art and websites using publisher IP	Fan content policy limiting to non commercial use	Fan content policy (Epic Games, 2025)
Roblox UGC platform	Large scale UGC with licensing complexity	Terms based UGC governance plus licensing tools for rights holders	Terms of Use and License Manager terms (Roblox, 2025-a; Roblox, 2025-b); licensing partnerships reported (Reuters, 2025; The Verge, 2025)
Franchise merchandising across borders	Counterfeit goods and consumer safety risks	Quality control clauses and active monitoring	EUIPO consumer risk evidence (EUIPO, 2019); OECD counterfeit trade evidence (OECD, 2025)
Release related impersonation sites	Phishing and cybersquatting around launches	UDRP readiness and fast registrar escalation	UDRP guide and registrar policy (WIPO, 2025; ICANN, 2020)

Sources: (Roblox, 2025; Valve, 2025)

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

News reporting also documents Roblox's expansion of IP licensing partnerships with major rights holders, which shows how compliance and licensing tooling become a commercial enabler rather than only a risk response mechanism (Reuters, 2025; The Verge, 2025).

Table 2.11 indicates that famous ecosystems converge on the same governance logic: publish clear public rules for community use, build scalable licensing pathways where UGC is central, and maintain rapid response capacity for consumer facing threats such as counterfeits and impersonation domains.

Practical examples show that cross border compliance is most effective when it is embedded in publicly intelligible rules, platform ready terms, and rapid enforcement playbooks that prioritize consumer harm reduction and consistent brand integrity.

Cross border use of IP in branding and compliance is best understood as a system of risks that travel through platforms and supply chains, not as a set of isolated legal disputes. EU trade mark protection provides a unified internal market basis for franchise identity, while EU copyright and platform frameworks structure UGC related risks and compliance expectations (European Parliament & Council, 2017; European Parliament & Council, 2019). Enforcement effectiveness depends on evidence readiness and on selecting the fastest appropriate channel, including civil remedies under Directive 2004/48/EC and expedited domain dispute options under UDRP (European Parliament & Council, 2004; WIPO, 2025; ICANN, 2020). Empirical evidence on counterfeits and e commerce misuse confirms that brand owners face persistent cross border exposure and that safety related counterfeits can escalate reputational harm beyond pure revenue loss (OECD, 2021; OECD, 2025; EUIPO, 2019).

4. Methodological approaches to integrating IP into reputational and compliance models across jurisdictions. A practical way to integrate IP into a reputational and compliance model is to treat IP as a measurable capability set rather than a purely legal status. A minimal model usually includes four measurable blocks. The first block is rights clarity, which assesses whether ownership and licensing are unambiguous for code, audiovisual assets, music, voice acting, middleware, and outsourced art. The second block is control effectiveness, which evaluates how technical measures, access controls, and platform tools reduce infringement probability in real time. The third block is market integrity, which measures trademark consistency, counterfeit risk, and consumer confusion signals. The fourth block is enforcement readiness, which evaluates evidence quality,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

decision speed, and cross border execution capacity using civil enforcement instruments.

This methodology is particularly important for live service games because content cycles are fast and community creation is central. In such settings, the DSM framework and Article 17 guidance imply that platform governance should be treated as part of IP compliance, not merely as community management.

IP should be embedded in reputational evaluation through measurable governance capabilities: rights clarity, control effectiveness, market integrity, and enforcement readiness.

5. Evidence, monitoring, and enforcement in cross border disputes: reputational loss and trust recovery. Enforcement in games must be designed around speed, credibility, and proportionality because reputational losses are often driven by public narratives about fairness, user rights, and innovation. Directive 2004/48/EC supports tools such as injunctions, corrective measures, and damages, but outcomes depend on evidence quality and procedural readiness. In the platform era, monitoring also includes domain name abuse, phishing, and impersonation sites that exploit game brands to deceive users. The UDRP framework provides an online mechanism for trademark based domain name disputes, which is operationally useful when rapid transfer or cancellation is needed to reduce consumer harm.

Table 2.12. Enforcement pathways and evidence requirements for the games ecosystem

Threat type	Primary tool	Evidence package	Reputational objective
Piracy and unauthorised distribution	Civil enforcement measures under Directive 2004/48/EC	Proof of ownership, chain of distribution, technical logs, market impact	Demonstrate protection of creators while avoiding overreach
Circumvention devices	Anti circumvention framework under Directive 2001/29/EC	Effectiveness of TPM, linkage to protected works, proportionality rationale	Reinforce integrity of ecosystems and fair competition
Brand impersonation domains	UDRP via WIPO or equivalent procedures	Trademark rights, confusing similarity, bad faith indicators	Protect users from deception and restore trust rapidly
UGC infringement on platforms	Licensing and “best efforts” governance under DSM Article 17 guidance	Notice records, filtering governance, complaint handling, licensing attempts	Show balanced governance that respects lawful user creativity

Sources: (European Parliament and Council, 2004; European Parliament and Council, 2016)

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

The Table 2.12 shows that enforcement is most effective when evidence is pre structured as a repeatable package rather than assembled ad hoc after a crisis. This reduces response time and supports consistent messaging that protects both rights and community legitimacy.

Trust recovery in IP disputes depends on evidence readiness, fast procedures such as UDRP for brand abuse, and balanced enforcement narratives anchored in EU legal standards.

6. Practical recommendations: IP due diligence, contract models, and protection policies in international operations. A due diligence model for EU game developers typically begins with a rights inventory that covers code, art, music, voice, middleware, and AI assisted assets, followed by a gap analysis of ownership and licensing clauses. Trade secret protection should be implemented as a governance system rather than a document set, using access segmentation, need to know controls, and incident response procedures consistent with the trade secrets directive. For community facing ecosystems, policies must be explicit about permitted uses, monetisation limits, and brand use boundaries. The Minecraft usage guidelines provide a clear example of how a major franchise communicates acceptable uses of its name and assets to reduce confusion and preserve brand integrity while supporting community creativity.

For platforms that host large scale UGC, licensing infrastructure can become a strategic compliance mechanism. Roblox's Terms of Use formalise the treatment of user generated content and the licensing relationship needed to operate the service, illustrating how platform contracts structure IP responsibilities at scale. More recently, Roblox has also advanced a formal IP licensing approach with major partners, signalling a move toward permissioned creation models that can reduce infringement risk while enabling new business models. Within the EU context, these developments align conceptually with the DSM direction toward clearer licensing markets and structured platform responsibility.

International IP protection becomes sustainable when due diligence, confidentiality governance, and explicit community licensing rules are integrated into product operations and platform strategy.

Conclusion. Strengthening IP protection in the EU games sector requires operational governance that connects harmonised legal rules with practical controls and evidence ready enforcement. The Information Society Directive anchors protection of technological measures, while the DSM framework and Article 17 guidance reshape responsibilities around user uploaded content and licensing markets. Trademark protection and trade secret governance remain central because brand integrity and confidential

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

know how are core to competitive advantage in games. Civil enforcement instruments and fast online mechanisms such as UDRP help reduce reputational harm when infringement targets users through piracy, impersonation, or deceptive domains. The most resilient model treats IP as a measurable capability set across rights clarity, technical and contractual controls, market integrity, and enforcement readiness, thereby protecting innovation while maintaining legitimate user creativity and trust.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. European Commission. (2021). *Guidance on Article 17 of Directive (EU) 2019/790 on copyright in the Digital Single Market* (COM/2021/288 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0288
2. European Parliament & Council. (1996). *Directive 96/9/EC of 11 March 1996 on the legal protection of databases*. https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng
3. European Parliament & Council. (1998). *Directive 98/71/EC of 13 October 1998 on the legal protection of designs*. https://eur-lex.europa.eu/eli/dir/1998/71/oj/eng
4. European Parliament & Council. (2001). *Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
5. European Parliament & Council. (2004). *Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights*. https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng
6. European Parliament & Council. (2009). *Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs*. https://eur-lex.europa.eu/eli/dir/2009/24/oj/eng
7. European Parliament & Council. (2012). *Regulation (EU) No 386/2012 of 19 April 2012 on entrusting the Office for Harmonization in the Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0386
8. European Parliament & Council. (2015). *Directive (EU) 2015/2436 of 16 December 2015 to approximate the laws of the Member States relating to trade marks (recast)*. https://eur-lex.europa.eu/eli/dir/2015/2436/oj/eng

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

9. European Parliament & Council. (2016). *Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
10. European Parliament & Council. (2017). *Regulation (EU) 2017/1001 of 14 June 2017 on the European Union trade mark (codification)*. https://eur-lex.europa.eu/eli/reg/2017/1001/oj/eng
11. European Parliament & Council. (2019). *Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market*. https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng
12. European Parliament & Council. (2019). *Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770
13. European Parliament & Council. (2022). *Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
14. European Parliament & Council. (2024). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
15. European Union. (2016). *Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
16. European Union. (2002). *Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs.* https://eur-lex.europa.eu/eli/reg/2002/6/oj/eng
17. Epic Games. (2025). *Fan Content Policy*. Retrieved December 14, 2025, from: https://www.epicgames.com/site/en-US/fan-art-policy
18. European Union Intellectual Property Office. (2019). *The risks posed by counterfeits to consumers: A qualitative study*.https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers/2019_Risks_Posed_by_Counterfeits_to_Consumers_FullR_en.pdf
19. ICANN. (2020). *Uniform Domain Name Dispute Resolution Policy (UDRP)*. https://www.icann.org/resources/pages/policy-2012-02-25-en
20. Mihus, O. (2024). STRENGTHENING INTELLECTUAL PROPERTY PROTECTION IN THE EU: IT LAW AND ITS IMPACT ON THE COMPUTER GAMES INDUSTRY. *Public Administration and Law Review*, (4(20), 20–34. https://doi.org/10.36690/2674-5216-2024-4-20-34
21. Mojang Studios. (2025). *Minecraft usage guidelines.* Retrieved December 14, 2025, from: https://www.minecraft.net/en-us/usage-guidelines
22. OECD. (2021). *Illicit trade: Misuse of e-commerce and online platforms for trade in counterfeits.* OECD Publishing. https://www.oecd.org/en/publications/illicit-trade-misuse-of-e-commerce-and-online-platforms-for-trade-in-counterfeits_07d1032d-en.html

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

23. OECD. (2025). *Mapping the global trade in fakes: Global trends and enforcement challenges.* OECD Publishing. https://www.oecd.org/en/publications/mapping-the-global-trade-in-fakes_8b2be95f-en.html
24. Reuters. (2025, July 15). *Roblox launches IP licensing platform, partners with Netflix, Lionsgate.* https://www.reuters.com/business/media-telecom/roblox-launches-ip-licensing-platform-partners-with-netflix-lionsgate-2025-07-15/
25. Roth, E. (2025, November 12). *Roblox is opening up its IP licensing platform. The Verge.* https://www.theverge.com/news/819407/roblox-is-opening-up-its-ip-licensing-platform
26. Roblox. (2025-a). *Roblox Terms of Use.* Retrieved December 14, 2025, from: https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use
27. Roblox. (2025-b). *License Manager Terms.* Retrieved December 14, 2025, from: https://en.help.roblox.com/hc/en-us/articles/42542704086548-License-Manager-Terms
28. World Intellectual Property Organization. (2025). *WIPO guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).* Retrieved December 14, 2025, from: https://www.wipo.int/amc/en/domains/guide/
29. Court of Justice of the European Union. (2014). *Nintendo Co. Ltd and Others v PC Box Srl and 9Net Srl (Case C-355/12).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0355

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Section 2.3. Legal Dimensions of Using Blockchain for Intellectual Property Protection

Alla Dombrovska[1]

[1]*Ph.D. (Law), Associate Professor, Associate Professor of the Department of Patent Science and Fundamentals of Law Enforcement Activities, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-4610-8220*

Citation:
Dombrovska, A. (2025). Legal Dimensions of Using Blockchain for Intellectual Property Protection. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 89–105). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-89-105

Abstract. *Blockchain technology presents both significant opportunities and notable challenges in the protection and management of intellectual property rights. Recent academic research and policy analyses explore its potential applications across copyright, trademark, and patent law, highlighting how distributed ledgers can function as immutable records, provide reliable timestamped evidence of authorship, and enable automated licensing through smart contracts. The aim of this study is to analyze the legal potential of blockchain technology in the protection and management of intellectual property rights, assess its effectiveness as a tool for evidencing ownership and facilitating licensing, and identify the regulatory gaps that must be addressed to enable its broader implementation within contemporary IP law. The study is based on a theoretical and doctrinal research approach that integrates several complementary methods to examine the relationship between blockchain technology and intellectual property protection. The analysis draws on existing legal frameworks, including statutory provisions, international IP agreements, regulatory guidelines, and relevant case law, to understand how blockchain-based evidence and smart contracts are currently treated within different legal systems. The analysis finds that blockchain technology can significantly enhance intellectual property protection by providing immutable timestamping, reliable authorship evidence, and transparent record-keeping. These features strengthen copyright and patent enforcement and support more efficient licensing through smart contracts, particularly in industries such as music and digital art. The study shows, however, that legal integration remains inconsistent across jurisdictions. Case-based examples confirm that blockchain improves traceability and rights management but cannot independently prevent infringement or verify originality. The results demonstrate that blockchain is a promising supplementary tool for IP governance, yet its broader adoption depends on clearer regulatory standards, institutional support, and alignment with existing legal mechanisms.*
Keywords: *blockchain; intellectual property; copyright; patent law; trademark protection; smart contracts; distributed ledger technology; digital rights management; authorship evidence; licensing automation; legal frameworks; IP enforcemen; regulatory challenges.*

ISBN 978-9916-9389-5-9 (pdf)

1. Theoretical Foundations of Blockchain Use in Intellectual Property Law. Intellectual property law aims to incentivize creativity by granting creators exclusive rights to their works. However, in the digital era, establishing ownership and provenance of creative or patented materials has become increasingly complex. Distributed ledger (blockchain) technology introduces a potential solution: a decentralized, cryptographically linked database in which all entries are time-stamped and immutable. As described in the literature, "blockchain is like a shared and immutable digital book (called 'ledger') that allows everyone to have a copy of all transactions…When someone wants to change their own version of the book, everyone must agree." (Rosati, 2022). This peer-to-peer system renders records nearly impossible to alter once stored. For intellectual property holders, blockchain therefore offers a mechanism for generating independent evidence of creation dates, transfers, and licensing arrangements without relying solely on centralized authorities.

The present study theorizes the role of blockchain in intellectual property protection. Recent legal scholarship, organizational white papers, and relevant case developments form the core of the analytical base. The methodological approach is descriptive and analytical, synthesizing existing literature to evaluate how blockchain can support ownership, registration, enforcement, and commercialization of IP rights. The analysis considers theoretical foundations such as the "code as law" paradigm, examines case studies from the music and digital art sectors, and outlines emerging international policy initiatives. The study ultimately identifies gaps within current IP law and proposes reforms aimed at enabling more effective use of blockchain technologies by creators and rights holders.

Findings drawn from legal literature and case examples indicate that blockchain can enhance IP protection by providing tamper-proof records of creation, transparent chains of title, and automated rights management systems (White Paper, 2022). Nevertheless, significant legal uncertainties persist: existing IP statutes frequently fail to recognize blockchain-based evidence explicitly, NFT transactions do not automatically transfer copyright, and the enforceability of smart contracts remains inconsistent across jurisdictions. Policymakers are therefore encouraged to modernize legal frameworks to accommodate blockchain-generated proof – as seen in the position taken by a French court (Moille, 2025) – clarify the legal status of tokenized rights and promote interoperable technical standards for distributed IP registries.

Scholars and IP organizations have begun exploring blockchain's applicability. A 2022 WIPO white paper maps out multiple use-cases: from

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

evidencing the creation of works (copyright, design, patent) to simplifying IP administration and licensing (White Paper, 2022). For example, WIPO explains that "by using blockchain to register creative works, creators can store their works in a hash that can be used as evidence of creatorship" – the immutable time-stamp can then be used in litigation to prove the work's existence at a specific date (White Paper, 2022). Similarly, blockchains could serve as "digital notaries" for patent filings and inventor documentation (White Paper, 2022). EU institutions and law review commentators note that distributed ledgers can yield secure, time-stamped and immutable records that help combat counterfeiting and supply-chain fraud in trademark- and design-intensive sectors (Clark, 2018; Rosati, 2022).

In academic literature, a body of work examines blockchain in IP contexts. Some focus on non-fungible tokens (NFTs) for digital art and media. For instance, Lee (Illinois Law Review) theorizes "decentralized intellectual property" whereby NFTs and smart contracts allow creators more direct control and record of transactions (Lee, 2023). Others critique misunderstandings: U.S. Copyright Office studies warn that minting an NFT does not itself confer copyright on the tokenized artwork, and one can even create ("mint") an NFT for a work one doesn't own (Report to Congress, 2024). Law reviews on music law emphasize that blockchain and smart contracts could remedy the music industry's "broken" royalty system (Sharp & Lobel, 2023), while commentary in trademark law considers how on-chain proof-of-use registries might simplify proving genuine use of marks (White Paper, 2022). Internationally, bodies like WIPO and EUIPO are analyzing legal standards. For example, Europe's Top 500 IP professionals discuss blockchain in an EUIPO News article (2024), and the EUIPO has held "Blockathon" forums to explore blockchain anti-counterfeiting. Although many questions remain unanswered, the literature generally agrees that blockchain offers novel tools (timestamping, transparency, automation) that existing IP mechanisms lack (Sharp & Lobel, 2023).

The core advantage of blockchain is its immutability and decentralization. Once data (e.g. a hash of a creative work or patent application) is recorded on-chain, it cannot be retroactively altered without consensus. As one WIPO analyst explains, a permissioned blockchain can act as an append-only ledger for IP assets (White Paper, 2022). In practical terms, this means a creator who hashes a work on the blockchain obtains a continuous, tamper-proof chain of evidence of authorship and transfer. Less formally, this confirms Lessig's insight that "code is law": the technology itself can enforce norms (here, priority of creation) independent of human registrars (Lee, 2023). In other words, blockchain shifts some functions of

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

IP law (like registration and proof of use) into code-mediated processes.

The theoretical underpinnings thus contrast blockchains with traditional registries. While patent and trademark law rely on government offices to issue certificates, a blockchain registry could be jointly maintained by multiple parties (e.g. decentralized or by consortium) so that no single entity controls the record (White Paper, 2022). This "distributed trust" model can reduce intermediaries and costs: for example, authors could make direct agreements with consumers or licensees without paying notaries or agents (White Paper, 2022). Moreover, smart contracts (self-executing code on blockchains) can encode license terms. WIPO notes that IP holders "may use smart contracts for licensing and assignment of registered IP rights", automating royalty payments when conditions are met (White Paper, 2022). In theory, this intertwines property rights with programmable contracts: as one commentator observes, NFTs can "tokenize" almost any asset, providing a permanent public record of ownership and transfers (Lee, 2023). These features constitute a new form of private ordering around IP, akin to Lessig's "code as law" paradigm (Lee, 2023).

Figure 2.3 summarizes the theoretical foundations of blockchain technology and highlights the relative conceptual emphasis found in the intellectual property law literature.

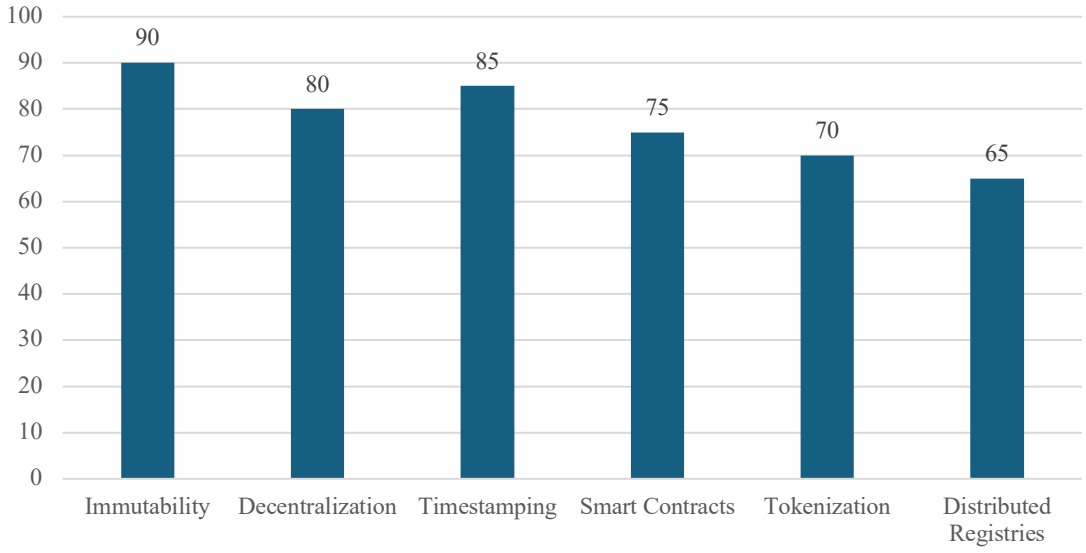

Figure 2.3. Conceptual Emphasis of Blockchain Features in Intellectual Property Scholarship

Source: developed by the author

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

2. Practical Applications of Blockchain in Intellectual Property Protection. Blockchain's core features – a decentralized, time-stamped, immutable ledger – lend themselves naturally to recording and protecting IP rights. WIPO has even established a Blockchain Task Force to develop models and standards for applying blockchain in IP (Rose, 2020). In practice, blockchain can serve as a trustable "digital notary" for creation and transactions. For example, an IP office could use blockchain to log every event in the life of a trademark or patent – from filing and first use in commerce to assignments or licenses – creating a tamper-proof audit trail of ownership and use (Clark, 2018). This improves data integrity and speed (EUIPO reports that its blockchain-enabled TMView/DesignView registers deliver trademark and design data in real time with higher security and throughput (2021)). More broadly, analysts note that blockchain "records and tracks assets … as a shared, immutable digital ledger," making it a reliable tool for IP asset management (Len, & Mann, 2025). In short, blockchain's immutable timestamps and consensus verification mean creators and owners can maintain authoritative proof of their works or inventions without fear of retroactive tampering (Clark, 2018).

Copyright and Creative Works. In the realm of copyright and other unregistered rights, blockchain is principally used to prove authorship and creation time. Creators can "hash" their work and write the hash into a blockchain, generating a public, dated record of existence. This serves as solid evidentiary proof of authorship: as one WIPO analysis explains, uploading a work's metadata to blockchain "will create a time-stamped record and solid evidence" of its conception (Clark, 2018). In practice, startups and collecting societies are already exploiting this. For instance, Canada's Access Copyright Foundation created an "Attribution Ledger" on blockchain that "immutably connects the work, [its] metadata and the entity able to authorize its use," thereby reliably linking each creative work to its legal owner (White Paper, 2022). In litigation, such proof can be decisive: a recent U.S. legal commentary notes a French court accepted a blockchain timestamp as proof of authorship date in a copyright dispute (Len, & Mann, 2025).

Blockchain also enables new licensing and royalty schemes for creative content. By encoding license terms into smart contracts, payments and permissions can be automated. For example, a smart contract might be programmed to release a digital artwork only when a payment is recorded on-chain, or to distribute royalty fees instantly every time a song is played. Kodak's blockchain-based image rights platform is a concrete example: it uses smart contracts to manage and monetize photographs, ensuring each use

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

triggers a micropayment to the photographer (Clark, 2018). In music and publishing, similar ledger-based systems can track streams or reproductions and directly route royalty shares to artists and rights-holders. As one law firm notes, smart contracts "may be used in IP transactions to monitor IP usage and collect royalties," turning copyright licenses into self-executing agreements (Clark, 2018; Len, & Mann, 2025). This streamlines licensing in digital markets and reduces reliance on centralized clearinghouses, making compensation for creators more transparent and efficient (Len, & Mann, 2025).

Patents and Innovation. Although patents themselves are registered rights, blockchain can enhance patent systems by anchoring disclosure events and simplifying transactions. Inventors can record an invention's disclosure or experimental data on a blockchain to establish a verifiable timeline, which can later support patent validity or demonstrate prior art. In essence, blockchain provides "solid proof of facts regarding the life cycle of an invention" (Bajwa, & Meem, 2024). For example, companies are exploring tokenizing patents – issuing blockchain tokens representing patent rights or licenses – to facilitate trading and financing of innovations. While still nascent, these models echo ideas like open patent ledgers. WIPO's Blockchain Task Force envisions blockchain-enabled "IP registries" where assignments, licenses, or pledges could be entered directly by participants, making registers more up-to-date and reducing administrative delay (Bajwa, & Meem, 2024). In the meantime, some innovators simply publish their technical disclosures on-chain as defensive publications, preventing others from patenting the same ideas – a practical use of blockchain's timestamping as prior art.

Like with copyright, smart contracts can automate patent licensing. For instance, a smart contract could automatically validate that a licensee has paid agreed fees (recorded on the chain) before allowing use of a patented technology. WIPO observers suggest blockchain could "validate the user's payment once access to digital content was granted" and monitor issuance of licenses and timely payment of royalties (Bajwa, & Meem, 2024). Though the U.S. Patent and Trademark Office (USPTO) itself has not changed patent law, it is tracking these trends. (A 2024 joint study by the U.S. Patent and Trademark Office and the U.S. Copyright Office Copyright Office on NFTs explicitly noted that blockchain-based registration remains an area for exploration rather than immediate reform (Rota, & Douglass, 2024)).

Trademarks, Brands and Anti-Counterfeiting. For trademarks and brand protection, blockchain offers ways to prove use in commerce, trace provenance, and combat fakes. In many jurisdictions, trademark owners

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

must show genuine use of a mark. By logging sales or distribution events on-chain, a blockchain register can provide indisputable, time-stamped evidence of when and where a mark was actually used (Clark, 2018). One WIPO commentary describes how a brand owner could collect usage data on a blockchain-based register, giving "reliable and time-stamped evidence of actual use" and facilitating defenses against claims of non-use or loss of distinctiveness (Clark, 2018). EU trademark systems are already experimenting: in 2021 EUIPO connected TMview and DesignView to a blockchain backbone so that searches reflect the latest cross-border registrations instantly.

Beyond evidence of use, blockchain is being leveraged for provenance tracking and anti-counterfeiting. By attaching a secure tag or digital token to a product and recording its supply-chain journey on blockchain, every participant (from manufacturer to customs to consumer) can verify authenticity. WIPO experts note that a ledger "showing who owns what, who is an authorized licensee, and so on" lets anyone validate a product and distinguish it from a fake (Clark, 2018). Today, luxury goods, pharmaceuticals, and even certification marks (like the Woolmark for wool products) can incorporate scannable blockchain-backed seals. For example, if a customs official scans a seized item and finds no matching on-chain record of that serial number or tag, it is immediately flagged as counterfeit. Recognizing this, the EU Intellectual Property Office has launched initiatives such as the Anti-Counterfeiting Blockathon and a blockchain "authentication platform" that interlinks product trace data with enforcement agencies' risk analysis (Lince, Little, & Diakun, 2021). The EUIPO explicitly states it will roll out a decentralized blockchain platform for authenticating products to combat the global trade in fakes (Lince, Little, & Diakun, 2021).

Table 2.13 systematizes the principal practical applications of blockchain technology across copyright, patent, and trademark law, highlighting their functional roles.

The blockchain oriented instruments can strengthen IP governance primarily by improving evidentiary readiness, reducing transaction friction through automated licensing, and enabling traceability mechanisms that are especially valuable for brand protection and supply chain integrity. Their practical value, however, depends on governance design, including trusted identity and metadata standards, legal recognition of time stamped records, and interoperability with existing registries and enforcement procedures.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 2.13. Blockchain Applications in Key Intellectual Property Fields: Evidence, Licensing, and Traceability Functions

IP Field	Blockchain Application	Practical Function
Copyright and creative works	1. Authorship and creation timestamping 2. Automated licensing and royalty distribution	Provides immutable, time-stamped evidence of authorship and date of creation Executes licenses and distributes royalties through smart contracts
Patents and innovation	1. Proof of invention lifecycle 2. Automated patent licensing	Establishes verifiable timelines for disclosures, and assignments Validates payments and enforces licensing conditions via smart contracts
Trademarks and brands	1. Proof of use in commerce 2. Provenance tracking and anti-counterfeiting	Supplies reliable, time-stamped evidence of genuine trademark use Ensures product authenticity and traceability across supply chains

Source: developed by the author

3. Legislative Perspectives on Blockchain in IP Protection. European policymakers have begun to explore how blockchain (DLT) might strengthen IP rights management. In the EU's 2020 Action Plan for Intellectual Property, the Commission explicitly endorsed blockchain as a means "to increase the effectiveness of our IP systems" (Hohn-Hein, 2022). Pursuant to this, the EUIPO launched in April 2021 the first blockchain-based registers for EU trademarks and designs (Hohn-Hein, 2022), creating an immutable ledger of filings across member states (linked to TMview/DesignView databases). These pilot registries improve data security and allow automated priority claims but exist alongside – and do not replace – formal national registrations. At the international level, WIPO has formed a Blockchain Task Force under its Standards Committee to draft interoperability standards for blockchain in the IP ecosystem, and published a 2021 White Paper on blockchain applications (e.g. provenance tracking, smart licensing).

• *EU IP Strategy:* Under the EU Action Plan IP, the EUIPO's "blockchain register" links national trademark/design filings on a shared ledger. The aim is greater transparency and traceability (e.g. chain-of-title searches) (EU Parliament study, 2022), but the register's legal effect depends on conventional law (registrations are still grounded in national systems).

• *Crypto-assets Regulation:* The EU's Markets in Crypto-Assets (MiCA) Regulation (in force June 2023) creates uniform rules for crypto-tokens (broadly including NFTs) (ESMA, 2025). However, MiCA focuses on financial-market integrity and consumer protection (transparency, authorization, AML) (ESMA, 2025), not on IP rights. No EU directive or

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

regulation yet addresses blockchain licensing or smart-contract enforcement per se.

• *Parliamentary and Commission Studies:* An EU Parliament study (2022) found that existing IP law suffices to govern NFT issues. It concluded that minting or trading an NFT of a copyrighted work without authorization still constitutes reproduction/infringement under copyright law (EU Parliament study, 2022). Likewise, an NFT sale by itself does not transfer the creator's copyright – only whatever license is explicitly attached to the token (EU Parliament study, 2022). The study noted, however, that enforcement is made harder by blockchain's decentralization and anonymity (EU Parliament study, 2022). The Commission's ongoing Data Governance/Finance initiatives have acknowledged blockchain and smart contracts but have not yet enacted IP-specific rules.

• *WIPO and Global Initiatives:* WIPO's Blockchain Task Force is drafting a standard for blockchain usage in IP records (WIPO, 2019). WIPO workshops and white papers highlight use-cases (e.g. timestamping works, automating royalty payments) but stop short of normative rules. Similarly, national IP offices (e.g. UKIPO) have run hackathons and pilot projects to explore blockchain for copyright metadata, registration or anti-counterfeiting measures.

• *Comparative Developments:* In the United States, a 2023 USPTO–Copyright Office report to Congress echoed the EU view, finding "changes to IP laws are not currently necessary" for NFTs or smart contracts (Report to Congress, 2024). It emphasized that NFTs simply pose familiar issues (e.g. unauthorized copying, lack of clear licensing), and that "smart contracts" are just code subject to ordinary contract law (Report to Congress, 2024). National courts are beginning to weigh in: notably, in Tribunal judiciaire de Marseille (March 2025) a French court accepted a blockchain timestamp (certified by a notary) as valid proof of design authorship and priority (Moille, 2025). Likewise, the UK High Court has even permitted serving legal documents via an NFT to on-chain addresses (Moille, 2025). These case-by-case decisions signal judicial openness to DLT-based evidence, though without altering substantive IP rights.

Blockchain intersects with core IP doctrines in complex ways:

• *Formalities and Registration:* Traditional IP protection often depends on formal registration or deposit. Blockchain can immutably record a creator's claim (a timestamped "hash"), but it does not substitute for statutory formalities. For example, EU copyright law has no mandatory register – authors must prove originality and date if challenged. A blockchain entry can bolster proof of "who came first," but without legal recognition it

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

cannot by itself create a registered right (EU Parliament study, 2022). (EUIPO's experimental SDR blockchain project links national filings for design/trademark, but each right still flows from the underlying office registration (EU Parliament study, 2022)). In sum, DLT can enhance the record-keeping of rights and chains of title, but jurisdictional formalities remain grounded in national law (EU Parliament study, 2022).

- *Territoriality and Enforcement:* IP rights are territorial, yet blockchain operates globally. A token or smart contract on a public ledger may be accessible worldwide, but the law that applies depends on locale. This creates friction: decentralized networks obscure infringer identity and location, raising jurisdiction and applicable-law questions (EU Parliament study, 2022). The European Parliament study warned that anonymity of blockchain users makes enforcement "difficult in cases in which the identity of the infringer is unknown" (EU Parliament study, 2022). In practice, rights-holders may need cross-border litigation and cooperation to tackle on-chain infringement. Thus, blockchain's cross-jurisdictional nature tests the IP principle of territorial scope and may require new international coordination (e.g. through WIPO or EU-level guidance).
- *Originality and Authorship:* Blockchain time-stamping can substantiate when a work was created, aiding proof of first authorship. However, it does not alter the originality requirement. EU copyright requires that a work be an author's own "intellectual creation," reflecting personal expression (EU Parliament study, 2022). A timestamped file on-chain cannot invent creativity – it merely verifies chronology. That said, courts are beginning to treat blockchain hashes as reliable evidence of priority. In the 2025 French case, the designer's sketches were stored on-chain months before a copying defendant's work was made, and the court accepted the blockchain log (verified by a bailiff) as proof of authorship (Moille, 2025). This reflects a doctrinal fit: DLT records help uphold authorship claims, but creativity is still measured by classic originality tests (Moille, 2025).
- *NFTs and Licensing:* Non-fungible tokens in themselves do not carry IP ownership. As both the EU study and Eurojust guidance note, buying an NFT typically conveys only a licence or certificate, not the copyright or design right in the underlying work (Report to Congress, 2024). Absent an explicit smart-contract licence, the token-holder gets no more rights than any member of the public. Conversely, minting an NFT of a protected work without the creator's permission is equivalent to unauthorized reproduction (EU Parliament study, 2022). Thus IP law "seen through" blockchain remains conventional: NFTs are treated like digital art sales, subject to exhaustion rules and copyright consent requirements. The

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

token's metadata (on-chain or off-chain) can document terms of use or transfers, but enforceability of those terms depends on private contract law, not a new IP principle (Report to Congress, 2024).

• *Smart Contracts:* Self-executing "smart contracts" promise automated license enforcement and royalty payments. Legally, however, a smart contract is simply code: "self-executing computer code, stored on the blockchain" (Report to Congress, 2024). By default, it may not meet formal contract requirements (e.g. clear offer/acceptance in human-readable form). EU contract law can treat a smart contract as binding if it meets the criteria for an agreement, but this is unsettled. As noted above, regulators find no need for special IP rules, and commentators warn that the term "smart contract" is misleading – parties still need legal agreements (written or coded) that a court will interpret in conventional terms (Report to Congress, 2024). In practice, blockchain adds transparency and automation to licensing, but those licenses must ultimately align with general contract and IP doctrines.

4. Doctrinal Perspectives on Smart Contracts in IP Protection in European Law. Under EU private law, smart contracts are not a separate legal category but must fit within traditional contract doctrine. Importantly, EU law expressly permits contracts "concluded by electronic means" (Directive 2000/31/EC, 2000). In practice, a blockchain-embedded code can constitute an offer (and acceptance) if it embodies a clear commitment by the parties. The European Law Institute (ELI) principles on blockchain note that smart contract code should be "an eligible way to express the will of a party" (ELI Principles, 2023). Indeed, if the "if X–then Y" logic is definite, it can satisfy the specificity and intent requirements of an offer (ELI Principles, 2023). Once a smart contract is immutably recorded on-chain, ELI argues it generally reflects binding intent (since it cannot be altered unilaterally) (ELI Principles, 2023). Thus, in principle a smart contract may be a legally binding agreement, "provided that the prerequisites for the conclusion of a contract" (e.g. offer and acceptance) are met (ELI Principles, 2023).

• *EU framework for electronic contracts:* Directive 2000/31/EC (the e-Commerce Directive) mandates that Member States must allow and give effect to contracts formed by electronic means (Directive 2000/31/EC, 2000). Similarly, the eIDAS Regulation (2014/910) ensures that electronic signatures and agreements have legal effect equivalent to handwritten form (ELI Principles, 2023). These rules mean there is no formal barrier to smart contracts – any form requirement in EU or national law generally cannot nullify a contract just because it is concluded by code.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

• *National contract law:* Smart contracts are governed by each Member State's contract law. For example, Germany has no special "smart contract" statute; under the BGB (Civil Code) contracts are generally valid if offer and acceptance coincide. Legal commentators note that German law "treat[s] [smart contracts] as valid contracts (assuming the appropriate formalities have been observed)" (Schmalenberger, 2022). French law likewise emphasizes consent of wills (C. civ. arts. 1101–1124) and recognizes electronic agreements, so long as any required formality (e.g. for assignments) is satisfied. In general, therefore, European civil-law systems can accommodate smart contracts through existing principles of freedom of contract and consensual formation.

Smart Contracts in IP Licensing. Smart contracts are being explored as tools for licensing and enforcing IP rights. Observers have highlighted potential use-cases: for example, smart contracts could "establish and enforce IP agreements, licenses or exclusive distribution networks" and trigger real-time payments to rights holders (Clark, 2018). In practice, this means a smart contract could automate royalty payments whenever a licensed work is used or resold. For instance, an NFT-based music or art license might encode in its contract that each resale automatically sends a percentage to the original creator. By embedding the licence terms (scope of rights, territory, payment triggers, etc.) in code, royalties can be distributed trustlessly without manual accounting. Blockchain projects (e.g. the EU's BlockStand) have even prototyped NFT licensing standards with on-chain rights metadata, hierarchical sublicensing controls and cryptographically enforced royalty flows (Reggianini, 2025). In short, European IP-intensive industries see smart contracts as promising transparent, tamper-proof means to manage licenses and royalties, complementing traditional registries or databases.

Doctrinal Challenges. A core issue is whether and how code captures the parties' consent. Contract law requires a meeting of minds; courts will scrutinize whether both parties intended the code's effects. As ELI emphasizes, the fundamental question is "whether declarations of intent can be expressed by program code" (ELI Principles, 2023). If a smart contract is simply deployed on-chain by one party, this must be treated as an "offer" under general law, and acceptance could occur by the other party's reciprocal action (e.g. transferring payment or calling the code) (ELI Principles, 2023). In practice, many transactions pair smart code with an off-chain agreement. Parties often execute a traditional license or terms sheet together with the smart contract: the code automates performance, while the written document records mutual consent to those terms. Legal commentators thus advise

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

drafting a parallel conventional contract "to cover what code can't" (Djamane, 2025), ensuring the parties' intent and remedies are clear beyond the black-box logic. EU consumer law likewise demands clear assent: for B2C licences, pre-contractual information rules (e.g. Directive 2011/83/EU) mean consumers must understand what rights they acquire, regardless of whether the contract is on-chain or off-chain.

The contract must be sufficiently certain. Smart-contract code is precise in execution, but ambiguities can arise if code is not human-readable. ELI notes that a valid offer must have clear content and intent (ELI Principles, 2023), and that the "if-then" nature of smart code typically makes its obligations explicit (ELI Principles, 2023). However, any logical errors or coding mistakes are treated under normal contract error doctrine. For example, if source code is miscompiled into on-chain bytecode, the parties may dispute what the true terms were – such disputes would be resolved by general principles of mistake or interpretation (ELI Principles, 2023). Importantly, code's immutability means parties need agreed mechanisms for updates or reversals: as ELI suggests, even a self-enforcing smart contract must allow a "safe termination or interruption" if needed (see EU Data Act Art. 30 requirements) (Schmalenberger, 2022). In short, European courts will likely demand that a smart contract's code is as intelligible and complete as any conventional clause.

If a smart contract automatically executes a transfer or restriction, the validity of that outcome depends on broader law. For instance, property or IP law might limit what code can do. In the recent German BGH case on a leased electric-car battery, the court implicitly held that code-enforced disabling of the battery violated German property law (no self-help allowed) (Dorigo, 2022). Similarly, a smart contract could not override IP statutes (e.g. moral rights cannot be coded away) or mandatory consumer protections. ELI's consumer principles make clear that EU rules like the Unfair Terms Directive (93/13/EEC) apply equally on-chain (ELI Principles, 2023). Any term embedded in code must still be fair and transparent: an unfair code clause "shall not" be part of the binding agreement (ELI Principles, 2023) (on-chain contracts would have to be "re-coded" or voided).

Under Rome I, parties can choose a governing law (which would cover any smart license); absent choice, general rules apply. No EU rule says blockchain agreements are inapplicable, but cross-border enforcement may involve issues of jurisdiction and evidence (blockchain records may serve as proof of transaction). In practice, disputes over smart-licensed IP rights would be treated like any contractual dispute: principles of contractual

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

liability, and possibly specialized IP remedies, would apply once liability is established.

In sum, smart contracts in the IP context must meet traditional standards of consent and clarity. EU law requires that agreements, even if automated in code, still reflect a meeting of minds, a lawful object (e.g. a valid license), and definite terms. Where code executes a license or royalty clause, courts will interpret it under contract law (applying mistake, interpretation or unfairness rules as needed). As one commentator puts it, smart contracts "offer efficiency and automation, but legal enforceability still depends on intent, clarity, and local laws" (Djamane, 2025). To mitigate uncertainty, parties frequently use fallback mechanisms: parallel legal contracts, clear metadata, or off-chain dispute resolution clauses. The EU data and finance policymakers have begun addressing technical safeguards (MiCA and the draft Data Act impose interoperability and robustness standards on smart contracts (Djamane, 2025; Schmalenberger, 2022), but the core contract-law analysis remains doctrinal: code can create binding IP licenses in Europe, but only by satisfying the same consent and fairness requirements as any other contract (ELI Principles, 2023).

Conclusions. The study demonstrates that blockchain technology holds considerable potential to strengthen the protection and management of intellectual property rights, but its legal integration remains incomplete and uneven across jurisdictions. The analysis shows that distributed ledger systems can serve as reliable mechanisms for establishing authorship, priority, and ownership through immutable timestamping and verifiable record-keeping. These features are particularly valuable in copyright and patent contexts, where evidentiary certainty plays a decisive role in disputes. The research further reveals that smart contracts offer a viable tool for automating licensing processes, reducing transaction costs, and enabling more transparent royalty distribution, especially in sectors such as the music and digital art industries.

Comparative examination of regulatory approaches indicates that while several jurisdictions recognize blockchain records as admissible evidence, they do not yet provide a harmonized framework for their legal effect. Some countries have taken steps to embed blockchain into copyright registration or commercial law, but these initiatives remain fragmented and often lack explicit provisions addressing tokenized assets or decentralized ownership models. The study also finds that the legal status of NFTs continues to be ambiguous, with courts and policymakers struggling to fit these digital tokens into traditional copyright and property categories.

The evaluation of practical examples confirms that blockchain can

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

enhance traceability and reduce unauthorized use of creative works, but the absence of unified technical standards and clear regulatory guidance limits large-scale adoption. Moreover, the research highlights that blockchain cannot independently verify the originality of creative output or prevent piracy; rather, it functions as a complementary evidentiary and transactional tool within the broader IP protection ecosystem.

The analysis of blockchain's theoretical underpinnings, practical applications, and emerging legislative approaches demonstrates that distributed ledger technology possesses considerable potential to enhance the administration and protection of intellectual property rights, yet its legal integration remains incomplete. The inherent qualities of blockchain – immutability, decentralization, and automated execution – align well with core evidentiary and transactional needs within IP systems, particularly in establishing authorship, documenting priority, maintaining reliable chains of title, and facilitating transparent licensing. As case studies in copyright, patent, and trademark practice illustrate, blockchain can strengthen evidentiary positions, support rights management in complex creative industries, and contribute to more secure anti-counterfeiting mechanisms.

However, doctrinal constraints and regulatory uncertainties continue to limit the technology's full assimilation into the existing legal order. Traditional principles of IP law – especially formal registration requirements, territoriality, and the originality standard – are not displaced by blockchain records but instead require interpretive alignment. Time-stamped blockchain entries may assist in evidentiary disputes but cannot create rights independently of statutory conditions. Likewise, tokenization and the proliferation of NFTs do not modify the substance of copyright ownership or transfer rules; the legal effects of tokenized assets ultimately depend on conventional contractual agreements and established IP doctrines.

The assessment of European and comparative legislative developments confirms that policymakers are gradually acknowledging blockchain's utility but have not yet introduced comprehensive frameworks governing its IP-related uses. EU-level initiatives, WIPO standards work, and select national court decisions demonstrate growing acceptance of blockchain evidence and interest in distributed IP registries. Yet the broader regulatory landscape remains fragmented: EU contract law can accommodate smart contracts, but their enforceability depends on meeting classical requirements of consent, clarity, and fairness. Moreover, the cross-border nature of blockchain heightens jurisdictional and enforcement complexities, revealing the need for greater international coordination.

Overall, blockchain should be regarded as a complementary mechanism

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

within IP governance rather than a substitute for institutional structures. Its benefits are most effectively realized when integrated into hybrid legal–technological models that combine decentralized ledgers with established statutory regimes, judicial oversight, and contractual safeguards. For future development, coherent legislative guidance, harmonized technical standards, and enhanced institutional engagement are essential to ensure that blockchain can operate as a reliable, legally recognized tool in the protection and commercial exploitation of intellectual property rights.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Bajwa, R., & Meem, F. T. (2024). Intellectual Property Blockchain Odyssey: Navigating Challenges and Seizing Opportunities. URL: https://arxiv.org/html/2410.08359v1
2. Blockchain and Intellectual Property. (2019). URL: https://www.wipo.int/en/web/cws/blockchain-and-ip
3. Blockchain technologies and IP ecosystems: A WIPO white paper. (2022). URL: https://surl.li/kgsezu
4. Clark, B. (2018). Blockchain and IP Law: A Match made in Crypto Heaven? URL: https://surl.lt/ukevhm
5. 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'). URL: https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng
6. Djamane, D. (2025). Smart Contracts: Global Perspectives and Legal Realities – Part 2 - Daily Jus URL: https://surl.lt/nmgknb
7. Dorigo, L. (2022). Smart Contracts work – but do they hold up in court? | Pestalozzi Attorneys at Law. URL: https://surl.li/mndszc
8. ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection. (2023) URL: https://surl.li/nivgkp
9. EUIPO connects to TMview and DesignView through blockchain. URL: https://surl.li/hvhixr
10. Hohn-Hein, N. (2022). EU IP Office launches first blockchain-based IP register,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Anti-Counterfeiting Blockathon Forum. URL: https://surli.cc/leegiq
11. Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art. (2022). URL: https://surl.li/yttfdp
12. Lee, E. (2023) NFTs as Decentralized Intellectual Property. URL: https://illinoislawreview.org/wp-content/uploads/2023/08/Lee.pdf
13. Len, G. D., & Mann, E. C. Benefits and Considerations of Protecting Your IP With Blockchain Technology. (2025). URL: https://surl.lu/zzqvsv
14. Lince, T., Little, T., &Diakun B. (2021). EUIPO approves blockchain platform; NFT trademark mystery; SHOP SAFE Act hearing set – news digest. URL: https://surl.li/gqzhxf
15. Marchenko, V., & Dombrovska, A. (2025). GLOBAL SOLUTIONS FOR SAFEGUARDING INTELLECTUAL PROPERTY: HOW BLOCKCHAIN REVOLUTIONIZES DIGITAL RIGHTS MANAGEMENT. *Public Administration and Law Review*, (2(22), 81–89. https://doi.org/10.36690/2674-5216-2025-2-81-89
16. Markets in Crypto-Assets Regulation (MiCA). (2025). URL: https://surli.cc/iknsyg
17. Moille, C. (2025). France Takes Pioneering Step in Recognizing Blockchain Time-Stamping as Proof of Authorship in Intellectual Property. URL: https://surl.lt/vtmrui
18. Non-Fungible Tokens and Intellectual Property: A Report to Congress. (2024). URL: https://surl.li/jcrygm
19. Reggianini, E. (2025). Standardizing On-chain IP Rights Management. URL:https://surl.li/dxyajr
20. Rosati, E. (2022). The missing link: How blockchain technology can help protect IP owners and consumers. URL: https://surl.li/pngeso
21. Rose, A. (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. URL: https://surl.li/sdrxzm
22. Rota, D., & Douglass S. M. (2024). Don't Forget About NFTs! USPTO and USCO Issue Joint Study on the Interplay Between NFTs and Intellectual Property. URL: https://surl.li/vlyuzq
23. Schmalenberger, A. (2022). Smart contracts in the Data Act. URL: https://surl.li/xybtvw
24. Sharp, A. J. & Lobel, O. (2023). Smart Royalties: Tackling the Music Industry's Copyright Data Discrepancies through Blockchain Technology, Smart Contracts, and Non-Fungible Tokens. URL: https://surl.li/cfjdvc

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Chapter 3
Sectoral and Procedural Models of Applied Intellectual Property Management and Enforcement

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Section 3.1. Features of Intellectual Property Protection in the Assessment of Corporate Business Reputation: International Aspects

Igor Korzhevskyi[1]

[1]*Ph.D. (Management), Director, LTD «Risk-Control», Kyiv, Ukraine, ORCID: https://orcid.org/0000-0003-3012-0735*

Citation:
Korzhevskyi, I. (2025). Features of Intellectual Property Protection in the Assessment of Corporate Business Reputation: International Aspects. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 107-132). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-107-132

Abstract. *Corporate business reputation is increasingly treated as a strategic intangible that reduces stakeholder uncertainty by signaling quality, reliability, and governance discipline. Intellectual property amplifies this signaling effect in international markets because it connects value creation to legally defensible claims and to an enterprise's demonstrated capacity to protect those claims under recognized rules and procedures. The study conceptualizes international intellectual property protection as an institutional and operational capability that can be integrated into corporate reputation assessment, with particular attention to enforceability readiness, evidence discipline, and cross border risk containment. The research uses an analytical synthesis of international and regional intellectual property architectures and translates them into assessable layers, governance artifacts, and measurable indicators. Reputation relevant intellectual property governance is operationalized through documentary evidence requirements, jurisdictional calibration principles, and validation logic suitable for composite reputation models. The analysis shows that global treaty based instruments establish standardized expectations that stakeholders interpret as signals of diligence and resilience, while regional enforcement frameworks raise procedural standards and reshape what effective governance requires in practice. The findings demonstrate that reputation outcomes depend less on the mere existence of registered or asserted rights and more on auditable evidence artifacts, including priority and ownership discipline, brand portfolio governance, content compliance records, digital enforcement readiness, and evidence preservation procedures. The study further proposes a calibration and validation approach that aligns indicator weights with enforcement predictability, digital exposure, and authenticity pressure, thereby strengthening comparability across jurisdictions. International intellectual property governance becomes reputationally decisive when it is operational, evidence based, and sufficiently rapid to contain harm, reduce dispute duration, and support credible trust recovery. Future studies should quantify how evidence readiness, monitoring intensity, and enforcement timing influence reputation loss trajectories and recovery speed across sectors, and empirically test indicator systems using incident level datasets.*

Keywords: *corporate business reputation; intellectual property governance; international intellectual property protection; enforcement readiness; treaty based standards; cross border branding; counterfeiting risk; cybersquatting; online dispute resolution; evidence preservation; IP due diligence; reputation model validation.*

1. Normative and institutional foundations of international IP protection in reputation assessment. Corporate reputation is increasingly treated as a strategic intangible that reduces uncertainty for stakeholders by signaling expected quality, reliability, and governance discipline. In the literature, a useful operational distinction is that reputation combines perceptions of an organization's ability to deliver quality and its prominence in stakeholders' minds, and these dimensions can influence economic outcomes in different ways (Rindova et al., 2005). In international markets, intellectual property strengthens this signaling function because it connects value creation to verifiable legal claims and to the organization's capacity to defend those claims under recognized rules. When IP is governed systematically, it becomes evidence that a firm competes through innovation, differentiation, and lawful appropriation of returns. When IP governance is weak, stakeholders often infer broader control deficiencies, including fragile contracting practices, higher exposure to imitation, and a greater probability of disruptive disputes that may affect continuity of supply, brand integrity, and investment security.

The normative foundation of cross border IP protection begins with the WTO Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), which sets minimum standards for protection and, importantly, contains a comprehensive section on enforcement. WTO materials explicitly emphasize that TRIPS is the only international agreement with a comprehensive enforcement section, and the agreement's Part III requires members to make available procedures that enable effective action against infringement (World Trade Organization, 2025). For reputation assessment, the enforcement dimension is central because reputation damage is rarely driven by the mere existence of infringement, but rather by the perceived inability to respond promptly, proportionately, and credibly. A firm that can demonstrate preparedness to use administrative, civil, and where applicable criminal pathways consistent with TRIPS expectations is often assessed as more resilient and less likely to experience prolonged crises triggered by counterfeits, piracy, or misappropriation (World Trade Organization, 2025). In other words, TRIPS matters to reputation not only as an international legal baseline, but as an external benchmark for whether IP protection is operational rather than symbolic.

Alongside TRIPS, WIPO administered treaties establish the principles that make cross border protection coherent and interpretable across jurisdictions. The Paris Convention is particularly important for industrial property because it embeds national treatment and the right of priority, enabling applicants to extend protection to other contracting states within

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

defined periods, such as 12 months for patents and 6 months for trademarks and industrial designs (World Intellectual Property Organization, 2025). In reputation analysis, this creates an observable diligence standard: stakeholders can evaluate whether an enterprise files early, claims priority correctly, and aligns territorial coverage with its commercialization strategy. Failures in priority management may be interpreted as managerial negligence, especially when they lead to avoidable brand conflicts, loss of exclusivity, or contested market entry. The Paris architecture also supports comparability because it makes it reasonable to ask the same governance questions across countries, even when national procedures differ.

For copyright relevant assets, including software code, product documentation, marketing content, and certain design elements, the Berne Convention adds another layer of reputational expectation. WIPO's summary explains that Berne is built on basic principles that include national treatment and automatic protection, and WIPO guidance further clarifies that authors should enjoy minimum rights without the need to observe formalities (World Intellectual Property Organization, 2025). This has a direct implication for reputation assessment in digital and content intensive industries. Since protection does not depend on registration, the risk of infringement is often viewed as primarily governance and behavior driven, meaning that stakeholders look for structured content clearance, licensing discipline, and documentation of authorship and permissions. In cross border campaigns, where localization and reuse are routine, the absence of such controls can turn into reputational harm through public disputes, takedowns, and allegations of unethical appropriation.

A second institutional tier consists of WIPO's global filing and management systems, which reduce transaction costs and enable consistent portfolio governance across multiple jurisdictions. The Madrid System allows a trademark owner to file a single international application and manage it centrally, and WIPO describes it as a convenient route for registering and managing trademarks worldwide, with centralized renewals and changes (World Intellectual Property Organization, 2025). From a reputational standpoint, Madrid use is often read as evidence of brand governance maturity because it supports consistency of protection and reduces gaps that facilitate consumer confusion and counterfeiting. Similarly, the Patent Cooperation Treaty (PCT) offers a unified procedure for seeking patent protection in multiple countries, and WIPO describes a PCT application as having the same legal effect as filing separate national applications in contracting states (World Intellectual Property Organization, 2025). In reputational narratives, a coherent PCT strategy signals

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

technological seriousness and the capacity to defend innovation claims, which can matter in investment due diligence, strategic alliances, and cross border licensing.

A third tier is dispute resolution infrastructure, especially in domains where reputational harm can escalate quickly. Domain name abuse is a salient example because misleading domains can facilitate fraud and consumer deception, harming not only the trademark owner but also users. WIPO defines the UDRP as a legal framework for disputes between domain name registrants and trademark owners concerning abusive registration and use, while ICANN positions the UDRP as a mandatory consensus policy for registrars that frames how disputes are handled before suspension or transfer (World Intellectual Property Organization, 2025; ICANN, 2020). For reputation assessment, the critical factor is procedural readiness: the enterprise's ability to gather evidence, act quickly, and communicate remediation coherently. This readiness reduces the time window during which stakeholders may be exposed to phishing, impersonation, or counterfeit storefronts.

Even though the focus is international, regional enforcement frameworks can function as institutional reference points that raise expectations for procedural effectiveness. In the European Union, Directive 2004/48/EC provides a minimum set of civil measures, procedures, and remedies, and it includes mechanisms related to preserving evidence, which can accelerate containment and improve credibility in disputes (European Union, 2004; European Union, 2018). For multinational enterprises, operating in regions with stronger enforcement infrastructures can affect the weighting of risks in reputation models, since stakeholders may expect more consistent and prompt legal remedies. In regions where enforceability is less predictable, stakeholders may instead expect firms to compensate through contracts, technical safeguards, and strict trade secret governance. This implies that international reputation assessment should treat the legal environment as a moderator that changes what "good governance" practically requires (Table 3.1).

Instead, it should interpret IP as an institutional capability that connects rights, procedures, and enforcement options into an actionable system. Under this lens, stakeholders assess whether the enterprise can convert rights into market integrity, not merely whether it holds registrations.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.1. Layers of international IP protection and reputation relevant inferences

Layer	Key instruments or systems	What is standardized	What it signals in reputation assessment
Global minimum standards and enforcement	TRIPS (WTO)	Baseline protection plus enforcement expectations	Predictability and procedural readiness to contain infringement risk
Core treaty principles for cross border protection	Paris Convention; Berne Convention (WIPO)	National treatment, priority rights, automatic copyright protection	Diligence in filings, ethical content governance, and compliance maturity
Portfolio scalability and transparency	Madrid System; PCT (WIPO)	Centralized filing and management routes	Structured global brand and innovation governance, legible to investors and partners
Rapid response dispute infrastructure	UDRP (WIPO, ICANN)	Standardized domain dispute pathway	Capability to mitigate fraud and deception risks quickly
Regional procedural reinforcement	EU enforcement framework	Civil remedies and evidence tools in the internal market	Higher expectations of consistent enforcement and documentation

Sources: systematized by the author

It is also useful to translate institutional alignment into concrete evidence artifacts, because reputation assessments typically rely on auditable documentation rather than abstract claims. A firm can be formally compliant in principle, yet reputationally fragile if it lacks documentation that demonstrates timely action, coherent portfolio management, and enforceability planning (Table 3.2).

These artifacts enable third parties to verify that the enterprise is capable of preventing misuse, containing incidents, and restoring trust, which is often more important than the theoretical scope of rights.

International IP protection shapes corporate reputation because it provides shared norms, scalable procedures, and enforceability pathways that stakeholders use to judge governance quality. TRIPS anchors expectations not only for protection but also for enforcement readiness, making response capacity a reputational attribute rather than a purely legal matter. WIPO treaties, especially Paris and Berne, create cross border principles that convert “diligence” into observable behaviors such as priority management and ethical content governance. WIPO systems such as Madrid and PCT institutionalize portfolio scalability and transparency, which strengthens the credibility of brand and innovation claims.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.2. Evidence artifacts that operationalize international IP governance for reputation assessment

Evidence category	Examples of artifacts	Stakeholder question addressed	Reputation implication
Filing diligence and priority discipline	Priority claim records; jurisdiction coverage map; renewal calendar	"Did the firm protect value where it commercializes?"	Signals strategic competence and reduces imitation risk
Brand portfolio governance	Madrid registrations; change and renewal logs; brand use guidelines	"Is the brand controlled consistently across markets?"	Signals authenticity, reduces confusion and dilution
Innovation protection governance	PCT filings; invention disclosure workflow; prosecution strategy notes	"Are innovation claims defensible and governed?"	Signals credible innovation and lower partner risk
Copyright and content compliance	Licensing files; authorship documentation; clearance protocols	"Does the firm respect third party rights and avoid piracy exposure?"	Signals integrity and reduces takedown and dispute volatility
Digital enforcement readiness	UDRP case templates; evidence packs; incident communication scripts	"Can the firm respond to online impersonation fast?"	Signals consumer protection orientation and crisis readiness
Litigation and evidence procedures	Evidence preservation plans; counsel engagement triggers; internal logs	"Can the firm prove infringement and act promptly?"	Signals enforceability and reduces duration of reputational harm

Sources: systematized by the author

Finally, dispute infrastructures such as the UDRP, reinforced by regional enforcement frameworks in some markets, determine how quickly reputational harm can be contained and how convincingly trust can be rebuilt. Overall, the decisive reputational signal is not the mere possession of IP rights, but the demonstrated capacity to govern, evidence, and enforce those rights consistently across jurisdictions.

2. Cross border use of IP objects in branding and compliance: risks and responsibility. Cross border branding relies on a bundle of intellectual property objects that jointly stabilize market identity, customer trust, and the credibility of corporate claims. At the center are trademarks and related distinctive signs, supported by industrial designs, copyright in marketing and software assets, domain names as digital identifiers, and trade secrets that protect non disclosed know how embedded in product quality, supply chain configurations, and go to market strategy (World Intellectual Property Organization, 2025). In international operations, these objects are used simultaneously across jurisdictions, languages, and platform ecosystems. This simultaneity increases the probability that a weakness in one element, for example an unprotected domain variant, an unmanaged distributor, or a fragmented trademark portfolio, will spill over into broader reputational

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

harm, because consumers interpret brand signals as a unified promise rather than as a set of separate legal rights.

A first analytical point is that cross border brand identity is legally territorial but reputationally global. Trademark rights are typically enforced within specific jurisdictions, while consumer perception is formed in transnational digital spaces where content, search, and marketplace listings circulate with minimal friction. The consequence is that brand integrity becomes vulnerable to localized weak points that can be exploited for counterfeiting, impersonation, or diversion, even if the core brand is well protected in primary markets. OECD reporting on illicit trade emphasizes that counterfeit and pirated goods remain a persistent component of global trade and that infiltration of supply chains poses public health and safety risks, which directly transforms IP infringement into a trust and legitimacy problem rather than a narrow legal dispute (OECD, 2025). From a reputation assessment perspective, the relevant question is not only whether infringement exists, but whether the enterprise's cross border control system can prevent recurring incidents and demonstrate credible consumer protection.

A second point is that cross border IP use is structurally exposed to scaling mechanisms that did not exist in the same form in traditional offline markets. E commerce and platform intermediation can lower entry costs for illicit sellers, accelerate the speed of imitation, and expand the reach of counterfeits into micro segments of demand. OECD analysis of illicit trade in fakes in the e commerce environment highlights that online platforms can be abused by counterfeiters and that the governance challenge involves multiple actors, including governments, platforms, brand owners, and consumers (OECD, 2021). This multi actor structure matters for responsibility allocation. Stakeholders will often attribute reputational accountability primarily to the brand owner, regardless of legal fault, because the brand is the focal point of trust and the perceived beneficiary of market recognition.

A third point concerns consumer harm. Counterfeits are not only deceptive substitutes, they may also be unsafe. EUIPO research on risks posed by counterfeits to consumers addresses the relationship between counterfeit products and safety concerns, reinforcing that infringement can quickly become a public interest issue, especially in categories where health and safety are salient (EUIPO, 2019). This shifts corporate responsibility from reactive enforcement toward preventive governance. In reputational terms, prevention is evaluated through evidence of monitoring, supplier and distributor controls, and cooperation with enforcement and platform

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

mechanisms, because these practices demonstrate that the enterprise treats consumer safety and market integrity as core obligations (Table 3.3).

Table 3.3. IP objects used in cross border branding and their primary risk channels

IP object in branding and compliance	Core business function	Typical cross border risk channel	Most visible reputational impact
Trademarks and distinctive signs	Identity, source attribution, consumer recognition	Counterfeiting, bad faith filings, confusingly similar marks	Confusion, authenticity doubts, trust erosion
Industrial designs and trade dress	Product appearance and differentiation	Fast imitation in manufacturing hubs, look alike products	Perceived quality dilution, loss of distinctiveness
Copyright in marketing and software assets	Communication, digital product features, documentation	Unauthorized reuse, plagiarism claims, takedowns	Public disputes, campaign disruption, perceived ethical weakness
Domain names and online identifiers	Access, legitimacy cues, anti fraud function	Cybersquatting, phishing, impersonation	Consumer harm, fraud association, credibility shock
Trade secrets and undisclosed know how	Competitive advantage, process quality, strategy	Leakage via partners, employees, vendors	Loss of innovation narrative, reduced partner confidence

Sources: systematized by the author

For example, a strong trademark portfolio can be undermined by weak domain name governance or by trade secret leakage that enables high fidelity imitation.

Cross border risk can be grouped into five interrelated clusters. The first cluster is illicit replication, including counterfeiting and deceptive look alike practices. OECD and EUIPO reporting on global trade in fakes uses customs seizure data to show that counterfeit and pirated goods accounted for a non trivial share of global trade and that the risk is persistent and structurally embedded in globalized supply chains (OECD, 2025). For reputation assessment, the inference is that exposure is not exceptional. It is a baseline risk that requires institutionalized controls and continuous monitoring rather than episodic legal action.

The second cluster is digital impersonation, particularly via domains and related online identifiers. WIPO describes the UDRP as a framework for resolving disputes between domain name registrants and trademark owners over abusive registration and use, and WIPO further emphasizes its role in addressing cybersquatting (World Intellectual Property Organization, 2025). ICANN positions the UDRP as a mandatory policy for registrars, which highlights that domain disputes are handled within a structured governance

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

regime rather than purely private negotiation (ICANN, 2020). In reputational terms, domain name abuse is damaging because it blurs authenticity cues and can directly enable fraud against consumers and partners.

The third cluster is compliance driven infringement risk, which often arises from internal processes rather than external attackers. Cross border marketing localization, influencer collaborations, and outsourced creative production can generate copyright and trademark infringements if rights clearance is weak. These events can become reputationally salient because they are interpreted as failures of ethical discipline and corporate governance, especially when disputes are public and involve culturally sensitive content. While the legal resolution may be jurisdiction specific, reputational judgments spread across markets through digital media.

The fourth cluster is confidential know how vulnerability. WIPO defines trade secrets broadly as confidential business information that provides a competitive edge and treats unauthorized acquisition, use, or disclosure as an unfair practice (World Intellectual Property Organization, 2025). In the EU, Directive (EU) 2016/943 establishes a legal framework for protecting undisclosed know how and business information against unlawful acquisition, use, and disclosure (European Union, 2016). Reputational consequences arise when leakage undermines the firm's innovation narrative or reveals inconsistencies between public claims and internal practices, for example regarding sustainability or product quality.

The fifth cluster is portfolio fragmentation and procedural weakness, which becomes visible when a brand expands rapidly without coherent international filing and maintenance. WIPO's Madrid System is designed to facilitate international trademark protection and portfolio management, including renewals and changes, and this procedural infrastructure supports coherent brand governance across markets (World Intellectual Property Organization, 2025). When enterprises fail to use scalable tools or fail to coordinate filings, stakeholders may interpret subsequent disputes and brand conflicts as predictable outcomes of weak strategic planning (Table 3.4).

Even where legal fault lies with external actors, reputational accountability is attributed to the brand owner if governance mechanisms appear insufficient.

An effective compliance response to cross border IP risk requires combining legal instruments with operational controls. Legal instruments include international registrations, licensing terms, and dispute procedures. Operational controls include monitoring, partner screening, and evidence management. OECD analysis of e commerce challenges emphasizes the need for coordinated measures involving platforms and brand owners, implying

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

that compliance must extend beyond the firm's boundaries into platform engagement and ecosystem governance (OECD, 2021). For reputational stability, the decisive factor is whether the enterprise can show that it uses a repeatable governance cycle consisting of prevention, detection, response, and learning.

Table 3.4. Cross border IP risks and responsibility allocation

Risk cluster	Primary actor with operational control	Secondary actors that shape outcomes	What stakeholders typically expect from the brand owner
Counterfeiting and illicit distribution	Brand owner and authorized channel governance	Platforms, customs, logistics intermediaries	Continuous monitoring, rapid takedowns, cooperation with enforcement bodies
Domain impersonation and cybersquatting	Brand owner digital governance	Registrars, dispute resolution providers	Fast detection, UDRP readiness, clear consumer warnings
Infringement via marketing and content	Brand owner internal compliance	Agencies, influencers, contractors	Rights clearance protocols, training, contract discipline
Trade secret leakage	Brand owner internal controls	Employees, vendors, joint venture partners	Classification, access control, NDAs, incident response
Portfolio fragmentation	Brand owner IP strategy	External counsel, local filing agents	Coherent international strategy, maintenance discipline via scalable systems

Sources: systematized by the author

Prevention includes portfolio coherence and contractual discipline. Portfolio coherence means that the firm protects core marks, transliterations, and relevant classes in priority markets and uses scalable management tools when possible. WIPO describes the Madrid System as supporting centralized management actions such as renewals and updates, which reduces the probability that rights lapse or become inconsistent across markets (World Intellectual Property Organization, 2025). Contractual discipline includes standardized licensing, franchising, and distribution agreements with quality control clauses and audit rights. In reputation assessment, these clauses are interpreted as safeguards against brand dilution because they indicate that the firm treats consistent quality as a governance objective.

Detection requires market surveillance and digital monitoring. In counterfeit intensive sectors, detection is increasingly data driven, combining platform scanning, customs alerts, consumer complaint channels, and distributor reporting. The persistence of counterfeit trade documented by OECD and EUIPO strengthens the argument that monitoring must be systematic rather than episodic (OECD, 2025; EUIPO, 2025). Where safety

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

is relevant, monitoring is also a consumer protection measure, as EUIPO research links counterfeits with safety concerns (EUIPO, 2019).

Response depends on procedural readiness and evidence quality. For domain name abuse, readiness includes the capacity to file UDRP complaints with structured evidence packages and to coordinate with registrars under the ICANN policy framework (World Intellectual Property Organization, 2025; ICANN, 2020). For offline counterfeiting, readiness includes coordinated takedown actions, customs engagement, and controlled communications that avoid amplifying illicit listings while still warning consumers. Learning closes the cycle through root cause analysis, updating partner screening, strengthening product authentication measures, and adapting monitoring to new channels (Table 3.5).

Table 3.5. Governance maturity indicators for cross border IP protection in branding

Governance dimension	Low maturity signals	Medium maturity signals	High maturity signals
Portfolio governance	Fragmented filings, weak maintenance discipline	Core markets covered, periodic reviews	Madrid supported portfolio management, continuous coverage optimization
Platform and digital enforcement	Reactive, ad hoc takedowns	Some monitoring tools, basic playbooks	Integrated scanning, rapid escalation, UDRP readiness, metrics driven response
Anti counterfeit program	Sporadic enforcement	Defined procedures, selective cooperation	Continuous surveillance, customs cooperation, partner audits, safety oriented response
Content and marketing compliance	Informal approvals	Basic clearance and licensing checks	Documented clearance workflow, contractor controls, training, evidence retention
Trade secret governance	Weak classification, broad access	NDAs and basic controls	Formal classification, least privilege access, vendor controls, incident response aligned to legal frameworks

Sources: systematized by the author

High maturity is visible through documentation, response metrics, and governance mechanisms that extend into the enterprise ecosystem, including platforms, distributors, and strategic partners.

Cross border use of IP in branding and compliance creates a risk environment where legal territoriality collides with global reputational perception. Counterfeiting and digital impersonation can rapidly convert IP infringement into consumer harm and trust loss, which is why prevention and monitoring must be continuous and ecosystem oriented (OECD, 2021; OECD, 2025; EUIPO, 2019). Responsibility is shared across platforms and intermediaries, but reputational accountability is concentrated on the brand

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

owner because stakeholders evaluate capacity to prevent and contain harm. Effective governance therefore requires portfolio coherence supported by scalable international systems, disciplined partner contracting, platform engagement, and procedural readiness for mechanisms such as the UDRP (World Intellectual Property Organization, 2025; ICANN, 2020).

3. Methodological approaches to integrating intellectual property into corporate reputation models across jurisdictions. Integrating intellectual property into models of corporate reputation requires a methodological shift from treating IP as a purely legal attribute to treating it as a multidimensional capability that stakeholders can observe, evaluate, and compare across markets. In the reputation literature, a practical starting point is the idea that organizational reputation includes at least two analytically distinct dimensions, perceived quality and prominence, which influence stakeholder decisions in different ways (Rindova et al., 2005). IP contributes to both dimensions, because it can signal quality and innovativeness through visible portfolios and awards, while also increasing prominence through brands, market presence, and publicized enforcement actions. However, comparability across jurisdictions is complicated by legal territoriality, enforcement variability, and the fact that stakeholders often form judgments in global digital environments rather than within national borders. Consequently, a robust methodology must combine legal, behavioral, and economic evidence, then calibrate the interpretation of that evidence to jurisdiction specific conditions.

A useful anchoring logic for such integration is the three pillar structure often used in brand valuation standards. ISO 10668 specifies requirements for monetary brand valuation and describes a framework that includes objectives, valuation bases, valuation approaches, data and assumptions, and reporting (ISO, 2010). While ISO 10668 is explicitly a monetary brand valuation standard rather than a general reputation standard, its logic is methodologically valuable for reputation models because it forces analysts to separate legal foundations, stakeholder perceptions, and financial outcomes. This separation prevents a common error in reputation assessment, namely treating IP registrations as direct proof of reputational strength without considering whether stakeholders perceive and reward those rights, and whether the firm can defend them when challenged.

In practice, reputation models can be classified into three broad families. The first family is perception based survey models that measure the emotional bond and stakeholder judgments through structured drivers. The RepTrak model, for example, operationalizes reputation through seven drivers including governance and innovation, both of which are directly

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

sensitive to IP governance and IP enabled differentiation (The RepTrak Company, 2020; Reputation Institute, 2016). The second family is elite respondent rankings that rely on executive and analyst perceptions, such as Fortune's World's Most Admired Companies, which uses multiple attributes including innovativeness and wise use of corporate assets, dimensions that can incorporate IP intensive capabilities (Fortune Media, 2025). The third family is evidence based composite models used in due diligence, procurement, and risk assessment, where reputation is inferred from documented governance, litigation exposure, compliance maturity, and incident history (Table 3.6).

Table 3.6. Families of reputation models and appropriate IP integration points

Model family	Core measurement logic	Typical data sources	Appropriate IP integration points
Perception based public or stakeholder models	Stakeholder judgments about drivers such as governance and innovation	Surveys, panels, media analytics	IP salience in innovation claims, trust in authenticity, perceived integrity of brand protection
Executive and analyst rankings	Peer evaluation on attributes of admiration and competitiveness	Executive and analyst surveys	IP as evidence of innovativeness, strategic use of assets, global effectiveness
Evidence based composite and due diligence models	Observable capability and risk profile	IP registers, contracts, litigation and enforcement records	Portfolio strength, enforceability readiness, compliance controls, counterfeit and cybersquatting response capability

Sources: systematized by the author

The main methodological conclusion is that IP indicators should be chosen to match the epistemic logic of the model. In survey models, IP should be integrated through stakeholder visible cues and narratives, while in evidence based models, IP should be integrated through auditable artifacts such as filings, governance routines, and enforcement outcomes.

A methodologically coherent integration of IP begins with choosing an integration route that is consistent with the reputation model family. Perception models require indicators that stakeholders can realistically perceive and interpret, whereas due diligence models can incorporate detailed legal and operational evidence. Mixing these logics without discipline can lead to overstating the reputational role of formal registrations or, conversely, ignoring IP governance that is invisible to the public but decisive for partners and investors.

To operationalize IP inside a reputation index, it is useful to define an indicator architecture with three layers: legal strength, organizational

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

capability, and market meaning. Legal strength captures existence and scope of rights, including territorial coverage and maintenance discipline. Organizational capability captures governance processes, including IP strategy, clearance workflows, contract discipline, and incident response. Market meaning captures whether stakeholders interpret IP signals as credible differentiation, trust, and legitimacy.

ISO 56005 provides a practical bridge for the capability layer because it proposes guidelines for supporting the role of IP within innovation management at strategic and operational levels, including the development of an IP strategy that supports innovation (ISO, 2020). Methodologically, this implies that reputation models should treat IP governance maturity as an observable management system, not merely as a count of patents or trademarks. A firm with a smaller portfolio but strong strategic alignment and disciplined processes may be reputationally safer in partnerships than a firm with a large portfolio and weak internal controls, especially in cross border commercialization (Table 3.7).

Table 3.7. IP indicator dictionary for reputation assessment and the logic of measurement

Indicator block	Example indicators	Preferred measurement form	Why it is cross jurisdiction usable
Portfolio integrity	Coverage of core marks and key markets; renewal discipline	Binary and ratio metrics, supported by registers	Registration data is standardized enough for comparison when normalized by business footprint
Governance maturity	Existence of IP strategy; integration into innovation process; clearance workflows	Structured maturity scoring aligned to IP management guidance	Focuses on management system capability rather than local legal technicalities
Enforceability readiness	Evidence preservation playbooks; dispute procedures; response timelines	Process evidence plus time to action metrics	Captures operational resilience, which is comparable even when courts differ
Market integrity and harm prevention	Counterfeit monitoring routines; platform takedown processes; consumer warning protocols	Incident rate trends and control coverage	Connects IP to stakeholder protection, which is reputationally legible across markets
Value linkage	Coherence between brand governance and valuation reporting	Documented assumptions and reporting quality	Encourages transparent link between legal assets and economic meaning

Sources: systematized by the author

Counts are highly sensitive to sector, patenting culture, and local filing incentives, so they should be normalized by market scope, R and D intensity,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

or revenue structure, and complemented by governance and enforceability measures.

Cross jurisdiction comparability improves when IP indicators are constructed as a layered system that separates rights, governance capability, and stakeholder meaning. ISO aligned guidance supports the operationalization of governance maturity as a measurable capability, while ISO 10668 oriented logic helps maintain clarity about how legal and behavioral evidence relates to economic valuation. The result is an indicator set that is auditable and less biased by sectoral differences in filing behavior.

A core challenge is that identical IP portfolios can carry different reputational risk depending on enforcement predictability and procedural effectiveness. In the EU, enforcement harmonization aims to provide a minimum set of measures, procedures, and remedies for civil enforcement across member states, supporting a more standardized protection baseline (EUR-Lex, 2018). Methodologically, this means that in more harmonized environments, external enforcement capacity can be treated as a partial substitute for internal controls, although never a full substitute. In less predictable environments, internal controls and contractual safeguards must carry more weight because external remedies may be slower or less effective (Table 3.8).

Table 3.8. Calibration logic for weighting IP indicators across jurisdictions

Context factor	Observable proxy	Implication for weighting
Enforcement standardization	Presence of harmonized civil remedies and procedures	Increase weight on portfolio integrity and compliance disclosure, reduce extreme reliance on private ordering
Procedural speed and predictability	Typical time to interim measures; availability of evidence preservation	Increase weight on enforceability readiness and documented response timelines
Digital risk exposure	Platform intensity, cross border e commerce reliance	Increase weight on monitoring, takedown capacity, and domain dispute readiness
Market salience of authenticity	High counterfeiting pressure industries	Increase weight on counterfeit prevention and consumer protection protocols
Stakeholder sensitivity	Regulated sectors and high trust industries	Increase weight on governance maturity and auditability of processes

Sources: systematized by the author

Without explicit calibration, the same indicator scores may be interpreted inconsistently across jurisdictions, which reduces reliability and increases bias.

Jurisdictional variability requires a transparent calibration layer that adjusts how IP evidence is interpreted. Harmonized enforcement environments support more consistent external remedies, while weaker

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

environments require greater emphasis on internal governance and contractual safeguards. Calibration improves fairness and predictive validity because it links indicator weights to observable institutional conditions rather than to subjective impressions.

A reputation model that integrates IP should be validated on two levels. First is construct validity, meaning that IP indicators genuinely represent the intended reputation dimension, such as governance or innovation, rather than acting as noisy proxies. Second is predictive validity, meaning that IP related scores correlate with relevant outcomes such as reduced dispute frequency, improved partner confidence, or reduced counterfeit harm (Table 3.9). ISO 10668 emphasizes reporting discipline, data quality, and transparency of assumptions in valuation contexts, and this logic is transferable to reputation modeling because stakeholders often challenge models that are opaque or unverifiable (ISO, 2010).

Table 3.9. Governance workflow for an IP integrated reputation model

Step	What is tested or documented	Deliverable
Indicator specification	Definitions, measurement rules, normalization	Indicator manual and data dictionary
Data integrity	Source reliability, sampling, audit trail	Data provenance log and audit checklist
Calibration justification	Context factors and weights	Weighting rationale memo
Validation	Convergent and predictive tests	Validation report with limitations
Disclosure	Assumptions, confidence bounds, update rules	Methodology statement aligned to reporting discipline

Sources: systematized by the author

This documentation supports both academic rigor and practical defensibility when reputational assessments influence procurement, licensing, financing, or litigation strategy.

Validation and governance are not optional add ons, because IP integrated reputation scores can affect high stakes decisions. Transparent reporting, auditable data provenance, and explicit calibration rules increase legitimacy of the model and reduce the risk that stakeholders interpret the assessment as arbitrary or biased. ISO style reporting discipline strengthens replicability and facilitates cross study comparability.

Methodologically integrating IP into corporate reputation models requires aligning IP indicators with the underlying reputation measurement logic, constructing layered indicators that separate rights, governance capability, and stakeholder meaning, and calibrating interpretation to jurisdictional enforcement conditions. Survey based models can incorporate IP through stakeholder visible cues linked to governance and innovation

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

drivers, while evidence based models can rely on auditable artifacts and enforceability readiness. ISO 56005 supports operationalizing IP management maturity within innovation management, and ISO 10668 provides a disciplined logic for separating legal foundations, behavioral evidence, and value linkage through transparent reporting (ISO, 2020; ISO, 2010). Finally, explicit validation and disclosure are essential for credibility across jurisdictions, especially when results are used in investment, partnership selection, and cross border commercialization decisions.

4. Evidence, monitoring, and enforcement in international disputes: effects on reputation loss and trust recovery. International IP disputes are reputationally consequential because they translate technical legal conflicts into stakeholder perceptions of integrity, competence, and control. In cross border markets, reputation loss is rarely driven only by the infringement itself. It is driven by the visibility of harm, the speed and coherence of the response, and the perceived ability of the firm to prevent recurrence. This is why the institutional design of enforcement and the firm's internal evidence discipline become central inputs for reputation assessment. TRIPS explicitly requires that enforcement procedures permit effective action against infringement, including expeditious remedies to prevent infringements and remedies that constitute a deterrent, which sets a baseline expectation that protection must be operational, not merely declarative (World Trade Organization, 2025). In the EU, the Enforcement Directive similarly frames a minimum set of civil measures, procedures, and remedies for effective enforcement and emphasizes fairness and the avoidance of unwarranted delays (European Union, 2018; European Parliament & Council, 2004). Within this framework, the core methodological issue is how evidence, monitoring, and enforcement actions shape trust trajectories after a public incident.

Evidence is the primary bridge between internal knowledge of infringement and external credibility in disputes, audits, and public communications. Without evidence that is timely, reliable, and properly documented, an enterprise may be unable to obtain interim relief, persuade platforms to act, or communicate responsibly without risking defamation claims or misinformation. The reputational effect is immediate, because stakeholders interpret uncertainty and inconsistent narratives as indicators of poor control. In TRIPS terms, "effective action" presupposes that parties can substantiate infringement and seek remedies that prevent continuation (World Trade Organization, 2025). In EU practice, the legal architecture explicitly includes measures for preserving evidence as part of a broader toolkit of civil enforcement, which encourages early action and supports

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

containment before harm spreads (European Parliament & Council, 2004).

In reputational terms, evidence does not function only as a litigation instrument. It also functions as a governance artifact that enables consistent decision making under pressure. A firm that can demonstrate chain of custody discipline, clear responsibility allocation, and reproducible incident records is usually perceived as more trustworthy by partners and regulators, even before a court outcome. Evidence quality also shapes the ethical dimension of enforcement. Aggressive action without adequate substantiation can be interpreted as abuse of rights, while inaction in the presence of strong evidence can be interpreted as indifference to consumer harm. The practical implication is that evidence governance should be designed as a routine capability, not as an improvised activity triggered only by crises (Table 3.10).

Table 3.10. Evidence architecture in cross border IP disputes and its reputation effects

Evidence category	Typical content	Primary function in disputes	Likely reputation effect if managed well	Likely reputation effect if managed poorly
Rights foundation evidence	Registration extracts, priority records, licensing chain	Establish standing and scope of protection	Signals legitimacy and professionalism	Creates doubts about ownership and diligence
Infringement documentation	Samples, screenshots, technical comparisons, purchase records	Substantiate infringement and material similarity	Enables prompt action and credible claims	Forces vague statements and slows response
Harm and consumer risk evidence	Complaints, safety reports, confusion metrics	Justify urgency and proportionality of response	Shows consumer protection orientation	Appears indifferent or alarmist without proof
Actor attribution evidence	Seller identifiers, domain registrant data, platform logs	Identify responsible parties and routes of distribution	Supports targeted enforcement, reduces collateral damage	Leads to broad accusations and reputational backlash
Process and decision logs	Timestamps, approvals, counsel notes, communications drafts	Demonstrate procedural fairness and consistency	Supports coherent public narrative and governance maturity	Exposes inconsistencies and weak internal control

Sources: systematized by the author

Strong evidence enables proportionate enforcement and precise communication. Weak evidence increases the probability of uncontrolled escalation, inconsistent messaging, and prolonged uncertainty that damages trust.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Evidence discipline is a reputation safeguard because it makes enforcement credible and communications defensible. TRIPS and EU enforcement frameworks implicitly assume that actors can substantiate infringement and seek timely relief, which elevates evidence preservation from a technical legal step to a signal of governance capability (World Trade Organization, 2025; European Parliament & Council, 2004). The higher the quality of evidence, the lower the probability that the firm will either overreact without proof or underreact despite harm.

Monitoring is the preventive counterpart of evidence. It reduces the time between infringement occurrence and organizational awareness, which is crucial because reputational harm grows with exposure time, especially in digital channels. The relevance of monitoring has increased with supply chain complexity and the rise of online trade. OECD reporting highlights that expanding supply chains and e commerce have facilitated illicit trade in counterfeit goods and that such trade poses risks to public safety and harms legitimate business (OECD, 2025). These empirical conditions imply that reputation resilience depends on the ability to detect and contain issues early rather than to litigate after widespread diffusion.

Monitoring should be designed as a multi layer system that covers markets, platforms, and identity infrastructure. Market monitoring includes sampling, distributor auditing, and customs cooperation signals. Platform monitoring includes marketplace scanning, social media ads tracking, and takedown pipelines. Identity monitoring includes domain name watching and abuse detection. The core reputational advantage of such monitoring is not only fewer incidents, but a better ability to demonstrate good faith and consumer protection orientation. When stakeholders see that a firm routinely monitors and acts proportionately, they tend to interpret infringement incidents as external shocks rather than as evidence of internal negligence. The inverse also holds. Repeated incidents with no visible monitoring capacity create an impression of chronic control weakness.

Monitoring reduces reputational volatility by shortening detection time and enabling earlier containment in environments where illicit trade scales rapidly through modern logistics and e commerce (OECD, 2025). A mature monitoring capability also improves credibility because it supports specific, evidence based claims and discourages panic driven communication.

Enforcement is not a single act. It is a portfolio of options that must be chosen according to jurisdictional constraints, evidence strength, and reputational risk. TRIPS frames enforcement as a system that should enable expeditious remedies to prevent infringements and remedies that deter further infringements (World Trade Organization, 2025). In the EU, the

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Enforcement Directive provides a civil enforcement toolkit designed to be effective while remaining fair and not unnecessarily costly or delayed (European Parliament & Council, 2004; European Union, 2018). These frameworks encourage proportionality, which is reputationally important because stakeholders evaluate whether the firm's response is reasonable relative to harm.

Digital enforcement illustrates the logic of proportionality particularly well. Domain name abuse can generate immediate fraud and confusion. The UDRP provides an expedited administrative mechanism for disputes concerning abusive registration and use of domain names corresponding to trademark rights, and ICANN's policy text describes the process as expedited administrative proceedings initiated by a trademark holder through an approved provider (World Intellectual Property Organization, 2025; ICANN, 2020). The reputational significance is that this pathway can remove a misleading identifier without the delays and visibility of full litigation, which can be desirable when the primary objective is rapid consumer protection. At the same time, UDRP outcomes are evidence dependent, which reinforces the centrality of documentation and disciplined claims.

Offline and hybrid enforcement, such as customs actions, civil litigation, and coordinated takedowns, is often necessary for counterfeiting and diversion. OECD and EUIPO reporting indicates the persistence and scale of counterfeit and pirated trade, including an estimate that in 2021 such goods accounted for up to 2.3 percent of global trade and within the EU up to 4.7 percent of total imports, which implies a structurally high baseline risk for brands (OECD, 2025). In this context, enforcement must be continuous and coordinated, because one time actions rarely produce lasting deterrence. From a reputation standpoint, continuity signals seriousness and consumer protection, whereas episodic enforcement followed by silence can be interpreted as symbolic compliance (Table 3.11).

The firm should select pathways that maximize harm containment and deterrence while minimizing unnecessary collateral visibility and procedural delays. Effective enforcement in cross border disputes requires a proportional selection of pathways grounded in evidence and aligned with institutional options such as TRIPS aligned remedies, EU civil measures, and UDRP administrative procedures (World Trade Organization, 2025; European Parliament & Council, 2004; World Intellectual Property Organization, 2025; ICANN, 2020). The reputational outcome depends less on the formality of action and more on whether the action credibly prevents further harm and communicates responsibility.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.11. Enforcement decision matrix in international IP disputes

Primary objective	Typical condition	Preferred pathway	Reputation upside	Reputation risk to manage
Fast consumer protection	High confusion or fraud risk, strong evidence	Platform takedown plus UDRP for abusive domains	Rapid containment, visible responsibility (World Intellectual Property Organization, 2025; ICANN, 2020).	Overstatement without proof, inconsistent messaging
Deterrence of organized infringement	Repeated incidents, distribution networks	Civil enforcement measures, coordinated actions, customs cooperation	Signals seriousness, discourages recurrence (World Trade Organization, 2025).	Escalation costs, jurisdictional fragmentation
Preservation of confidential know how	Risk of disclosure in open proceedings	Targeted actions, protective orders where available, controlled disclosure	Protects innovation narrative and partner trust	Leaks during proceedings, uncontrolled internal access
Reputation repair and reassurance	Public attention, stakeholder anxiety	Evidence based communication plus visible remediation steps	Rebuilds confidence if aligned with responsibility norms	Perceived defensiveness, admitting more than verified

Sources: systematized by the author

Trust recovery is shaped by how stakeholders attribute responsibility and how the firm's response matches these attributions. Situational Crisis Communication Theory proposes that crisis response strategies should be matched to crisis type and perceived responsibility to protect reputational assets, and empirical work has tested how response strategies affect reputation restoration (Coombs, 2007; Claeys et al., 2010). Image restoration research similarly emphasizes that organizational discourse strategies matter for repairing reputation after accusations and crises (Benoit, 1997). In IP disputes, stakeholders typically distinguish between victim type events, where the firm is harmed by external infringement, and preventable governance failures, where weak controls made harm likely. The same infringement can be interpreted in either way depending on the firm's prior monitoring posture and its response quality.

Trust repair scholarship also highlights the role of credible evidence in shifting stakeholder beliefs. Research on trust repair conceptualizes trust restoration as a process that depends on perceptions of integrity, competence, and benevolence, and evidence that clarifies innocence or guilt can be decisive in restoring trust (Kim et al., 2009). For IP disputes, this implies that the firm should avoid speculative narratives and instead communicate verified facts, the protective steps taken, and the prevention measures adopted. Where consumer harm is possible, reassurance must be linked to

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

concrete actions such as takedowns, warnings, and remediation, rather than to generic statements. Where the firm shares responsibility, trust repair requires acknowledgement and demonstrable system improvement, since stakeholders interpret denial in the presence of strong evidence as unethical.

Trust recovery in IP disputes depends on matching response strategy to perceived responsibility and maintaining evidence based communication. Crisis communication and image restoration research indicates that response strategies influence reputational outcomes, while trust repair research emphasizes that credible evidence and corrective actions shape the restoration trajectory (Coombs, 2007; Claeys et al., 2010; Benoit, 1997; Kim et al., 2009).

5. Practical recommendations for companies: IP due diligence, contract models, and protection policies in international operations. A practical approach to protecting IP within reputation assessment begins with the recognition that stakeholders evaluate both legal assets and managerial capability. Therefore, IP due diligence should be designed as a repeatable process, not a one time legal review. ISO 56005 emphasizes integrating IP management into innovation management at strategic and operational levels, which supports the development of institutional routines for identifying, protecting, and exploiting IP (International Organization for Standardization, 2020). For reputation, this integration is valuable because it reduces the risk of accidental disclosure, inconsistent filings, and uncontrolled licensing that can trigger public disputes.

An internationally oriented due diligence program should include at least the following modules. The first module is portfolio mapping and gap analysis, linked to target markets and planned commercialization. The second module is freedom to operate and third party rights screening, especially for marketing, software, and product design. The third module is contract architecture, including confidentiality, licensing, franchising, and technology transfer agreements. The fourth module is digital protection, including domain name strategy, platform enforcement protocols, and incident response plans. The fifth module is disclosure governance, ensuring that external communications about innovation, sustainability, or product claims are consistent with protectable assets and do not unintentionally waive secrecy (Table 3.12).

The practical implication is that reputational resilience depends on documentary discipline. In cross border contexts, documentation is the bridge between internal actions and external credibility.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.12. IP due diligence and policy checklist for international operations

Area	Minimum controls	Evidence that supports reputation assessment
Portfolio governance	Filing strategy, renewal calendar, geographic coverage aligned to markets	Portfolio register, renewal logs, filing rationale documentation
Contract models	NDA templates, licensing terms, quality control clauses, audit rights	Signed agreements, audit reports, license compliance records
Trade secret protection	Access control, classification, employee training, vendor controls	Policies, training logs, access logs, incident reports
Digital enforcement	Domain name strategy, UDRP readiness, platform takedown procedures	Domain inventory, case files, takedown metrics, response timelines
Counterfeit response	Monitoring, customs engagement, channel controls	Monitoring reports, seizure cooperation records, distributor audits
Value and reporting	Brand valuation governance, transparency of assumptions	ISO aligned valuation reports, board level review notes

Sources: systematized by the author

Companies can strengthen both IP protection and reputational stability by institutionalizing IP due diligence as a continuous process and by aligning it with innovation management and brand governance standards. Contract models, trade secret controls, and digital enforcement playbooks reduce cross border exposure to infringement, counterfeits, and misrepresentation. The presence of auditable evidence, such as portfolio registers, training logs, and response metrics, increasingly functions as a reputation asset in itself.

Conclusion. International aspects of IP protection are inseparable from modern assessments of business reputation because IP simultaneously structures legal defensibility and signals governance maturity. Global frameworks such as TRIPS and WIPO administered treaties establish minimum expectations and enable cross border protection pathways, which shape how stakeholders interpret a firm's diligence and integrity. Cross border branding amplifies IP related reputational risks, particularly through counterfeiting, cybersquatting, and inadvertent infringement, making monitoring and rapid response central to trust preservation. Methodologically, IP can be integrated into reputation models through portfolio, enforcement, governance, and value linkage indicators, with standards such as ISO 10668 and ISO 56005 supporting transparency and comparability. In disputes, evidence quality and procedural readiness influence whether reputational harm escalates or converts into a resilience narrative. Practically, firms that operationalize IP due diligence, adopt robust contract architectures, and maintain digital enforcement capabilities are better positioned to protect both intangible assets and stakeholder trust across

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

jurisdictions.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177–186. https://doi.org/10.1016/S0363-8111(97)90023-0
2. Claeys, A. S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the situational crisis communication theory and the moderating effects of locus of control. *Public Relations Review, 36*(3), 256–262. https://doi.org/10.1016/j.pubrev.2010.05.004
3. Coombs, W. T. (2007). Protecting organizational reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*, 163–176. https://doi.org/10.1057/palgrave.crr.1550049
4. EUR-Lex. (2018, June 11). *Enforcement of intellectual property rights* (summary). https://eur-lex.europa.eu/EN/legal-content/summary/enforcement-of-intellectual-property-rights.html
5. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights*. https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng
6. European Parliament and Council of the European Union. (2016). *Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
7. European Union Intellectual Property Office. (2019). *The risks posed by counterfeits to consumers: A qualitative study*. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers/2019_Risks_Posed_by_Counterfeits_to_Consumers_FullR_en.pdf
8. Fortune Media. (2025, January 29). *World's most admired companies*. https://fortune.com/ranking/worlds-most-admired-companies/ Fortune
9. Internet Corporation for Assigned Names and Numbers. (2020). *Uniform Domain-Name Dispute-Resolution Policy*. https://www.icann.org/resources/pages/uniform-domain-name-dispute-resolution-policy-01-01-2020-en

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

10. International Organization for Standardization. (2010). *Brand valuation: Requirements for monetary brand valuation (ISO 10668:2010)*. https://www.iso.org/standard/46032.html
11. International Organization for Standardization. (2020). *Innovation management: Tools and methods for intellectual property management: Guidance (ISO 56005:2020)*. https://www.iso.org/standard/72761.html
12. Kim, P. H., Dirks, K. T., & Cooper, C. D. (2009). The repair of trust: A dynamic bilateral perspective and multilevel conceptualization. *Academy of Management Review, 34*(3), 401–422. https://doi.org/10.5465/amr.2009.40631887
13. Korzhevskyi, I. (2025). Methodological Approaches to Assessing Corporate Reputation and Economic Security of Enterprises. *Economics, Finance and Management Review*, (3(23), 106–118. https://doi.org/10.36690/2674-5208-2025-3-106-118
14. Korzhevskyi, I. (2025). A Conceptual Approach to Enhancing Enterprise Economic Security Under the Influence of Business. *Economy and Society*, (73). https://doi.org/10.32782/2524-0072/2025-73-121
15. Organisation for Economic Co-operation and Development. (2021). *Illicit trade: Misuse of e-commerce and online platforms for trade in counterfeits*. OECD Publishing. https://www.oecd.org/en/publications/illicit-trade-misuse-of-e-commerce-and-online-platforms-for-trade-in-counterfeits_07d1032d-en.html
16. Organisation for Economic Co-operation and Development, & European Union Intellectual Property Office. (2025). *Mapping the global trade in fakes: Global trends and enforcement challenges*. OECD Publishing. https://www.oecd.org/en/publications/mapping-the-global-trade-in-fakes_8b2be95f-en.html
17. Reputation Institute. (2016, March 22). *2016 Global RepTrak® 100: The world's most reputable companies*. https://www.rankingthebrands.com/PDF/Global%20RepTrak%20100%20Report%202016%2C%20Reputation%20Institute.pdf
18. Rindova, V. P., Williamson, I. O., Petkova, A. P., & Sever, J. M. (2005). Being good or being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal, 48*(6), 1033–1049. https://doi.org/10.5465/amj.2005.19573108
19. The RepTrak Company. (2020). *2020 Global RepTrak: A decade of reputation leaders*. https://www.reptrak.com/wp-content/uploads/2022/04/2020-Global-RepTrak-Report.pdf
20. World Intellectual Property Organization. (2025). *Trade secrets*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/trade-secrets
21. World Intellectual Property Organization. (2025). *Summary of the Berne Convention for the Protection of Literary and Artistic Works (1886)*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/ip/berne/summary_berne
22. World Intellectual Property Organization. (2025). *Summary of the Paris Convention for the Protection of Industrial Property*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/ip/paris/summary_paris
23. World Intellectual Property Organization. (2025). *Summary of the Madrid Agreement concerning the international registration of marks*. Retrieved December

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

14, 2025, from https://www.wipo.int/en/web/treaties/registration/madrid/summary_madrid_marks
24. World Intellectual Property Organization. (2025). *Summary of the Patent Cooperation Treaty (PCT) (1970)*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/registration/pct/summary_pct
25. World Intellectual Property Organization. (2025). *WIPO guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*. Retrieved December 14, 2025, from https://www.wipo.int/amc/en/domains/guide/
26. World Trade Organization. (2025). *Agreement on Trade-Related Aspects of Intellectual Property Rights: Part III, enforcement of intellectual property rights*. Retrieved December 14, 2025, from https://www.wto.org/english/docs_e/legal_e/27-trips_05_e.htm

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Section 3.2. Intellectual Property Management in Polygraph Methodology Development Projects: Policies, Procedures, Compliance

Oleksandr Akimov[1]

[1]*Doctor of Sciences in Public Administration, Professor, Honored Economist of Ukraine, Professor, Scientific and Methodological Centre of Personnel Policy of the Ministry of Defence of Ukraine, Kyiv, Ukraine, ORCID: https://orcid.org/0000-0002-9557-2276*

Citation:
Akimov, O. (2025). Intellectual Property Management in Polygraph Methodology Development Projects: Policies, Procedures, Compliance. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions*. 208 p. (pp. 133-150). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-133-150

Abstract. *Polygraph assessment methodologies should be conceptualized as composite intellectual assets rather than as a single protectable method, since they integrate expressive materials, functional workflow logic, confidential know how, and digital implementation components. This structure determines the protection strategy because copyright is limited by the idea versus expression boundary, and software copyright protects the expression of a program rather than the underlying principles that the software operationalizes. As a result, legally robust protection requires a portfolio approach in which each layer of the methodology is aligned with the most appropriate legal instrument and with a corresponding governance mechanism that can be demonstrated in practice. The study aims to systematize legal routes for protecting polygraph methodology components through copyright, trade secrets, and operational controls, while maintaining legitimacy through controlled transparency. The analysis uses a doctrinal and policy synthesis of relevant international and EU frameworks and translates these norms into an operational segmentation model and an evidence readiness logic for enforcement. The results show that protectability increases when methodology content is segmented into public, partner, and restricted components, since this enables principled disclosure without sacrificing confidentiality of calibration and decision rules. The findings also demonstrate that trade secret protection is governance dependent, because enforceability requires proof of secrecy, commercial value derived from secrecy, and reasonable steps to preserve confidentiality, which elevates access discipline and documentation to core protection instruments. In addition, the study identifies evidence readiness as decisive, because copyright and trade secret claims rely on different proof packages, including version histories, secret registers, access logs, and contract documentation. Finally, the study operationalizes reasonable steps as layered controls that map key risks to specific evidence outputs, strengthening cross border defensibility and improving response capacity. The effective legal protection of polygraph methodologies is portfolio based and operational, combining protection of authored expression with secrecy governance, licensing discipline, and evidence preservation embedded into project workflows. Future research should test how particular evidence artifacts, access controls, and licensing constraints influence dispute outcomes, and the long term durability of secrecy in training intensive ecosystems.*

Keywords: *polygraph methodology; intellectual property portfolio; copyright scope; idea expression dichotomy; software copyright; trade secrets; undisclosed know how; reasonable steps; evidence readiness; licensing governance; access control; cross border enforcement.*

ISBN 978-9916-9389-5-9 (pdf)

1. Polygraph methodologies as layered IP assets: what can be protected and how. Polygraph assessment methodologies should be treated as composite intellectual assets rather than as a single protectable "method." In operational terms, a methodology usually includes at least four layers: (1) expressive materials (manuals, protocols, scripts, training content), (2) functional logic (workflow rules, question sequencing logic, decision rules), (3) confidential know-how (interpretation heuristics, calibration thresholds, internal quality assurance routines), and (4) digital implementation (software-assisted capture, processing, reporting, and evidence storage). This decomposition matters because intellectual property law protects different layers through different legal tools, and the failure to separate them creates unrealistic protection claims and weak enforcement positions.

The first boundary is the idea–expression dichotomy: copyright protects expression, not ideas, procedures, methods of operation, or mathematical concepts as such (World Intellectual Property Organization [WIPO], 2025). In practice, this means a competitor may be able to replicate a functional approach while avoiding infringement if they do not copy protectable expression. Consequently, the methodology's defensible core often shifts toward the materials' originality and the governance of non-public know-how.

The second boundary concerns software-supported methodologies. EU law clarifies that only the expression of a computer program is protected, while ideas and principles underlying elements of a program, including interfaces, are not protected by copyright under the specific regime for computer programs (European Parliament and Council, 2009). This is particularly relevant when a polygraph methodology is embedded in tooling that automates scoring assistance, report generation, or pattern comparison. The protectable object is the code and its expressive architecture, whereas the abstract logic of the scoring approach may require confidentiality, contractual controls, or other legal strategies.

The third boundary concerns trade secrets and confidential know-how. Under TRIPS, protection of undisclosed information depends on three criteria: secrecy, commercial value because of secrecy, and reasonable steps under the circumstances to keep it secret (World Trade Organization, 1994). EU law aligns with this approach through the Trade Secrets Directive, which frames trade secrets as protectable business information and sets remedies for unlawful acquisition, use, and disclosure, including breaches of confidentiality duties and duties limiting use (European Parliament and Council, 2016). This alignment supports a coherent cross-border rationale: the more the methodology relies on internal heuristics and calibration, the

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

more the project should invest in proving "reasonable steps," since protectability depends on demonstrable governance rather than on registration.

To make this logic operational, the methodology should be segmented into "public," "partner," and "restricted" components. Public components can be disclosed for transparency, marketing, or training previews without destroying the value of secrecy. Restricted components include the elements that create competitive advantage or reduce error, such as examiner decision heuristics, internal case libraries, calibration rules, and quality control thresholds. Partner components sit between the two and are shared under strict license scope, auditability, and dissemination limitations. This segmentation allows the project to remain credible in compliance contexts while preserving the legal prerequisites for trade secret protection.

The table 3.13 clarifies how typical polygraph methodology components map to the most realistic protection instruments.

Table 3.13. Legal characterization of polygraph methodology components

Component	Primary legal nature	Most realistic protection route	Typical governance requirement
Manuals, protocols, diagrams, training texts	Expression	Copyright	Authorship and version control (WIPO, 2025)
Training videos, slides, tests	Expression	Copyright	Licensing and controlled reuse (WIPO, 2025)
Question sets and structured scripts	Expression plus compilation features	Copyright for wording and selection; secrecy for restricted sets	Tiered access and controlled distribution
Workflow logic and scoring methodology (abstract)	Method of operation	Not protected by copyright as such	Protect refined variants through secrecy and contracts (WIPO, 2025)
Interpretation heuristics and calibration thresholds	Confidential know-how	Trade secret	Reasonable steps and access governance (World Trade Organization, 1994; European Parliament and Council, 2016)
Software implementing capture, analysis, reporting	Expression of program	Copyright for code and structure	Repository governance and clean ownership (European Parliament and Council, 2009)
Method name, certification label, program identity	Distinctive sign	Trademark strategy	Anti-confusion governance and monitoring

Sources: (World Intellectual Property Organization, 2025; World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2009).

Table 3.13 indicates that the strongest protection strategy is portfolio-based, with copyright shielding the expressive layer and trade secrets protecting the competitive core that must remain confidential.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

A second operational question is how to decide, at design time, whether an element should be published, licensed, or kept secret. The decision should be driven by the legal preconditions of trade secret protection and by the reputational need for defensible transparency, particularly when a methodology is used in sensitive evaluations.

Table 3.14. Decision matrix for disclosure, licensing, and secrecy

Decision factor	If high, preferred route	Reason	Practical consequence
Competitive advantage comes from the element	Keep restricted as trade secret	Value depends on secrecy (World Trade Organization, 1994)	Tight access, logs, restricted training cohorts
Element must be publicly explained for legitimacy	Publish expressive explanation, restrict operational details	Copyright covers explanation, secrecy covers heuristics (WIPO, 2025)	Two-layer documentation, public guide plus restricted annex
Element must be shared with partners to operate	License with strict scope plus secrecy controls	Trade secret protection requires reasonable steps (European Parliament and Council, 2016)	NDA, audit rights, no redistribution, breach remedies
Element is embedded in software tooling	Protect code; keep key parameters confidential	Code is protected as expression (European Parliament and Council, 2009)	Repository controls and parameter secrecy

Sources: (World Intellectual Property Organization, 2025; World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2009).

Table 3.14 shows that the same methodology can remain transparent at the level of principles while preserving protectability and enforceability through controlled secrecy of high-value operational details.

Table 3.15. Evidence artifacts needed to support each protection route

Protection route	What must be proven	Core evidence artifacts	Why it matters
Copyright	Ownership, originality, copying of expression	Dated versions, authorship records, publication history, similarity analysis	Supports fast takedown and civil claims (WIPO, 2025)
Trade secret	Secrecy, value due to secrecy, reasonable steps, unlawful use or disclosure	Secret register, access logs, NDAs, tier policies, incident records	Protectability depends on governance performance (World Trade Organization, 1994; European Parliament and Council, 2016)
Software copyright	Expression of program, ownership, infringing reproduction	Repository logs, contributor agreements, dependency licensing ledger	Clean chain of title reduces dispute risk (European Parliament and Council, 2009)
Trademark (if used)	Distinctiveness, likelihood of confusion, unauthorized use	Clearance files, monitoring screenshots, use evidence	Prevents reputational dilution through confusing branding

Sources: (World Intellectual Property Organization, 2025; World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2009).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Finally, a layered IP approach must be "evidence-ready." Copyright and trade secret protection both depend on traceability, but the proof points differ. Copyright disputes emphasize originality, copying, and ownership, while trade secret disputes emphasize secrecy status, reasonable steps, and unlawful acquisition, use, or disclosure (World Trade Organization, 1994; European Parliament and Council, 2016).

Table 3.15 confirms that legal protection is inseparable from documentation discipline, because enforceability requires different proof packages depending on the right invoked.

A polygraph methodology is best protected through structured asset segmentation: copyright protects the expressive documentation and software expression, while trade secrets protect calibration know-how and internal heuristics, provided that secrecy and reasonable steps are consistently demonstrated under TRIPS and EU standards (World Trade Organization, 1994; European Parliament and Council, 2016; WIPO, 2025).

2. Copyright protection of methodological materials: scope, limits, and evidence discipline. Copyright is most effective for polygraph methodology projects when the methodology is expressed in fixed, original materials, such as manuals, structured examiner protocols, training modules, video lectures, and software code. This is because copyright protects the author's expression, while it does not protect ideas, procedures, methods of operation, or abstract principles as such (World Intellectual Property Organization, 2025). In the polygraph context, this boundary is decisive: the functional logic of testing can often be reproduced in another form, whereas the concrete expression of how the method is described, structured, and taught can remain legally protectable. A second core element is originality. In EU copyright doctrine, protection is tied to originality understood as the author's own intellectual creation, a standard articulated in EU case law and applied broadly across subject matter (Court of Justice of the European Union, 2009; European Parliament and Council, 2001). As a result, the practical strengthening of the copyright layer depends on deliberate authorial choices in sequence, explanatory architecture, terminology systems, examples, and didactic design rather than on the method's functional novelty.

A further complication arises when a polygraph methodology is embedded in software, for example scoring assistance tools, report generators, or data capture pipelines. Under the EU Software Directive, only the expression of a computer program is protected, while ideas and principles underlying any element of a program are not protected by copyright (European Parliament and Council, 2009). This implies that code, interface

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

layouts as expressive choices, and documentation can be protected, whereas the underlying scoring logic is more safely managed through confidentiality and contract-based controls. When methodological materials are distributed digitally, additional relevance arises from harmonized EU rules on reproduction and communication to the public, because copying, sharing in closed groups, and hosting on platforms can trigger distinct exclusive rights and exceptions (European Parliament and Council, 2001).

Table 3.16. Copyright scope in polygraph methodology materials: protectable expression versus functional content

Material type	What is typically protected	What is typically not protected	Practical design implication
Manuals and protocols	Structure, narrative, diagrams, examples as expression	The procedure itself as a method of operation	Increase original explanatory architecture and systematization
Training slides and videos	Script, visuals, editing and pedagogical sequencing	General teaching ideas	Separate "public overview" from "restricted operational detail"
Question sets and scripted scenarios	Wording, selection and arrangement	Generic questions and functional constraints	Maintain differentiated restricted sets and controlled distribution
Scoring explanations and rubrics	Explanatory text, illustrative cases	Abstract scoring logic and thresholds	Keep thresholds and heuristics confidential while publishing rationale
Software code and documentation	Code and documentation as expression	Underlying algorithms and principles	Isolate confidential parameters from publishable documentation

Sources: (World Intellectual Property Organization, 2025; European Parliament and Council, 2001; European Parliament and Council, 2009).

Table 3.16 indicates that copyright strength can be increased through intentional authorial design, while the functional core should be positioned for complementary protection, especially through secrecy and contracting.

Because methodology projects frequently involve joint authorship, outsourced content production, and iterative revisions, evidence discipline becomes the bridge between legal theory and enforceability. In EU practice, the originality threshold and the assessment of "copying" often depend on whether the claimant can show a coherent creation history and a stable chain of title. This is why internal documentation must be treated as a core IP governance artifact rather than as administrative overhead. The logic is strengthened by the EU originality approach emphasized in Infopaq, which links protection to the author's intellectual creation and requires a concrete assessment of protected expression (Court of Justice of the European Union, 2009).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.17. Evidence package for copyright enforceability in methodology projects

Evidence artifact	What it demonstrates	Typical use case	Minimum operational standard
Version-controlled master files	Timeline of creation and evolution	Authorship disputes, priority claims	Immutable timestamps, locked releases
Authorship and contribution records	Identity of creators and scope of contribution	Joint work and contractor conflicts	Signed contribution statements
Assignment and licensing agreements	Ownership and permitted use	Enforcement standing and licensing clarity	Mandatory for all contractors and trainers
Distribution register	Controlled dissemination and scope	Defense against implied license arguments	Recipient, purpose, and date tracking
Similarity comparison dossier	Copying of protected expression	Litigation and takedown escalation	Side-by-side mapping of copied fragments

Sources: (World Intellectual Property Organization, 2025; Court of Justice of the European Union, 2009; European Parliament and Council, 2001).

Table 3.17 shows that enforceability relies on the ability to reconstruct the work's provenance and to show controlled dissemination consistent with legitimate licensing expectations.

Methodology projects also face recurring operational risks specific to training and certification ecosystems. Content is often reproduced informally, recorded during trainings, shared inside institutional networks, or modified into derivative materials that circulate without supervision. These patterns require a licensing structure that distinguishes internal use, instructor rights, derivative work permissions, and reuse conditions. In digital distribution settings, clarity on reproduction and making-available behaviors becomes important because unauthorized copying and sharing can be scaled quickly through platforms, even when the initial violation is small (European Parliament and Council, 2001).

Table 3.18. Licensing architecture for polygraph methodology materials

Licensing scenario	Core permission granted	Key restriction	Recommended control
Institutional internal training	Internal use of materials	No redistribution, no recording	Access-limited portals and audit clause
Certified examiner program	Use of restricted materials by credentialed users	No sharing outside cohort	Credential revocation and watermarking
Trainer or franchise model	Delivery rights for training	No derivative works without approval	Pre-approval workflow for updates
Software-enabled methodology	Use of tool plus documentation	No reverse engineering and no extraction of parameters	License keys, logs, and restricted parameter access

Sources: (European Parliament and Council, 2001; European Parliament and Council, 2009).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.18 supports the conclusion that copyright must be operationalized through licensing segmentation, because the main threat is not only copying by competitors but uncontrolled diffusion through legitimate user networks.

Finally, a polygraph methodology often relies on structured collections, including question libraries, case templates, and standardized reporting fragments. Even when a collection is not treated as a "database" in a strict legal sense, the EU framework highlights that selection and arrangement can be protected when it reflects the author's own intellectual creation, and that separate database-related protections may become relevant where systematic compilation is central (European Parliament and Council, 1996; Court of Justice of the European Union, 2009). This reinforces a practical drafting strategy: emphasize original selection logic, categorization, and the explanatory rationale that ties the materials into a coherent authored system.

Table 3.19. Design strategies to maximize protectable expression without disclosing core know-how

Strategy	What it strengthens	What it avoids	Implementation example
Two-layer documentation	Copyright in the "open" explanation	Exposure of thresholds and heuristics	Public guide plus restricted annex
Modular authored structure	Original selection and arrangement	Easy paraphrase by competitors	Unique taxonomy and decision-tree narration
Controlled examples	Demonstrates originality and pedagogy	Disclosure of real case library	Synthetic cases with safeguarded parameters
Separation of parameters from narrative	Protects text while keeping logic secret	Reverse engineering of scoring rules	Narrative rationale with withheld thresholds

Sources: (World Intellectual Property Organization, 2025; European Parliament and Council, 1996; Court of Justice of the European Union, 2009).

Table 3.19 indicates that the most resilient approach is to publish enough expression to ensure legitimacy and teachability, while preserving the competitive core through confidentiality and restricted access.

Copyright protection for polygraph methodology projects is strongest when the expressive layer is intentionally authored, originality is reinforced through structured presentation, and enforceability is supported by provenance evidence, clean chain of title, and segmented licensing for training and digital dissemination (World Intellectual Property Organization, 2025; European Parliament and Council, 2001; European Parliament and Council, 2009; Court of Justice of the European Union, 2009).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

3. Commercial secrecy, trade secrets, and know-how: legal criteria and "reasonable steps". Trade secret protection is the most structurally compatible mechanism for safeguarding the operational core of polygraph methodologies, especially where competitive advantage lies in calibration, interpretation heuristics, internal validation routines, and examiner decision rules that are not intended for public disclosure. Unlike registered IP rights, trade secrets remain enforceable only while confidentiality and control are preserved, which makes governance performance a constitutive element of protection rather than a secondary compliance layer. The minimum international baseline is articulated in TRIPS Article 39, which links the protectability of undisclosed information to secrecy, commercial value because of secrecy, and reasonable steps to keep the information secret. In the EU, Directive (EU) 2016/943 aligns with this logic by defining a "trade secret" through the same three-part test and by providing civil law remedies against unlawful acquisition, use, and disclosure.

A critical methodological implication for polygraph projects is that trade secret claims typically fail when the holder cannot specify what the secret is and cannot demonstrate proportional protective measures. WIPO emphasizes that reasonable steps should not be treated as a formal hurdle but as a practical risk management discipline calibrated to the value of the information and the threat landscape. For methodologies deployed through training ecosystems and institutional clients, this calibration must account for the predictable leakage channels: repeated exposure in trainings, informal reproduction inside corporate or public sector networks, contractor access, and digital storage vulnerabilities. Where disputes emerge, confidentiality preservation in proceedings becomes strategically important, because litigation can otherwise force disclosure of the very information the claimant seeks to protect. The Trade Secrets Directive therefore requires Member States to ensure confidentiality of trade secrets in the course of legal proceedings through obligations on parties and other participants, alongside the possibility of specific confidentiality-preserving measures.

Table 3.20 systematizes the legal test and translates it into proof requirements that can be operationalized in methodology governance.

Table 3.20 suggests that "reasonable steps" should be treated as a designed control system that produces auditable evidence, because the legal definition itself requires a demonstrable governance posture.

Beyond the definition, polygraph methodology projects must anticipate lawful acquisition pathways that weaken enforceability if not managed.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.20. Trade secret legal test and evidentiary proof points for polygraph methodologies

Legal element	Core meaning in practice	Typical proof expected	Polygraph-specific implication
Secrecy	Not generally known or readily accessible in relevant professional circles	Restricted access records; controlled dissemination; "restricted annex" structure	Distinguish public principles from restricted operational rules
Value because of secrecy	Competitive or operational advantage is tied to confidentiality	Business rationale; reliance evidence; differentiation narrative	Show how calibration and heuristics reduce error or improve consistency
Reasonable steps	Proportionate measures under the circumstances	NDAs; access controls; labeling; logs; training restrictions	Demonstrate tiering across manuals, trainings, and client deliverables

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; World Intellectual Property Organization, 2019; World Intellectual Property Organization, 2025).

Under the EU Directive, acquisition is lawful, for example, through independent discovery or by observation, study, disassembly, or testing of a product that is publicly available or lawfully possessed without a duty to limit acquisition. This provision is especially relevant when methodology outputs are packaged as tools, templates, or software features that can be inspected by users. The governance response is to design deliverables so that exposure of functional outputs does not reveal the confidential internal configuration, thresholds, and decision rules that constitute the secret. This is one reason why separating parameters from explanatory narratives, and keeping high-value calibration logic server-side or access-restricted, tends to be more defensible than distributing complete operational rulebooks to broad audiences.

Table 3.21 links common polygraph know-how assets to a risk taxonomy, clarifying where misappropriation pressure is highest.

Table 3.21 indicates that the highest-risk assets are precisely those most likely to be exposed repeatedly, namely through trainings, partner deployments, and routine operational access, which makes human-factor controls and contractual architecture decisive.

The "reasonable steps" requirement becomes actionable when measures are selected as a coherent, layered set that maps to specific risks and produces evidence artifacts. WIPO's guidance frames trade secret management as a plan with steps that include identifying and valuing secrets, assessing risks, applying reasonable measures, and monitoring and reacting to misappropriation or leakage.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.21. Risk taxonomy for polygraph methodology know-how and typical misappropriation channels

Know-how asset	Why it is sensitive	Primary risk channel	Secondary risk channel
Scoring thresholds and calibration rules	Enables replication of accuracy profile	Insider leakage during role transition	Contractor reuse across clients
Interpretation heuristics and decision trees	Encodes expert judgment and consistency	Recording or copying during trainings	Informal sharing inside institutions
Internal case libraries and validation datasets	Demonstrates performance and edge cases	Unauthorized duplication from shared drives	Accidental disclosure via cloud links
Quality assurance protocols and audit rubrics	Enables "certification mimicry"	Partner overreach beyond license scope	Competing programs adopting identical rubrics
Software configuration parameters	Makes tooling replicable	Reverse engineering of client-side components	Credential compromise and scraping

Sources: (World Intellectual Property Organization, 2019; World Intellectual Property Organization, 2025; European Parliament and Council, 2016).

This planning approach is especially suitable for polygraph methodologies, because the asset portfolio changes over time as scripts, thresholds, and training materials evolve. It also supports a proportionality logic: controls for a restricted calibration annex should be more stringent than controls for a general overview brochure, even if both are part of the same methodology package.

Table 3.22 operationalizes reasonable steps into a control catalogue that can be embedded in methodology development and deployment.

Table 3.22. Control catalogue for "reasonable steps" in polygraph methodology projects

Control layer	Measures	Evidence artifact produced	Primary legal function
Asset identification	Trade secret register; component tiering	Dated register; scope definitions	Specifies what is claimed as secret
Access governance	Role-based access; least privilege; cohort rules	Access logs; credential lists	Demonstrates secrecy and control
Contractual controls	NDAs; confidentiality clauses; use limitations	Signed agreements; audit clauses	Establishes duties and breach basis
Document discipline	"Confidential" marking; controlled exports	Watermarked copies; distribution register	Proves notice and controlled dissemination
Technical security	Encryption; secure repositories; monitored sharing	System logs; incident reports	Supports traceability and containment
Training governance	No-recording policy; restricted modules	Attendance logs; policy acknowledgements	Reduces predictable training leakage
Monitoring and response	Leak detection; escalation workflow	Evidence preservation pack	Enables timely remedies

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; World Intellectual Property Organization, 2019; World Intellectual Property Organization, 2025).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.22 supports the conclusion that trade secret protection is governance-intensive but scalable, because each measure both reduces risk and produces proof that the reasonable steps condition is met.

Finally, polygraph methodology disputes require a confidentiality-preserving enforcement stance to avoid "self-defeating litigation," where the attempt to enforce secrecy triggers broader exposure. The EU Directive explicitly addresses this risk by requiring confidentiality obligations in legal proceedings and by allowing measures necessary to preserve confidentiality of trade secrets or alleged trade secrets used or referred to during proceedings. This design makes trade secret enforcement more practicable for methodology holders, provided that the claimant can define the secret precisely, demonstrate reasonable steps, and preserve evidence early. The same Directive also provides for damages appropriate to actual prejudice and specifies factors relevant to assessing damages, which is relevant when disclosure causes both economic harm and longer-term degradation of competitive position.

For polygraph methodologies, trade secret and know-how protection is the legally coherent route for safeguarding calibration, heuristics, and internal validation routines, but it is viable only when the holder can demonstrate the TRIPS and EU three-part test and can show a proportional, evidence-producing system of reasonable steps, including confidentiality-preserving litigation readiness.

4. Contracting, licensing, and enforcement: making protection scalable and dispute-ready. Polygraph methodology projects are implemented through multi-actor ecosystems that typically include developers, certified examiners, trainers, institutional clients, software vendors, and sometimes public authorities. In such settings, intellectual property protection cannot rely only on the abstract existence of rights. It must be converted into operational control over access, permitted uses, and evidence creation, especially because trade secret protection depends on demonstrable secrecy measures and enforceable confidentiality duties (World Trade Organization, 1994; European Parliament and Council, 2016). Contracting and licensing therefore function as the "connective tissue" between copyright in materials, trade secrets in know-how, and the practical reality of repeated dissemination during trainings and deployments.

A robust contractual architecture begins with clear allocation of ownership and authorship for manuals, training modules, templates, and software components, with special attention to contractor-created deliverables and joint development. This is complemented by licensing clauses that define scope (internal use only, named users, geographic limits,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

term), prohibit unauthorized copying and redistribution, and regulate derivative works such as updated protocols or localized training programs. For the confidentiality layer, agreements should define the protected confidential information precisely, impose duties to limit use to authorized purposes, and introduce auditability and incident notification obligations. These elements are directly aligned with the EU trade secrets framework, where unlawful use or disclosure often hinges on breaches of confidentiality duties or contractual duties limiting use (European Parliament and Council, 2016). In parallel, dispute readiness requires drafting that anticipates evidence preservation and proportionate remedies, consistent with EU civil enforcement standards for IP-related disputes (European Parliament and Council, 2004).

The table 3.23 distinguishes the most common agreement types used in polygraph methodology ecosystems and the protection function each one serves.

Table 3.23. Contract stack for polygraph methodology projects and its IP function

Agreement type	Typical parties	Primary IP function	Core operational risk addressed
Authorship and assignment agreement	Developers, contractors, trainers	Secures chain of title for materials and software	Ownership disputes and unenforceable rights
NDA and confidentiality agreement	All collaborators and clients	Establishes secrecy duties and limits use	Trade secret leakage through informal sharing
Methodology license agreement	Provider and institutional client	Defines scope of use and controls redistribution	Uncontrolled diffusion within institutions
Certification and examiner agreement	Provider and certified examiner	Restricts access to “restricted tier” know-how	Credential misuse, copying during practice
Trainer agreement	Provider and trainers	Controls derivative works and recording	Unlicensed updates and content drift
Software terms and access policy	Provider and users	Controls tool access and parameter exposure	Reverse engineering and scraping risks
Incident notification and cooperation addendum	Provider and key partners	Creates rapid containment coordination	Delayed response and evidentiary gaps

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

Table 3.23 indicates that scalability is achieved not by adding more documents, but by ensuring that each agreement produces a specific form of control or evidence that supports later enforcement.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

A common failure pattern in methodology projects is that contracts are drafted as generic templates that do not map to realistic risks. A more reliable approach is clause-to-risk engineering, where each critical clause is justified by a specific threat model and evidence need.

Table 3.24. Clause-to-risk mapping for polygraph methodology licensing and secrecy governance

Clause group	Minimum clause content	Risk it mitigates	Evidence it generates
Definitions of confidential information	Tiered definition with examples and exclusions	Ambiguity that undermines trade secret claims	Clear secret scope and notice to recipients
Purpose limitation	Use only for defined assessments or training	Repurposing methods outside license	Proof of unauthorized use beyond scope
Dissemination limits	Named users, internal network limits, no forwarding	"Institutional leakage" through internal sharing	Distribution trail and breach traceability
No recording and no extraction	Ban recording trainings and extracting parameters	Copying through recordings and screenshots	Policy acknowledgements and compliance basis
Derivative works and updates	Approval workflow for modifications and translations	Uncontrolled adaptations that erode exclusivity	Change logs and authorized update trail
Audit rights and compliance reporting	Audit triggers, remediation timelines	Hidden non-compliance and silent diffusion	Audit reports and corrective action records
Offboarding and credential revocation	Return or destruction, access termination	Leakage at role transition	Offboarding checklist and termination evidence
Incident notification and cooperation	Time limits, containment duties, evidence hold	Delayed response magnifying harm	Incident logs and preservation chain

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016).

Table 3.24 supports the conclusion that enforceability is strengthened when contracts are drafted as operational controls that create predictable evidence outputs, rather than as purely formal legal instruments.

Because polygraph methodologies are often used in sensitive contexts, enforcement must be designed to preserve confidentiality while still enabling effective remedies. The EU trade secrets regime explicitly supports confidentiality-preserving litigation measures, which reduces the risk that enforcement actions inadvertently expose protected know-how (European Parliament and Council, 2016). At the same time, general IP enforcement principles in the EU emphasize effective, proportionate, and dissuasive measures, along with tools for preserving evidence and stopping ongoing infringement, which can be adapted to methodology disputes that involve

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

copyrighted manuals or unauthorized distribution of training content (European Parliament and Council, 2004).

The table 3.25 proposes a dispute-ready enforcement workflow that aligns with confidentiality needs and cross-border practicalities.

Table 3.25. Enforcement workflow for polygraph methodology disputes with confidentiality safeguards

Phase	Key action	Primary objective	Confidentiality safeguard
1. Triage	Classify event: copyright copy, trade secret leak, license breach	Choose correct legal basis early	Limit internal circulation of facts
2. Containment	Revoke access, suspend credentials, stop distribution	Prevent ongoing exposure	Evidence hold and restricted access to records
3. Evidence preservation	Secure logs, versions, agreements, and copies	Support later remedies	Sealed evidence pack with chain-of-custody
4. Notice and negotiation	Send structured notice, demand cessation, propose remediation	Resolve quickly and quietly when possible	Use controlled disclosure of secret details
5. Platform and intermediary steps	Takedown or marketplace reporting where relevant	Rapid removal of distributed copies	Provide only necessary proof materials
6. Litigation readiness	Select forum, request confidentiality measures	Secure enforceable remedies	Protective orders and limited access filing
7. Recovery and hardening	Update controls and training	Reduce recurrence	Post-incident control review and audit

Sources: (European Parliament and Council, 2016; European Parliament and Council, 2004).

Table 3.25 shows that the core enforcement problem is sequencing: confidentiality protection improves when evidence is preserved first, disclosure is minimized, and escalation is proportional to harm.

A dispute-ready strategy also requires a standardized evidence pack. This is particularly important because methodology disputes often include mixed claims, for example a copyright claim for copying manuals and a trade secret claim for leaking scoring heuristics. The table 3.26 offers a structured checklist that can be used as a governance artifact. Table 3.26 indicates that evidence readiness is not a litigation-only practice. It is a continuous governance capability that reduces response time and prevents avoidable disclosure of confidential materials.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.26. Evidence pack checklist for mixed copyright and trade secret disputes

Evidence category	What it contains	Supports which claim	Typical mistake avoided
Chain of title	Assignments, contributor agreements, ownership policy	Copyright and software rights	Lack of standing to enforce
Work provenance	Version history, timestamps, authorship records	Copyright	Inability to show originality and priority
Dissemination control	Distribution register, watermarks, access lists	Both	Defense that content was "freely shared"
Secrecy governance	Secret register, tier policy, training restrictions	Trade secrets	Failure to prove reasonable steps
Access traces	Logs, credential histories, offboarding records	Trade secrets	No attribution or timing evidence
Breach proof	Copies, screenshots, repository snapshots, witness notes	Both	Late collection and spoliation risk
Remedy mapping	Harm narrative, business impact, proposed injunction scope	Both	Overbroad claims that expose secrets

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

Finally, polygraph methodology projects frequently operate across borders through training partners or multinational clients. Cross-border deployment increases the relevance of harmonized legal baselines (TRIPS and EU directives), but it also introduces practical decisions about which remedies are realistic and how to coordinate actions.

Table 3.27. Cross-border deployment scenarios and preferred protection posture

Cross-border scenario	Main risk	Preferred protection lever	Practical priority
Multi-country institutional client	Internal redistribution across affiliates	License scope and auditability	Named-user limits and reporting
Training partner in another jurisdiction	Derivative works and uncontrolled updates	Trainer agreement and update governance	Approval workflow and watermarking
Remote examiner network	Credential misuse and copying	Certification agreement plus access controls	Revocation mechanism and cohort segmentation
Software-enabled methodology abroad	Parameter exposure and reverse engineering	Tool access policy and confidentiality layer	Server-side storage of sensitive parameters
Online diffusion of materials	Rapid mass distribution	Copyright enforcement plus platform steps	Fast takedown and evidence pack

Sources: (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.27 reinforces that cross-border protection is strongest when legal instruments are paired with operational controls that limit dissemination and maintain traceability.

Contracting and licensing translate IP doctrine into enforceable control over dissemination, use, and evidence production. In polygraph methodology projects, this translation is essential because trade secret protection depends on demonstrable secrecy and use-limitation duties, while copyright protection depends on provable authorship, controlled dissemination, and clear licensing scope (World Trade Organization, 1994; European Parliament and Council, 2016; European Parliament and Council, 2004).

Conclusion. Legal protection of polygraph assessment methodologies is strongest when implemented as a portfolio that reflects the layered structure of the asset. Copyright is effective for manuals, training content, and software expression, but it does not confer exclusivity over procedures or methods of operation, which makes the confidentiality layer essential. Trade secret protection and know-how governance are therefore central, because TRIPS and the EU Trade Secrets Directive provide a coherent test grounded in secrecy, value, and reasonable steps, and they attach legal consequences to unlawful acquisition, use, or disclosure, including breaches of confidentiality and use-limitation duties. Finally, contracting and enforcement readiness transform rights into operational capability, because licensing scope, access governance, and rapid evidence preservation determine whether remedies are achievable without unnecessarily expanding disclosure of the very information that must remain confidential.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

References:

1. Akimov, O., & Andrusiak, M. (2025). Professional standardization of polygraph examiner's psychophysiological competencies in the context of ukraine's national security. *Society and Security*, (2(8), 72–79. https://doi.org/10.26642/sas-2025-2(8)-72-79
2. Akimov, O. O., Andrusiak, M. V. & Rusetskyi, R. Y. (2025). Tools for enhancing personnel security under martial law: an interdisciplinary approach to polygraph application. *Efficiency of Public Administration*, *1*(82/83), 86–93. https://doi.org/10.36930/508211
3. Court of Justice of the European Union. (2009, July 16). *Infopaq International A/S v Danske Dagblades Forening* (Case C-5/08) [Judgment]. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62008CJ0005
4. European Parliament and Council of the European Union. (1996, March 11). *Directive 96/9/EC on the legal protection of databases*. *Official Journal of the European Communities*, L 77, 20–28. EUR-Lex. https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng
5. European Parliament and Council of the European Union. (2001, May 22). *Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*. *Official Journal of the European Communities*, L 167, 10–19. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
6. European Parliament and Council of the European Union. (2004, April 29). *Directive 2004/48/EC on the enforcement of intellectual property rights*. *Official Journal of the European Union*, L 157, 45–86. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0048
7. European Parliament and Council of the European Union. (2009, April 23). *Directive 2009/24/EC on the legal protection of computer programs (codified version)*. *Official Journal of the European Union*, L 111, 16–22. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2009/24/oj/eng
8. European Parliament and Council of the European Union. (2016, June 8). *Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. *Official Journal of the European Union*, L 157, 1–18. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
9. World Intellectual Property Organization. (1996, December 20). *WIPO Copyright Treaty (WCT)*. WIPO Lex. https://www.wipo.int/wipolex/en/treaties/textdetails/12740
10. World Intellectual Property Organization. (2019). *Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps"*. *WIPO Magazine* (Issue 5/2019). https://shorturl.at/9IM2Q
11. World Intellectual Property Organization. (2025). *Copyright*. Retrieved December 15, 2025, from https://www.wipo.int/en/web/copyright
12. World Trade Organization. (1994). *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)* (Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization). https://www.wto.org/english/docs_e/legal_e/27-trips.pdf

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Section 3.3. Intellectual Property Rights in the Digital Age: Challenges Posed by Artificial Intelligence and Digital Platforms

Inga Bochkova[1]

[1]*Ph.D. (Law), Senior Lecturer of the Department of Patent Science and Fundamentals of Law Enforcement Activities, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-0522-2908*

Citation:
Bochkova, I. (2025). Intellectual Property Rights in the Digital Age: Challenges Posed by Artificial Intelligence and Digital Platforms. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions.* 208 p. (pp. 151-169). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-151-169

Abstract. *The rapid diffusion of artificial intelligence in creative, scientific, and commercial environments is reshaping the practical meaning of intellectual property protection, especially where digital platforms mediate creation, dissemination, and monetization. In this setting, regulatory debates increasingly shift from the legal status of AI outputs toward transparency duties, content labelling, and accountability for the datasets and processes that enable AI generation. The study aims to identify priority directions for Ukraine's future legal regulation of intellectual property in response to AI deployment, taking into account European integration and the emerging EU governance architecture for AI and copyright in the digital environment. The study combines doctrinal legal analysis of EU and Ukrainian sources with comparative legal assessment of regulatory models. It also uses content analysis of platform policies, analytical reports, and selected court-related materials to evaluate how transparency, copyright compliance, and labelling mechanisms work in practice, supported by aggregation of open indicators on AI readiness and regulatory dynamics. The analysis substantiates that the EU model is evolving as a coherent system in which the AI Act interacts closely with the DSM copyright framework, creating an institutional infrastructure for copyright compliance through transparency, labelling, and publication of aggregated information about training data. Particular attention is devoted to obligations for providers of general-purpose AI models, including compliance policies, procedures for rightholder claims, and respect for reservation of rights mechanisms, while preserving protections for trade secrets. For Ukraine, the AI Act functions as a regulatory benchmark for AI governance and as a practical basis for harmonizing intellectual property regulation, especially regarding access to evidence of potential infringements and the balancing of transparency with confidentiality. Future research should develop enforceable procedural tools for evidence access under confidentiality safeguards, evaluate the effectiveness of labelling and training-data summaries in dispute prevention, and test implementation pathways for harmonized standards in national practice.*

Keywords*: AI Act; intellectual property; digital platforms; generative AI; content labelling; training data; transparency; disclosure summaries; copyright compliance; reservation of rights; trade secrets; EU harmonization.*

ISBN 978-9916-9389-5-9 (pdf)

1. The path of transformation of doctrinal and legislative approaches to the regulation of intellectual property law. The rapid development of digital technologies and artificial intelligence (AI) systems has significantly transformed traditional approaches to the legal regulation of intellectual property (IP). Just a few years ago, scholarly and practical discussions primarily focused on determining the legal regime of objects generated by artificial intelligence, in particular on establishing their copyright attribution, the possibility of recognising the results of artificial intelligence activity as protectable objects, and the role of human involvement in the creation of such results.

However, with the further deployment of generative models and the widespread use of artificial intelligence systems across creative industries, science, education, and business, the focus of legal analysis has gradually shifted. Priority is increasingly given not only to the legal status of the final output, but also to the process of its creation – specifically to the need for labelling content generated or modified with the involvement of artificial intelligence, as well as to the disclosure of information regarding the training data used.

The impact of artificial intelligence on human rights and intellectual property has long remained at the centre of attention of scholars, theorists and practitioners in the fields of law, ethics, technology and privacy. Academic research has examined the moral and ethical foundations of AI use, the challenges posed to legal regulation, the transformation of traditional legal institutions, as well as the technological aspects of AI systems and their influence on privacy, individual autonomy and the protection of creative outputs. A significant body of this scholarship has contributed directly to the development of the European Union's contemporary approach to the regulation of artificial intelligence.

A substantial contribution to the European ethical and legal discourse on AI has been made by Gry Hasselbalch, who was directly involved in the development of the EU's ethical guidelines for artificial intelligence and explored their relationship with human rights and data protection (Hasselbalch, 2019). In the field of intellectual property and European law, particular attention has been drawn to the work of scholars from Leiden University, notably Ana Ramalho, who advances the concept of a special legal regime for outputs generated by artificial intelligence systems and analyses the limits of applying classical copyright constructs in the digital age (Ramalho, 2021). Her research provides a solid theoretical foundation for ongoing debates on authorship, originality and the lawful use of AI-generated content.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Within the Ukrainian legal context, issues relating to the regulation of digital technologies, intellectual property, and the adaptation of European standards have also been actively examined. In particular, Justice of the Supreme Court Vasyl Krat, in his academic and practice-oriented works, focuses on the evolution of civil law institutions under the influence of digitalisation and emerging technologies. (Krat, 2024). Petro Bilyk (Bilyk, 2024), Liubov Maidannyk (Maidannyk, 2024) and other Ukrainian scholars analyse recent developments in national legislation, clarify the substance and expected effects of implementing EU legal acts in the fields of copyright, data protection and digital markets, and highlight the risks associated with fragmented or selective transposition of European norms.

Special importance should also be attributed to the contributions of practitioners, consultants and developers of the terminological glossary in the field of privacy and artificial intelligence (including D. Chumachenko, D. Mishkin, O. Andriienko, O. Krakovetskyi, among others) (Ministry of Digital Transformation of Ukraine, 2024). Their work, as well as their participation in the preparation of White Papers, recommendations and advisory documents, has facilitated the development of a shared conceptual framework and a practical understanding of the challenges arising from the use of AI in both the public and private sectors.

At the same time, most of the aforementioned studies remain fragmented and focus on specific, narrowly defined aspects – ethical, technological, copyright-related or private-law issues. Moreover, the legal regulation of artificial intelligence is inherently dynamic: the European Union is gradually introducing new regulatory instruments, including the Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, AI Act) and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (Framework Convention on Artificial Intelligence), which necessitates the continuous updating of scholarly approaches. Against this background, the present study aims to systematise existing research, align it with the latest stages of European law-making, and develop a coherent vision of possible directions for legal regulation in Ukraine in the context of European integration. The practical value of this research lies in the development of conceptual and practice-oriented recommendations for the harmonization of Ukrainian legislation with European Union law, taking into account Ukraine's obligations within the EU integration process, ensuring an adequate level of protection for the rights of rightholders, and creating the

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

necessary preconditions for the sustainable development of innovation and the digital economy.

In this context, particular relevance is acquired by issues concerning the lawful use of copyrighted works and related rights objects for the training of artificial intelligence models, the scope of the obligation to disclose information about the sources of such data, and the need to maintain a fair balance between the interests of rightholders and the demands of innovative development. These issues are already receiving normative consolidation at the level of the European Union, notably through the formation of a new regulatory framework for artificial intelligence, which significantly affects the system of intellectual property protection in the digital environment.

Accordingly, the study of the legal regime of intellectual property in the digital age acquires a new substantive dimension, shifting from debates focused primarily on authorship and protectability towards the analysis of transparency, accountability and regulatory requirements imposed on entities that develop, deploy and use artificial intelligence systems.

To achieve the stated objective, the study pursues the following research tasks: to analyse contemporary approaches in legal doctrine and law-enforcement practice to the regulation of intellectual property objects created with the use of artificial intelligence; to examine the evolution of the legal discourse on the status of AI-generated outputs – from determining their legal regime to addressing issues of labelling and transparency of origin; to analyse the provisions of European Union legislation (in particular, the Artificial Intelligence Act and related instruments) concerning content labelling, disclosure of training data and the protection of rightholders' interests; to assess the impact of digital platforms and generative AI models on the intellectual property protection system; to identify the key risks and challenges for Ukraine's national intellectual property regime arising from the use of artificial intelligence; and to substantiate possible directions for the adaptation and harmonisation of Ukrainian legislation with European Union law in the field of intellectual property under conditions of digital transformation.

2. Implementation of European AI legislation into national law: a two-stage approach. The contemporary approach to the development of national legislation in new and technologically complex fields is increasingly based on awaiting legal solutions developed at the level of the European Union. It is within the European legal space that the initial conceptualisation of societal and technological challenges takes place, along with the development of conceptual approaches and regulatory models that subsequently serve as reference points for national legal systems. Thereafter,

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

states adapt these approaches to their domestic legal frameworks, either in a directive manner – through the adoption of binding legislative acts – or in a soft and flexible form, through the elaboration of non-binding policy instruments, in particular so-called "white papers".

This phased approach allowing time for businesses and other stakeholders to adapt, as well as for assessing the practical results of the application of European legislation, which helps to minimise regulatory risks and enhance the effectiveness of legal regulation. This approach has been adopted by the Ukrainian legislator in response to contemporary challenges, including the protection of personal data in view of the technological capacity to process large volumes of data, including for marketing purposes, as well as the regulation of the use of artificial intelligence across all spheres of public life. While Ukraine already had a basic legislative framework in the field of personal data protection, the Law of Ukraine "On Copyright and Related Rights" (No. 2811-IX, 2022) a different path has been chosen with regard to AI. In this area, the legislator has initiated the development of a *White paper on the regulation of artificial intelligence in Ukraine* (Ministry of Digital Transformation of Ukraine, 2024) (*White paper)* and is awaiting the emergence of practical experience in order to identify those manifestations of AI use that will require legal regulation.

It should be noted that the content of EU legislation regulating the use of artificial intelligence closely correlates with concerns regarding potential violations of fundamental rights, particularly the right to privacy (including the protection of personal data) and intellectual property rights. In addition, challenges related to the information security of individuals and the state, as well as ethical issues surrounding the use of AI, have emerged. These concerns justify the introduction of legislative prohibitions or strict restrictions for businesses intending to deploy products or services that operate on the basis of artificial intelligence systems.

The most advanced European legislation forming the regulatory framework for the use of artificial intelligence, the protection of intellectual property rights, and the safeguarding of fundamental human rights and freedoms against AI-related risks is based on several key EU instruments. These include the AI Act, Directive (EU) 2019/790 on Copyright in the Digital Single Market (DSM Directive), and the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. The analysis of these acts provides a starting point for understanding both the existing and future regulation of these issues in Ukraine.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

The DSM Directive has been implemented by Ukraine, and the relevant legislative framework has been fully adopted in compliance with the Directive's provisions ahead of the originally planned deadline of 31 December 2025. The EU Directive on Copyright in the Digital Single Market (Directive (EU) 2019/790) was adopted in response to profound changes in the ways content is created, disseminated, and consumed in the digital age. Its key innovations aim to achieve a balance between the rights of authors and rightholders and the interests of digital platforms and users. Among the most significant provisions are the introduction of a neighbouring right for press publishers (the so-called press publishers' right), new rules on the liability of online platforms for user-generated content (Article 17), as well as specific exceptions for text and data mining, which are of fundamental importance for the development of artificial intelligence and scientific research. The Directive also strengthens transparency requirements in relations between authors and entities that commercially exploit their works.

The expected effects of implementing the DSM Directive include a redistribution of responsibility in the digital environment. Large content-sharing platforms can no longer fully shift the risks of copyright infringement onto users and are required either to obtain appropriate licences or to introduce effective mechanisms for preventing infringements. At the same time, the Directive is intended to strengthen the bargaining position of creators and rightholders vis-à-vis platforms, ensure fairer remuneration, and enhance transparency in the use of works. However, the implementation of these provisions in EU Member States has also prompted intense debates regarding the risks of excessive content filtering and potential restrictions on freedom of expression.

The approximation of Ukrainian IP legislation to the standards of the DSM Directive is reflected in the adoption of an updated Law of Ukraine "On Copyright and Related Rights", the development of regulation governing collective management organisations, and the legislator's increased attention to issues of digital content use and the liability of online services. As a result of active legislative activity, normative and institutional preconditions have been established for further consideration of DSM Directive provisions in the context of Ukraine's adaptation to the EU Digital Single Market.

As regards the direct regulation of artificial intelligence activities, Ukraine's national regulatory framework on AI is currently at an early, formative stage characterised by planning and preparatory measures. In parallel with the development and adoption of the AI Act at the EU level,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Ukraine is implementing a two-stage preparatory process aimed at the future implementation of the provisions of this instrument.

The first stage, which is expected to be completed by 2026, is characterised by the creation and implementation of non-legislative instruments designed to assist relevant sectors of business in preparing for forthcoming mandatory regulation. At this stage, it is envisaged to develop, adapt and introduce such instruments as a regulatory sandbox, a methodology for assessing the impact of AI on human rights, AI labelling tools, as well as soft-law instruments, including voluntary codes of conduct and general as well as sector-specific guidelines.

Examples of such soft-law instruments include advisory and recommendation-based acts issued by ministries and governmental bodies, published either in final form or for public consultation. In particular, the White Paper on Artificial Intelligence (White Paper) was published in June 2024; the Recommendations on Responsible Use of AI: Intellectual Property Issues (Ministry of Economy, 2024) and Human Rights in the Age of Artificial Intelligence: Challenges and Legal Regulation (Ministry of Digital Transformation & the Ombudsman's Office, 2024) were published in November 2024; and the Glossary of Terms in the Field of Artificial Intelligence was released in December 2024. In addition, a Roadmap for the Regulation of Artificial Intelligence in Ukraine was developed, which defined the above-mentioned two-stage approach. In 2025, several sector-specific guidelines were also made publicly available, including the Guidelines for the Responsible Use of Artificial Intelligence for Legal Professionals (Ministry of Digital Transformation, 2025) and the Guidelines for the Responsible Use of Artificial Intelligence for Media (Ministry of Digital Transformation, 2024).

After providing businesses with sufficient time and appropriate preparatory tools, and after building the necessary regulatory capacity within the state, the development and adoption of a law analogous to the EU Artificial Intelligence Regulation is envisaged. According to the position expressed by the authors of the White Paper, Ukraine's future AI law should not contradict the EU AI Act but, on the contrary, should serve as its national legislative embodiment. Accordingly, in order to achieve the objectives of this study, the analysis will focus on the provisions of the said Regulation.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.28. Two-stage preparatory process for the future implementation of the provisions of the AI Act in Ukraine

Stage	Planned measures	National legislation acts to be adopted during implementation
1st stage	It is envisaged that tools such as a regulatory sandbox, a methodology for assessing the impact of AI on human rights, AI labeling tools, and soft law tools such as voluntary codes of conduct and general and sectoral recommendations will be developed, adapted, and implemented.	White Paper on Artificial Intelligence (June 2024, developed by the Ministry of Digital Transformation of Ukraine), Glossary of Terms in the Field of Artificial Intelligence (December 2024), Roadmap for the regulation of artificial intelligence in Ukraine Sectoral recommendations: Recommendations for the responsible use of artificial intelligence for lawyers (July 2025), Recommendations for the responsible use of artificial intelligence for the media (January 2024)
2nd stage	Development and adoption of a law analogous to the AI Act, which should not contradict the EU Regulation and should be its expression in national legislation.	The Law of Ukraine on Artificial Intelligence; other legislation of Ukraine brought into line with this law

Source: systematized by the author.

3. General characteristics of the AI Act as a foundational act regulating the functioning of AI systems and their impact on the rights of intellectual property rights holders. On 1 August 2024, the EU Artificial Intelligence Act (AI Act) entered into force, establishing a comprehensive regulatory framework governing all aspects of the use of artificial intelligence, from development to end-user deployment. This far-reaching AI regulation applies across all 27 EU Member States and is expected to have a potential "Brussels effect," whereby EU regulatory practices are implemented or mirrored globally.

The AI Act introduces a broad definition of artificial intelligence systems and, accordingly, extends its requirements to a wide range of uses of such systems. Under the AI Act, AI systems include any systems capable of making decisions autonomously (with a certain degree of autonomy) and demonstrating adaptability after deployment. Such systems, pursuing explicit or implicit objectives, are able to analyse input data and generate outputs – such as predictions, content, recommendations, or decisions – that may influence physical or virtual environments. In other words, they perform tasks that previously required human intervention. This definition encompasses both narrowly specialised models and general-purpose AI systems (GPAI) (Article 3).

In its approach to regulating the use of AI in business, the AI Act is comparable to the General Data Protection Regulation (GDPR) and its approach to personal data processing. Both legal instruments require the

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

adoption of a risk-based approach to the analysis of business processes, the designation within organisations of responsible persons for monitoring, controlling, and advising employees on the use of relevant technologies (AI or personal data), interaction with public authorities on compliance matters, as well as the imposition of significant administrative fines for non-compliance.

With regard to risk assessment and the imposition of restrictions or prohibitions, GDPR prohibits the processing of sensitive personal data, while other categories of data may be processed only on the basis of defined legal grounds. By contrast, the AI Act prohibits the use of AI systems classified as presenting an unacceptable level of risk (the fourth risk category) (Article 5). Examples of prohibited practices include AI systems used for behavioural manipulation, social scoring, and biometric categorisation. Such AI systems are almost entirely prohibited due to their potential threat to society and to individual fundamental rights. The remaining three risk tiers comprise: minimal-risk systems, for which legal regulation relies primarily on voluntary codes of conduct aimed at ensuring appropriate use; limited-risk systems, which are subject to transparency obligations, including mandatory disclosure to users that AI is being used in a given product or service; high-risk systems, which are subject to strict regulatory requirements designed to ensure safety, fundamental rights protection, and compliance with established standards.

Each risk category entails specific requirements relating to safety, transparency, and ethical use. As with GDPR, the context of use and the specific functions performed by AI within a product are of decisive importance. The principle of ensuring an individual's right to human oversight or review of automated decision-making applies; however, while GDPR frames this as a right of the individual, under the AI Act, where AI does not merely provide technical assistance in organising processes (such as chatbot functionality) but instead makes decisions affecting individuals, the system is likely to qualify as high-risk or even prohibited. Consequently, such systems may either be disallowed entirely or permitted only under strict regulatory conditions.

In Ukrainian regulatory practice, the classification of risk levels associated with AI systems is, for the time being, outlined in the act of the Ukrainian Parliament Commissioner for Human Rights entitled Human Rights in the Age of Artificial Intelligence (Ministry of Digital Transformation of Ukraine & Office of the Ombudsman of Ukraine, 2024). This document proposes a four-tier classification of AI systems, distinguishing between: *AI systems with minimal or no risk*, in which AI is

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

used as a tool for performing routine tasks, the outcomes of which do not affect individual rights and primarily serve to accelerate preparatory processes; AI *systems with limited risk*, where decision-makers use AI while retaining control over their queries and maintaining the ability to reject AI-generated outputs and make independent decisions at any time; *High-risk AI systems*, where a specific process is carried out entirely by an AI-based computer program, resulting in automated decision-making that directly affects the rights of data subjects.

In such cases, AI systems must comply with mandatory requirements and undergo conformity assessment procedures, and both providers and users of these systems are subject to clearly defined obligations.

Prohibited AI systems, which include technologies that may pose a threat to individuals or society as a whole, such as those used for surveillance, manipulation, propaganda, or targeting vulnerable social groups.

Thus, the AI Act lays down the fundamental rules for businesses regarding the use of AI systems, based on principles of transparency and good faith. As regards the protection of intellectual property, the Act addresses these issues only indirectly; however, through its regulatory approach, it shifts the overall vector of intellectual property protection.

In particular, the transparency obligations established by Article 50 of the AI Act require that, when using certain categories of AI systems – including those that interact with humans, generate or modify content (text, images, video, audio), or produce deepfake content – users must be informed that the content has been created or modified by artificial intelligence, where this is not otherwise apparent. This provision introduces, for the first time at the level of pan-European regulation, a mandatory disclosure of the artificial origin of creative outputs. Such disclosure directly affects the determination of authorship, the good-faith use of content, and the evidentiary framework in copyright infringement proceedings. Transparency is thus framed not as an element of copyright law per se, but as a preventive tool for the protection of intellectual property rights, aimed at reducing the risk of deception as to the origin of a work.

A second important requirement of the AI Act that indirectly concerns intellectual property law is the obligation to label AI-generated content. Pursuant to paragraphs 2–4 of Article 50 of the AI Act, providers and deployers are required to label the results of synthetic content generation in a machine-readable format as “AI-generated” or “AI-manipulated.” For deepfake content, enhanced disclosure requirements apply. From the perspective of intellectual property protection, these requirements do not

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

themselves identify the right holder; however, they significantly influence the legal regime governing the use of such content. In effect, a new criterion for classifying creative outputs is emerging, distinguishing between works that are: created by a human, created with the assistance of AI, and fully generated by AI. In the future, this differentiation will have consequences for licensing practices, the application of presumptions of authorship, and the assessment of originality.

It is worth noting that the only – highly cautious – legislative attempt by the Ukrainian legislator to regulate the legal regime of copyright objects created using AI does not conflict with the above-described provisions of the AI Act. This refers to Article 33 of the Law of Ukraine "On Copyright and Related Rights" of 1 December 2022 No. 2811-IX, which introduces a sui generis right for non-original objects generated by a computer program. The content of this provision also reflects a differentiation between original works, non-original works generated by a computer program, and works created with the assistance of a computer program that are nonetheless considered original.

These provisions already have practical implementation. Rubryka (2024) reports that the Ukrainian IP Office granted copyright protection to works including AI-generated images for the first time. These included a children's book and a poetry collection illustrated with AI-generated images. The Office emphasized that Ukrainian legislation grants copyright protection only to those images created by a human; if images are generated exclusively by AI, copyright does not arise.

As for the doctrinal approach to determining the legal regime of works created autonomously by AI or by AI under human instructions, Judge Vasyl Krat of the Civil Cassation Court of the Supreme Court of Ukraine has argued that Article 33 of the Law "On Copyright and Related Rights" should be interpreted in light of the understanding that objects generated by a computer program do not fit within the traditional paradigm of copyright law; instead, the legislator classifies them as a form of "quasi-copyright." The sui generis rights regime for non-original objects generated by a computer program (Article 33 of the Law of Ukraine "On Copyright and Related Rights") is only analogous to copyright, but is not copyright in essence (Krat, 2024).

Accordingly, this provision should not create inconsistencies with the legislation to be developed at the second stage of implementation of the EU AI Act, particularly with respect to the regulation of the use of AI systems.

Another important aspect associated with the transformation of approaches to the substance and protection of intellectual property is the

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

requirement to disclose information about training data as a response to the copyright crisis. Pursuant to Article 53 of the AI Act, providers of general-purpose AI models, including generative models (GPAI), are required to prepare and make publicly available a sufficiently detailed summary of the content used for training and to act in compliance with EU copyright law, including the "reservation of rights" mechanism under Directive (EU) 2019/790. At the same time, in order to ensure a regulatory compromise between the interests of right holders and AI developers, providers are not required to disclose specific datasets or a complete list of sources, and the protection of trade secrets is expressly safeguarded.

As a result, right holders are provided with a minimum tool for assessing the risk of use of their protected works and for substantiating potential legal claims arising from the use of those works by AI systems. In international judicial practice, cases have already emerged in which the disclosure of training data was sought to prove the presence or absence of use of intellectual property-protected materials.

Notably, in the copyright dispute between OpenAI and The New York Times (NYT.N), along with other media organisations, a federal judge in Manhattan ordered OpenAI to produce millions of anonymised ChatGPT user chat logs. The judge held that 20 million logs were relevant to the media organisations' claims and that their disclosure would not threaten user privacy, as several layers of protection were in place due to the highly sensitive and private nature of much of the disclosed data. The plaintiffs' claims were based on the assertion that OpenAI's business model relies on data produced by journalists and that such data had effectively been misappropriated by AI systems. The court ordered OpenAI to produce the logs within seven days of removing users' identifying information (Brittain, 2024).

Another prominent case involving alleged violations of the intellectual property rights of individuals whose works were used as training data is the lawsuit filed by a group of visual artists against Stability AI, Midjourney, DeviantArt, and Runway AI. On August 12, U.S. District Judge William Orrick of California ruled that the artists had plausibly alleged that the companies infringed their rights by unlawfully storing copyrighted works, and that Stable Diffusion, the AI image generator at issue, may have been built "to a significant extent on copyrighted works" and was "created to facilitate that infringement by design." The lawsuit has been allowed to proceed to discovery, during which the artists may obtain information on how the AI companies collected copyrighted materials used to develop their image-generation systems (Whiddington, 2024).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Taking into account the existing precedents in both theory and practice of applying legislation on the disclosure of training data, it can be concluded that the provisions of the AI Act, although they will not create a mechanism for the automatic verification of compliance with copyright or personal data protection rights, will nevertheless provide opportunities for the application of further mechanisms for the protection of individual rights.

An analysis of the AI Act's provisions on trade secrets indicates that a balance is embedded between transparency and the protection of commercial secrets. The AI Act expressly stipulates that compliance with transparency obligations must not lead to the disclosure of trade secrets. In order to achieve the objectives of the AI Act, supervision and monitoring of compliance with rules applicable to artificial intelligence systems – particularly with regard to the use of general-purpose AI models and systems – will be carried out by the European AI Office, without interference in internal algorithmic solutions.

Table 3.29. Key Aspects of the AI Act

New Rule	Description	AI Act Article
Labelling / watermarking requirement	An obligation is introduced to inform users that content has been generated or substantially modified by AI (including deepfakes and synthetic images, audio, video, and text), in a machine-readable or other appropriate form. The aim is to prevent deception and misuse.	Article 52
Balance of data disclosure	Disclosure of information about AI systems (including GPAI) must be sufficient to ensure transparency and oversight, while avoiding excessive interference with providers' rights and preventing the disclosure of sensitive information.	Article 53(1), Recitals
Protection of trade secrets	The AI Act explicitly provides that compliance with transparency and disclosure obligations (including those related to training data) must not undermine the protection of trade secrets and confidential business information.	Article 53(1), Recitals
Disclosure of training data	Providers of general-purpose AI models (GPAI) are required to prepare and make publicly available a summary of the training data used, with particular regard to compliance with copyright law and the *reservation of rights* mechanism under Directive (EU) 2019/790.	Article 53(1)(d)
Transparency principle	Transparency is established as a cross-cutting principle of AI regulation: users and regulators must be informed about the functioning, capabilities, and limitations of AI systems, especially in cases involving human–AI interaction or AI-generated content.	Articles 13, 52
Establishment of a supervisory authority (AI Office)	The European AI Office is established as a specialised EU-level body responsible for supervising general-purpose AI models, coordinating enforcement, developing standards, issuing guidance, and ensuring uniform application of the AI Act.	Articles 64–66

Source: systematized by the authors.

Summarizing the analysis of the AI Act in the context of intellectual property regulation, it should be noted that in the modern digital era

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

intellectual property law operates at the intersection of three regimes: copyright, patent and trade secret protection, and regulatory transparency. The AI Act does not priorities any single regime but instead employs a balancing regulatory approach, which is characteristic of contemporary EU legislation.

4. The role of large digital platforms in protecting intellectual property rights. In the context of the emergence and prevention of challenges related to the use of artificial intelligence, an important role is assigned to "major players" – large digital platforms which, according to the IOT Analytics 2023 study, account for 84% of the AI market. These include OpenAI (39%), Microsoft (30%), AWS (8%), and Google (7%). In order to implement the provisions of the AI Act, the European Commission developed and published a Code of Practice for General-Purpose Artificial Intelligence (GPAI) systems as an additional voluntary instrument to facilitate the application of the AI Act. The document establishes principles of transparency, copyright compliance, and safety in the development and use of such systems, and its endorsement is intended to provide greater legal certainty for stakeholders within the EU. As of the last week of July 2025, the companies that have confirmed their intention to join the Code include U.S.-based AI developers Anthropic and OpenAI. In their statements, both companies emphasized the importance of adhering to the principles of responsible technology use and described the Code as a practical step toward regulated and transparent engagement with European markets.

Accordingly, information has appeared on the OpenAI website regarding updates to the Terms of Use for OpenAI tools, which outline the company's priorities (responsible use, safety, and continuous improvement), specify prohibited purposes, and establish limitations on free use (OpenAI, 2025). The list of restricted uses largely corresponds to the unacceptable risk category under the AI Act, including prohibitions on using services for manipulation and deception, human rights violations, exploitation of vulnerable situations, and restricting access to education or essential services. This includes activities such as academic misconduct; deception, fraud, scams, spam, or impersonation; political campaigning, lobbying, electoral interference (domestic or foreign), or activities aimed at suppressing voter participation; and the automation of critical decisions in sensitive areas without meaningful human oversight (such as critical infrastructure, education, housing, employment, financial transactions and credit, insurance, legal services, healthcare, essential public services, product safety components, national security, migration, and law enforcement).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

By contrast, Meta has become the first – and so far the only – major technology company to announce its refusal to sign the Code, arguing that it creates new legal uncertainties for GPAI model developers, goes beyond the scope of regulation established by the AI Act, and may hinder innovation. Meta's website contains an updated Privacy Policy, with a new version entering into force on 16 December 2025. The policy includes a section titled "Other Rules and Articles" and a subsection "How Meta Uses Information for Generative AI Models and Features," which outlines the company's commitment to responsible development, user awareness of how generative AI works, and how user information is used to improve its services. The policy also identifies five core values guiding Meta's approach to AI: privacy and security; fairness and inclusiveness; reliability and protection; transparency and user control; and governance and accountability (Meta, 2025). Overall, the key requirements of the AI Act concerning the activities of AI developers and users appear to be largely reflected in Meta's internal policies; however, certain gaps remain, particularly the lack of explicit identification of areas in which the company would refrain from using AI, as required by the AI Act.

According to the White Paper, Ukraine's position on cooperation with major digital platforms is to conclude four partnership agreements with the identified platforms, which would make it possible to address up to 84% of potential violations of individuals' rights. The White Paper proposes an interesting mechanism for dispute resolution with these platforms during the adaptation period: it envisages the involvement of civil society organizations, so-called Trusted Flaggers – trusted observers with expertise in the field of AI – to act as intermediary filters between the platforms and individuals whose rights may have been violated by these companies. Complaints are expected to be submitted to Trusted Flaggers, who will review them for potential breaches of the platforms' terms of use and either forward them to the addressee or dismiss them as unfounded. The involvement of such an intermediary is expected to reduce the time required to process complaints (White Paper, p. 6).

Ukraine is actively implementing the roadmap and the two-stage action plan for the implementation of European legislation, including the AI Act, in the field of AI regulation, and this activity is already producing results. Ukraine is steadily improving its readiness indicators according to studies conducted by various organizations. According to the Oxford AI Readiness Index, Ukraine has climbed several positions in recent years and improved its overall score: while in 2022 it ranked 60th globally with a score of 52.8

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

(*Oxford Insights, 2022)*, in 2024 its score increased to 60.57 (*Oxford Insights, 2024)*.

Table 3.30. Ukraine in Government AI Readiness Index (Oxford Insights)

Year	Total Score	Government Pillar	Technology Sector Pillar	Data & Infrastructure Pillar
2022	52.80	68.96	34.68	54.74
2023	53.29	68.93	36.18	54.75
2024	60.57	73.42	41.93	66.37

Source: systematized for Ukraine by the author on data from Oxford Insights

A significant milestone in ensuring the protection of human rights in the context of the use of artificial intelligence technologies was Ukraine's accession in the summer of 2025 to the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. This international instrument sets out the fundamental benchmarks that the state must observe when shaping national policy and regulatory frameworks in the field of AI application, in particular in the public sector. These benchmarks include respect for human dignity, the provision of transparency, non-discrimination, protection of private life, as well as requirements for the reliability and safety of AI systems.

The importance of signing the Convention is significantly increased in light of the active development of e-government in Ukraine, primarily through the "Diia.Services" ecosystem, plans to integrate an AI assistant into the functioning of the platform, and the overall digitalization of public services. In this context, the early definition of standards for the safe and rights-oriented use of AI in public digital products is of fundamental importance. At the same time, the Convention has already been joined by the governments of several predominantly technologically advanced countries, including the United Kingdom, the United States of America, Canada, the European Union, Israel, Japan, and others.

Although the Convention is directly focused on state policy, its principles will also indirectly affect the private sector, as the state will initiate mechanisms and instruments designed to promote the implementation of these approaches in business activities. In particular, the Ministry of Digital Transformation plans to implement the HUDERIA methodology developed by the Council of Europe, which provides for the assessment of AI products in terms of their compliance with standards of human rights, democracy, and

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

the rule of law. At the same time, the Convention does not apply to the use of artificial intelligence technologies in the field of defense.

The draft Convention was developed over three years with the participation of representatives of the Council of Europe Member States, other countries involved in the negotiation process, as well as experts from the business community and civil society. Ukraine took an active part in drafting this document as a member of the Council of Europe Committee on Artificial Intelligence.

Conclusion. In conclusion, the study demonstrates that the legal regulation of artificial intelligence in the European Union is being shaped as a comprehensive and coherent system, within which the AI Act is closely linked to the provisions of Directive (EU) 2019/790 on copyright in the Digital Single Market. The AI Act directly places an obligation on providers of general-purpose AI models to have a clearly defined policy for compliance with copyright and related rights, considering the "reservation of rights" mechanisms provided for in that Directive. This means that the responsibility of AI providers is not limited to purely technical requirements, such as content labelling, but extends to the need to establish internal organisational and legal procedures for responding to claims by rights holders, including in relation to licensing, removal, or restriction of the use of protected works.

Thus, the synergy between the AI Act and Directive 2019/790 forms a new model for the protection of intellectual property, in which digital platforms and providers of AI systems act as active participants in ensuring a balance between innovative development and the protection of rights holders' interests. The AI Act does not directly reform copyright law, but it creates a new infrastructure for the protection of informational and intellectual rights of individuals. New requirements on transparency, labelling, and disclosure of information on training data do not resolve all conflicts in the field of intellectual property, but they establish a mandatory minimum standard of good faith conduct for participants in the AI market.

For Ukraine, the AI Act serves as a benchmark for future legal regulation of AI and as a foundation for harmonizing intellectual property legislation in the context of European integration. In view of the key aspects of the AI Act analysed above, it is possible to outline the main directions for preparing stakeholders involved in the use of AI for the introduction of the requirements of this Act. Rights holders should expect the emergence of public summaries of training data (Article 53), which will enable the identification of potential infringements and the preparation of response procedures, requests, and evidence regarding the origin of content. Platforms

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

providing AI systems need to implement technical machine-readable labelling and copyright compliance policies, as well as to find a balance between information disclosure and the protection of trade secrets. For judicial practice and the legislator (Ukraine), when implementing EU norms, it is necessary to provide procedural tools for access to more detailed evidence (where a summary indicates a risk of infringement), while also guaranteeing the protection of commercial secrets. In this regard, the level of practicality and universality of the harmonised standards to be developed and implemented by the AI Office is of particular importance, to ensure that the proposed labelling mechanisms do not remain declaratory but become a functional and unified instrument.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Bilyk, P. (2024). *AI Act: A new era of artificial intelligence regulation in Europe*. Liga Zakon: Analytics. https://surl.lt/xrykty
2. Brittain, B. (2024, May 20). *OpenAI loses fight to keep ChatGPT logs secret in copyright case*. Reuters. https://surl.li/kwewyy
3. Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. https://rm.coe.int/1680afae3c
4. European Parliament & Council of the European Union. (2016, April 27). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88. https://surl.lu/offgny
5. European Parliament & Council of the European Union. (2019, April 17). *Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*. Official Journal of the European Union, L 130, 92–125. https://surl.li/mdoooy
6. European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 on artificial intelligence (AI Act)*. Official Journal of the European Union, L 1689. https://surl.li/ylettv

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

7. Hasselbalch, G. (2029). *A human-centric approach to AI: The EU Ethics Guidelines for AI*. DataEthics. https://surl.li/frmohg
8. Krat, V. (2024). *Will artificial intelligence rule the "authorial" world: A judge's thoughts on the nature of AI regulation*. Supreme Court: Expert discussion "Sui generis right to protect AI 'creations'". https://surl.li/dcbbek
9. Maidannyk, L. (2024). *Towards the EU: Legislative changes in Ukraine regarding copyright*. *Yuridichna Gazeta*, 3(781). https://surl.li/avlhyw
10. Meta. (2025, October 25). *Privacy Policy*. https://www.facebook.com/privacy/genai
11. Ministry of Digital Transformation of Ukraine. (2024). *Glossary of terms in the field of artificial intelligence*. https://surl.li/pucezu
12. Ministry of Digital Transformation of Ukraine. (2024, January). *Guidelines for responsible use of artificial intelligence for media*. https://surl.li/ejekki
13. Ministry of Digital Transformation of Ukraine. (2024). *White paper on the regulation of artificial intelligence in Ukraine: Vision of the Ministry of Digital Transformation (Consultation version)*. https://surl.li/vgnrns
14. Ministry of Digital Transformation of Ukraine. (2025, July). *Guidelines for responsible use of artificial intelligence for legal professionals*. https://surli.cc/qrmood
15. Ministry of Digital Transformation of Ukraine & Office of the Ombudsman of Ukraine. (2024). *Human rights in the age of artificial intelligence: Challenges and legal regulation*. https://surli.cc/dhwont
16. Ministry of Economy of Ukraine, Intellectual Property and Innovation Office. (2024, November). *Guidelines on responsible use of artificial intelligence: Intellectual property issues*. https://surli.cc/tbvymf
17. OpenAI. (2025, October 25). *Terms of Use*. https://openai.com/uk-UA/policies/usage-policies/
18. Oxford Insights. (2022–2024). *Identifying risks in public contracts: Generative AI and the Company Analysis Tool*. https://surl.li/nfgyye
19. Ramalho, A. (2021). *Intellectual property protection for AI-generated creations*. Routledge. https://surl.li/lfskzy
20. Rubryka. (2024, September 24). *Solutions from Ukraine: Ukrainian IP Office grants copyright to AI-generated images for first time*. https://surl.li/czcath
21. Verkhovna Rada of Ukraine. (2022, December 1). *Law of Ukraine "On copyright and related rights" (No. 2811-IX)*. *https://surl.li/bnqgnt*
22. Whiddington, R. (2024, August 15). *Artists have won a small victory in a potentially landmark artificial intelligence copyright case*. Artnet. https://surli.cc/heagsn

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Section 3.4. Intellectual Property Protection in Online Litigation

Sergii Vasyliev[1]

[1]*Ph.D. (Law), Associate Professor, Legal Department of the Kharkiv City Council, Kharkiv, Ukraine, ORCID: https://orcid.org/0000-0003-3226-6981*

Citation:
Vasyliev, S. (2025). Intellectual Property Protection in Online Litigation. In V. Marchenko (Ed.), Intellectual property: protection in modern conditions. 208 p. (pp. 170-186). Scientific Center of Innovative Research. https://doi.org/10.36690/IPP-170-186

Abstract. *Online intellectual property disputes have become structurally complex because infringement propagates through intermediary-controlled infrastructures and across multiple jurisdictions. As a result, rights holders commonly combine platform notice mechanisms, civil litigation on the merits, interim measures, and administrative procedures to contain harm, identify responsible actors, and secure durable relief. The study frames online IP litigation as an operational enforcement system in which procedural timing and evidence discipline are decisive for effective protection. The objective is to systematize online IP protection as a coordinated enforcement strategy in the EU context. The study focuses on the interaction between intermediary-facing pathways, cross-border jurisdiction and applicable law, and evidence-driven remedy design. It also develops practical decision logic for selecting fora and sequencing actions under conditions of rapid digital diffusion. The study applies doctrinal and analytical synthesis of EU enforcement rules and private international law and translates these legal standards into an operational model. It proposes a portfolio approach to enforcement routes, a rights-sensitive approach to jurisdiction planning, and a layered evidence architecture that progresses from proof of right and scope, to proof of infringing acts and accessibility, and finally to proof of linkage and scale. It further integrates integrity and chain-of-custody discipline to strengthen admissibility and reduce authenticity challenges. The analysis shows that effective online protection depends on orchestration: platform action supports rapid containment, while court procedures enable enforceable injunctions, disclosure measures, and compensation. It demonstrates that cross-border disputes require careful forum selection and remedy scoping due to territorial constraints. It also shows that evidence readiness is decisive because online traces are volatile, and that remedy effectiveness increases when requests are narrowly targeted, technically executable, and proportionate. Online IP protection is most effective when designed as a sequenced strategy that integrates containment, preservation, attribution, and calibrated remedies. Future work should empirically test how notice quality, platform response latency, and evidence integrity practices influence dispute duration, containment success, and final relief outcomes.*

Keywords: *online IP litigation; EU enforcement; intermediary governance; Digital Services Act; jurisdiction strategy; applicable law; evidence readiness; chain of custody; digital proof integrity; interim measures; disclosure orders; remedy calibration.*

ISBN 978-9916-9389-5-9 (pdf)

1. Online IP litigation as a multi-forum enforcement system. Online IP disputes are structurally multi-forum because illegal uses of protected content typically propagate through intermediary-controlled infrastructures rather than through a single, easily identifiable distribution channel. As a result, rights holders rarely rely on one procedural track. They combine platform-facing procedures, civil litigation, and administrative mechanisms that target different "enforcement nodes," such as hosting, indexing, advertising, payment facilitation, and domain name resolution. This architecture reflects the basic enforcement logic in EU law that civil measures and remedies should be effective, proportionate, and capable of stopping infringement under practical market conditions, including fast-moving online dissemination (European Parliament and Council, 2004).

A central shift in the contemporary EU environment is that "online enforcement" increasingly depends on procedural design inside intermediaries. The Digital Services Act formalizes this interface by requiring providers of hosting services to implement notice and action mechanisms (Article 16) and to process notices in a timely, diligent, non-arbitrary, and objective manner. It also strengthens procedural accountability by linking content restriction decisions to reason-giving duties (Article 17) and by supporting structured redress systems, which is relevant when IP complaints intersect with freedom of expression concerns (European Parliament and Council, 2022). At the same time, the DSA preserves an important boundary condition for litigation strategy by maintaining the principle that no general obligation to monitor or actively seek illegal activity should be imposed on intermediary service providers, which limits the feasibility of broad "filtering" demands and pushes enforcement toward targeted, item-specific intervention (European Parliament and Council, 2022).

The legacy intermediary liability logic remains relevant for interpreting how litigation and platform enforcement interact, particularly where hosting services are involved. The E-Commerce Directive has historically structured the legal discussion around hosting and intermediary roles in the internal market, and it continues to be referenced in disputes about what can reasonably be expected from an intermediary once notified (European Parliament and Council, 2000). In practical terms, this legal environment channels online IP enforcement into a sequence where the first objective is containment, the second is attribution and evidence consolidation, and the third is merits litigation for durable relief. The same dispute may therefore generate multiple proceedings that are complementary rather than redundant,

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

especially when the primary infringer is hard to identify or is located outside the claimant's jurisdictional reach.

To make the multi-forum logic operational, it is useful to treat each forum as producing a specific enforcement output, and to select fora based on the "friction point" at which infringement can be most efficiently disrupted.

Table 3.31. Online IP enforcement fora as complementary tracks in a single dispute portfolio

Track	Typical addressee	Primary output	Strategic function in online IP disputes	Core limitation
Platform notice and action	Hosting services and platforms	Disabling access or removal of specific items	Rapid containment and disruption of viral spread	Does not establish liability or damages
Court litigation on the merits	Primary infringer	Final determination, injunctions, damages	Durable accountability and compensation	Slow relative to online diffusion
Interim measures proceedings	Infringer, sometimes intermediaries	Provisional injunctions	Immediate stop of ongoing harm	High proof pressure early
Authority orders and regulated cooperation	Intermediaries	Orders to act or provide information	Attribution and scaling enforcement	Procedural thresholds and proportionality
Domain name administrative procedure (UDRP)	Domain registrant	Transfer or cancellation of a domain	Fast response to cybersquatting-type disputes	Narrow scope and non-monetary remedies

Sources: (European Parliament and Council, 2004; European Parliament and Council, 2022; Internet Corporation for Assigned Names and Numbers, 2020).

Table 3.31 shows that online IP protection is typically achieved through orchestration. A platform process may remove content quickly, while court proceedings address persistent actors and enable remedies that platforms cannot provide.

Because the DSA imposes structured procedural obligations, an effective litigation strategy should also incorporate "compliance-aware" notice design. Notices should be sufficiently precise and substantiated to trigger timely action, and the claimant should anticipate that the platform's decision-making will generate reasoned outcomes and potential downstream complaints.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.32. DSA procedural anchors that shape IP enforcement through intermediaries

DSA procedural anchor	Practical meaning for IP claimants	Enforcement value	Litigation implication
Notice and action mechanisms (Article 16)	Standardized channel for submitting illegal content notices	Improves predictability and processing discipline	Encourages structured notice drafting and evidence attachment
Timely, diligent, non-arbitrary processing	Platforms must process notices under defined quality expectations	Supports faster containment	Makes weak or vague notices strategically costly
Statement of reasons (Article 17)	Decisions must be accompanied by reason-giving	Enhances accountability and traceability	Creates records that can support later court arguments
No general monitoring obligation	Limits broad filtering demands	Protects intermediary neutrality and rights balance	Pushes enforcement toward targeted items and repeat-actor logic

Sources: (European Parliament and Council, 2022).

Table 3.32 indicates that online litigation planning increasingly depends on procedural literacy. A claimant's effectiveness improves when the enforcement process is designed around the intermediary's legally structured obligations rather than around informal escalation alone.

Online IP litigation functions as a multi-forum enforcement system in which containment, attribution, and durable relief are distributed across platforms, courts, and specialized administrative procedures, and in which the DSA's procedural architecture materially shapes how rights holders should design notices, preserve records, and sequence escalation.

2. Cross-Border Jurisdiction and Applicable Law in Online IP Litigation. Online IP disputes are structurally cross-border because the same infringing act can be initiated in one state, hosted in a second state, and monetized through users or customers located across many additional jurisdictions. In EU private international law, the starting point is the general jurisdiction rule that a defendant should normally be sued in the courts of the Member State where it is domiciled (European Parliament & Council, 2012).

However, online infringements frequently trigger special jurisdiction for tort, allowing proceedings in the place "where the harmful event occurred or may occur" (European Parliament & Council, 2012). This dual entry point produces a practical strategic choice: either litigate where the operator is established, or litigate where the online harm materializes. The difficulty is that "harm" in online environments is diffuse, so EU case law has developed a set of differentiations that depend on the type of IP right and the territorial logic of its protection.

For copyright infringements, the Court of Justice has accepted that jurisdiction can be founded on the accessibility of infringing content in a

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Member State, provided that the relevant right is protected there, while limiting that court's competence to damage occurring within that territory.

A key clarification is that, for this copyright scenario, the special tort forum does not require proof that the website activity was "directed to" the forum state, because Article 5(3) Brussels I was interpreted as not containing a targeting requirement of that type. The consequence is a predictable "mosaic" model: multiple Member States' courts can hear claims for local damage, while full relief typically points back toward a forum capable of addressing the infringement's overall center of gravity. This matters for digital distribution of creative assets such as game art, music, cinematics, or narrative text, where the same unauthorized upload is instantly viewable across the internal market.

For EU trade marks, the jurisdictional logic is more explicitly operational and tied to EU trade mark courts and to the location of the infringing act. Regulation (EU) 2017/1001 permits infringement proceedings to be brought where the act of infringement has been committed or threatened, while also stating that when jurisdiction is based on that local act, the court's competence is limited to acts committed or threatened in that Member State. This structure parallels the mosaic effect but is written directly into the EU trade mark regime, and it becomes particularly relevant for online storefronts and marketplaces that target EU consumers with counterfeit or look-alike marks. In addition, CJEU case law has linked the "place where the harmful event occurred" analysis for internet advertising to the territorial scope of the protected right, supporting the idea that the forum most closely connected to the protected right's territorial validity is often best positioned to assess infringement and harm.

Table 3.33. Online IP infringement: practical jurisdiction triggers in the EU (rights-sensitive approach)

IP right and digital scenario	Typical EU jurisdiction entry points	Practical implication for online litigation
Copyright infringement via content accessible online	Courts where infringing content is accessible, limited to local damage; defendant domicile remains available	Enables multi-state local-damage claims; encourages careful remedy scoping
National trade mark infringement via online ads or listings	Courts connected to the territory where the mark is protected and where harm occurs; defendant establishment may connect to "event giving rise"	Strong territorial framing; forum choice often tracks registration and market impact
EU trade mark infringement via online targeting	EU trade mark courts where infringement is committed or threatened; competence may be territorially limited when based on local act	Procedural predictability for cross-border e-commerce enforcement

Sources: (European Parliament & Council, 2012; Court of Justice of the European Union, 2013; European Parliament & Council, 2017).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

The mapping shows that EU jurisdiction analysis is not purely technical but rights-sensitive: the stronger the territorial anchor of the right, the stronger the territorial framing of jurisdiction and remedies.

Choice of law further reinforces territoriality in IP disputes. Under Rome II, the law applicable to a non-contractual obligation arising from an infringement of an IP right is the law of the country "for which protection is claimed," which operationalizes lex loci protectionis as the default conflict rule. For unitary EU IP rights, Rome II adds a specific rule that, for questions not governed by the EU instrument itself, the applicable law is the law of the country where the act of infringement was committed. In litigation planning, this means that forum selection and applicable law selection cannot be treated as interchangeable: a claimant may obtain jurisdiction in one forum for local damage while still needing to argue substantive infringement elements under the law(s) tied to the protected territory or to the locus of the infringing act. For digital products, including games, this becomes decisive when the infringement spans multiple distribution channels such as app stores, mod repositories, streaming overlays, and unauthorized "skin" marketplaces, because each channel leaves different technical traces and creates different territorial market effects.

Evidence, Interim Measures, and "Platform-First" Legal Pathways. Online IP litigation is evidence-intensive because infringement is often transient: listings disappear, domains change registrants, and content is re-uploaded under new accounts. EU enforcement standards therefore emphasize evidence preservation and provisional measures as a functional bridge between detection and final adjudication. Directive 2004/48/EC requires Member States to provide measures to preserve relevant evidence and to ensure that enforcement procedures are fair, not unnecessarily complex, and not subject to unwarranted delays.

In practice, this translates into a litigation posture where the claimant's credibility is strengthened by disciplined evidence packages, including time-stamped captures of infringing pages, chain-of-custody logs for downloaded files, authenticated records of ownership and priority, and demonstrable linkage between the infringing account and commercial benefit. These artifacts are not merely supportive; in many cases they are determinative, because online disputes frequently turn on speed, traceability, and the capacity to attribute acts to identifiable operators.

At the same time, EU platform governance increasingly shapes the pre-litigation layer of online IP enforcement. The Digital Services Act requires hosting services to provide notice and action mechanisms and to process notices in a timely and non-arbitrary manner. It also requires a statement of

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

reasons for certain moderation restrictions, which can become practically valuable for a rights holder as a contemporaneous record of platform decision-making and of the grounds invoked. This "platform-first" pathway does not replace court litigation, but it frequently determines whether infringement is contained early enough to prevent reputational harm, consumer deception, or irreversible dilution of an IP-based brand signal.

Table 3.34. Evidence and remedy logic for online IP disputes: from detection to enforceable outcomes

Stage	Core objective	Evidence artifacts that increase enforceability	Typical remedies or outputs
Detection and triage	Confirm infringement and prioritize	Verified ownership record; time-stamped captures; technical identifiers; distribution mapping	Internal legal assessment; preservation plan
Rapid containment	Stop ongoing harm quickly	Notice dossier aligned with platform requirements; repeat-infringer history; targeted URL/item identifiers	Takedown or disabling access; account actions; marketplace delisting
Court-ready escalation	Convert incident into a justiciable claim	Chain of custody; attribution narrative; damages model; jurisdiction and applicable-law memo	Injunctions; evidence preservation orders; damages claims
Trust recovery and deterrence	Restore market confidence and deter recurrence	Compliance documentation; monitoring logs; remediation timeline	Public corrective statements; enhanced monitoring; licensing reforms

Sources: (European Parliament & Council, 2004; European Parliament & Council, 2022).

The table 3.34 indicates that online IP enforcement is operationally sequenced: the legal theory is necessary, but the winning condition is often the ability to produce fast, auditable proof and to align each remedy with the correct procedural channel.

Administrative and Hybrid Routes: Domain Names and Cross-Border Friction Reduction. Certain online IP disputes are resolved through specialized administrative procedures rather than full civil litigation, most prominently in domain name conflicts. The ICANN Uniform Domain Name Dispute Resolution Policy provides a standardized administrative route for trademark-based domain disputes, enabling transfer or cancellation without requiring full recourse to national courts in many cases.

The WIPO Arbitration and Mediation Center operationalizes this process at scale and publishes guidance that systematizes key interpretive issues, which supports procedural predictability for cross-border complainants.

For brand owners in sectors with high impersonation pressure, including game publishers and platforms, this route is strategically important

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

because cybersquatting can function as a gateway for fraud, malware distribution, counterfeit key sales, or deceptive "support" pages that erode consumer trust. A realistic enforcement design therefore treats UDRP as a fast harm-containment tool that complements, rather than substitutes for, court-based relief such as damages, injunctions, or disclosure orders.

Online IP litigation is best understood as a coordinated system of jurisdiction selection, territorially anchored applicable-law reasoning, and evidence-driven remedy sequencing. EU rules permit plaintiffs to pursue local harm where online accessibility or local infringing acts create a legally relevant connection, but the resulting competence is often territorially limited, which makes remedy design and damages modeling central to procedural efficiency. Rome II consolidates this territorial discipline through lex loci protectionis, ensuring that IP disputes remain tied to the state for which protection is claimed, while providing a workable rule for unitary EU rights when gaps exist in the sectoral instrument. Effective practice therefore depends on an operational evidence posture that can survive cross-border scrutiny, interact productively with platform notice systems, and escalate to court measures under IP enforcement standards when rapid containment fails.

3. Evidence, preservation, and digital proof discipline. Online IP litigation is evidence-centric because the factual object of the dispute is often volatile. Infringing listings, posts, and repositories can be deleted, geo-blocked, edited, or re-uploaded under new identifiers within hours, which means that the "event" must be converted into stable proof while it is still observable. This is why EU civil enforcement design treats evidence as a core enforcement bottleneck. Directive 2004/48/EC establishes a structured approach to evidence that includes court powers to order the production of evidence (Article 6) and to order prompt and effective provisional measures to preserve relevant evidence even before proceedings on the merits begin (Article 7).

In practice, these provisions create a procedural bridge between detection and adjudication, allowing claimants to move from "screenshots and suspicion" to court-recognizable evidentiary packages that can support interim relief and a merits claim.

A modern proof posture must also reflect the intermediary-centered structure of online markets. Platforms and other intermediary services frequently control the most valuable attribution data, including account identifiers, transaction traces, and certain visibility signals. The Digital Services Act formalizes the notice and action interface (Article 16) and requires structured decision outputs such as statements of reasons for certain

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

restrictions (Article 17), which can become practically important as contemporaneous records that corroborate timelines and platform responses.

At the same time, the DSA preserves the prohibition on imposing general monitoring obligations (Article 8), which means that evidence strategy should be designed for targeted items, repeat patterns, and concrete identifiers, rather than for broad "monitor everything" demands that are legally and operationally misaligned.

To operationalize these legal frameworks, evidence readiness should be structured as a layered model that separates (1) proof of right and scope, (2) proof of infringing acts and public availability, and (3) proof of linkage and scale. This layered logic matters because different procedural requests require different thresholds. Measures for preserving evidence are not identical to requests for information, and requests for information are not identical to merits proof. Directive 2004/48/EC explicitly includes a "right of information" (Article 8) that, in online contexts, is often pivotal for moving from content-level proof to actor-level attribution.

However, attribution is not frictionless. CJEU case law on Article 8 illustrates that the scope of "addresses" in the right of information can be contested and may not automatically include all digital identifiers a claimant would prefer, which reinforces the need to combine legal requests with strong technical linkage evidence.

The table 3.35 consolidates the layered evidence model into a litigation-ready structure.

Table 3.35. Layered evidence model for online IP disputes and its procedural function

Evidence layer	What must be shown	Typical artifacts	Procedural value
Right and scope	Standing, ownership, protected subject matter	Registrations or authorship proof; chain of title; deposit copies; product release records	Establishes that the claimant can sue and defines what is protected
Infringing acts and availability	What happened and where it was accessible	URLs; time-stamped captures; archived pages; downloaded files; marketplace listing histories	Supports urgency and plausibility of infringement
Linkage and scale	Who did it and how broadly it operated	Account IDs; domain registrant records; payment or delivery signals; repeat postings; networked account patterns	Enables attribution, remedy targeting, and damages framing

Sources: (European Parliament and Council, 2004; European Parliament and Council, 2022; Court of Justice of the European Union, 2020).

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Table 3.35 indicates that online disputes become materially stronger when claimants treat proof as an architecture that progresses from protected object to observable act to attributable actor.

Digital proof discipline also requires integrity and admissibility design. Courts do not evaluate screenshots and downloads only as "information," but as items that can be challenged for manipulation, incompleteness, or uncertain provenance. For this reason, chain-of-custody documentation and integrity mechanisms should be treated as first-order litigation assets. ISO/IEC 27037 provides guidance for identification, collection, acquisition, and preservation of digital evidence, emphasizing integrity-oriented handling that reduces later challenges to authenticity.

In the EU context, eIDAS supports the broader admissibility logic by establishing non-discrimination principles for electronic signatures and electronic documents, which strengthens the general legal footing for evidence that is natively digital, provided it is handled with credible integrity safeguards.

The table 3.36 translates digital evidence integrity into a practical chain-of-custody template that aligns with recognized evidence handling logic.

Table 3.36. Chain-of-custody and integrity controls for online infringement evidence

Control element	Practical action	Integrity benefit	Typical challenge it mitigates
Evidence identification	Record the exact item, source, and context	Clarifies what was captured and why it matters	Claims of ambiguity or misidentification
Controlled collection	Use repeatable capture methods and document tools used	Reduces variability and missing metadata	Allegations of selective capture
Acquisition and preservation	Store originals in restricted, immutable storage where feasible	Limits alteration risk	Claims of post-capture editing
Hashing and timestamping	Generate hashes for files and log timestamps	Supports integrity verification	Manipulation allegations
Access logging	Track who accessed the evidence and when	Preserves provenance discipline	Disputes about custody and contamination
Presentation package	Produce a court-ready bundle with explanations and indexes	Improves clarity and proportionality	Procedural confusion and credibility loss

Sources: (International Organization for Standardization, 2012; European Parliament and Council, 2014).

Table 3.36 shows that the strongest online enforcement posture is not only "having evidence," but being able to prove that evidence remained stable, attributable, and procedurally reliable.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Finally, evidence strategy in online litigation must align with remedy strategy. Interim relief depends on fast, credible proof, while damages and final injunctions depend on scale, recurrence, and causality narratives that can survive adversarial scrutiny. The DSA's structured notice processing and reason-giving duties can help claimants build a defensible timeline of actions and responses, but it does not replace court-based preservation and information measures under Directive 2004/48/EC.

The operational implication is that enforcement should be sequenced so that platform actions contain diffusion, court preservation stabilizes proof, and information measures support attribution, after which a merits case can be calibrated for durable relief.

Evidence readiness in online IP litigation is a standing capability that integrates EU evidence and preservation measures with integrity-oriented digital proof handling and targeted intermediary interaction. A claimant's effectiveness increases when proof is structured in layers, preserved through disciplined custody and integrity controls, and sequenced to support both urgent containment and enforceable merits outcomes.

4. Remedies, intermediary measures, and limits on monitoring. Online IP litigation remedies combine classical civil enforcement tools with intermediary-facing measures that are designed to stop dissemination, stabilize evidence, and enable attribution in markets where direct defendants may be anonymous, foreign, or operationally elusive. The EU Enforcement Directive provides a harmonized minimum set of measures, procedures, and remedies for civil enforcement, including injunctive relief, corrective measures, damages, and procedural mechanisms that support effective action against infringement.

In online environments, these remedies must be operationalized under conditions of rapid diffusion and high replication. This shifts remedy design toward speed, specificity, and reversibility, because the practical objective is frequently to prevent further harm rather than to litigate historical copying alone.

A distinctive feature of online enforcement is that effective relief often requires action by intermediaries that provide hosting, marketplace access, search visibility, payment routing, or domain name resolution. Intermediary involvement does not remove the need to establish liability against a primary infringer, but it changes the remedy architecture by adding a second axis: relief aimed at disruption and de-amplification. The E-Commerce Directive historically shaped this environment by structuring conditional liability limitations for intermediary services and, crucially, by prohibiting Member

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

States from imposing a general obligation to monitor or to actively seek facts indicating illegal activity.

The Digital Services Act updates and consolidates this governance environment, preserving the no-general-monitoring principle while strengthening procedural obligations and enforcement interfaces such as orders to act against illegal content, orders to provide information, and standardized notice-and-action processing for hosting services.

This combination produces a central constraint for remedy design. Courts and rights holders can pursue targeted measures aimed at specific illegal items, accounts, or clearly defined patterns, but broad, open-ended monitoring demands conflict with the EU's prohibition on general monitoring obligations.

Consequently, successful online IP litigation relies on remedy calibration: matching the requested relief to the correct enforcement node and framing it narrowly enough to satisfy proportionality while still being operationally effective.

Table 3.37. Remedy matrix for online IP litigation: objectives, addressees, and legal constraints

Remedy type	Typical addressee	Operational objective	Proof burden focus	Key constraint in EU online context
Interim injunction	Primary infringer and, in some contexts, intermediaries	Stop ongoing infringement quickly	Credible right and urgency, basic linkage	Proportionality and feasibility under time pressure
Final injunction	Primary infringer and, in some contexts, intermediaries	Prevent recurrence and secure durable relief	Established infringement and recurrence risk	Territorial scope and enforcement practicalities
Disabling access or takedown	Hosting services, platforms, marketplaces	Rapid containment and disruption of diffusion	Precise identifiers, item-level proof	Procedural safeguards and error risk management
Disclosure or information orders	Platforms, registrars, service providers	Attribution and mapping of distribution pathways	Necessity and proportionality, linkage indicators	Data protection boundaries and procedural thresholds
Corrective measures	Infringer and distribution points	Remove infringing goods or content from circulation	Traceability and relationship to protected subject matter	Practical tracing across mirrors and re-uploads
Damages and cost recovery	Primary infringer	Compensation and deterrence	Causality, quantification, scale evidence	Quantifying digital harm and proving commercial impact

Sources: (European Parliament and Council, 2004; European Parliament and Council, 2000; European Parliament and Council, 2022).

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Table 3.37 indicates that online remedies are most effective when they are framed as technically executable actions against specific actors or items, supported by proof that is sufficient for the procedural stage being pursued.

A second dimension is the monitoring boundary, which functions as a structural limit on what courts can demand from intermediaries. Article 15 of the E-Commerce Directive prohibits general monitoring obligations for conduit, caching, and hosting services.

The DSA preserves this logic and situates it within an updated framework that also recognizes orders to act against illegal content and orders to provide information as structured tools for enforcement.

In practical terms, the prohibition does not eliminate intermediary involvement. It shapes the form of involvement by privileging specific, notice-based, and order-based interventions over continuous surveillance requirements. It also reinforces the importance of precision in claimant submissions, because narrowly defined notices and requests are more compatible with the EU framework than broad demands that would require intermediaries to make generalized legal assessments at scale.

Table 3.38. Limits on monitoring and the compliant design of intermediary-facing relief

Design question	Non-compliant direction	Compliant direction	Why the difference matters
Scope of monitoring	Ongoing general monitoring of all user activity	Targeted action against identified illegal items or clearly defined patterns	EU law prohibits general monitoring obligations
Identification of content	Vague references to categories of illegality	Specific URLs, listings, hashes, identifiers, and timestamps	Enables diligent processing and reduces error rates
Responsibility allocation	Intermediary makes open-ended legality decisions	Court or authority orders define the action, claimant supplies substantiation	Reduces arbitrariness and supports procedural safeguards
Evidence and audit trail	No record of action and rationale	Structured notice and reasoned decision trail	Supports accountability and later litigation proof
Proportionality	Broad measures affecting lawful content	Narrow measures minimizing collateral impact	Aligns with proportionality expectations in enforcement remedies

Sources: (European Parliament and Council, 2000; European Parliament and Council, 2022; European Parliament and Council, 2004).

Table 3.38 shows that online IP litigation is not only about which remedy is theoretically available, but about whether the remedy is framed in a way that the EU intermediary framework permits and intermediaries can implement without transforming their role into generalized surveillance.

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

A third issue concerns the evidentiary function of intermediary interaction. The DSA strengthens procedural structure around notices and service-provider responses, which can generate a traceable chronology of alleged illegality, platform action, and stated reasons. This record can be strategically valuable in later proceedings because it helps demonstrate urgency, recurrence, and response latency. Yet it does not replace court-based tools under the Enforcement Directive, particularly where the claimant needs preservation measures, disclosure orders, or enforceable injunctions that bind a defendant beyond the platform's internal rules.

Remedies in online IP litigation are most effective when they are sequenced and calibrated across two axes: classic civil relief against primary infringers and targeted, order- or notice-based measures that engage intermediaries as enforcement nodes. The EU framework supports strong enforcement but constrains remedy form through proportionality and through the prohibition of general monitoring obligations, which makes precision, item-specific targeting, and evidence-driven requests central to successful outcomes.

Conclusion. Online IP litigation should be conceptualized as a coordinated enforcement strategy rather than a single judicial episode, because the digital environment converts infringement into a moving target that changes faster than traditional procedural timelines. The central challenge is that online violations spread rapidly across platforms and jurisdictions, while the evidentiary traces that prove them are unstable and can be altered, deleted, or reconstituted under new accounts with minimal friction. Under these conditions, the decisive determinant of success is not only the substantive strength of the legal claim, but also the quality of early sequencing: immediate containment to limit further diffusion, prompt preservation of proof before it disappears, systematic attribution to connect content to accountable actors, and precise remedy targeting that matches each intervention to the enforcement node where it can actually work.

A defensible enforcement posture begins with forum architecture that reflects the territorial logic of IP protection and the practical realities of online distribution. This requires anticipating whether a case will demand local relief to stop harm quickly, broader proceedings to reach the operator behind repeated infringement, or parallel tracks that address different parts of the same infringement ecosystem. In parallel, the claimant must build an evidence posture designed for adversarial scrutiny. This involves moving beyond casual screenshots toward structured proof packages that document what was observed, when it was observed, how it was captured, and how integrity was preserved, including clear chains of custody and internal

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

consistency across technical identifiers, timestamps, and contextual elements. Evidence design should also be proportional to the stage of escalation, since urgent measures demand fast plausibility and traceability, while final relief requires stronger demonstrations of recurrence, scale, and causality.

Remedies become realistically enforceable when they are aligned with the correct actor and the correct operational leverage point. Primary infringers may be responsible for the underlying unlawful act, yet intermediaries often control the pathways that give infringement reach, persistence, and monetization. Effective strategy therefore distinguishes between liability-focused actions that seek durable accountability and compensation, and disruption-focused actions that aim to disable access, reduce visibility, interrupt transactions, or remove deceptive identifiers. Remedy requests are strongest when they are narrow enough to be executable and verifiable, while still broad enough to address foreseeable re-uploads, mirror distribution, and repeat-actor behavior. This alignment reduces collateral impact, strengthens proportionality, and improves the likelihood that courts and intermediaries will treat the requested measures as both legitimate and feasible.

Ultimately, effective online IP protection is achieved when procedural discipline is integrated with operational readiness. Litigation must be supported by governance routines that enable rapid decision-making, consistent documentation, controlled disclosure, and coordinated action across legal, security, and business functions. When these elements are present, digital traces can be converted into admissible proof, containment can be executed without undermining confidentiality, and enforcement can shift from episodic takedowns toward credible deterrence and sustained protection of intangible value.

Funding. The author declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The author declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The author declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this section are solely those of the author and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this section, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

References:

1. Bryntsev, O. V. (2016). “Electronic Court” in Ukraine: Experience and prospects [Monograph]. Kharkiv: Pravo.
2. Court of Justice of the European Union. (2013). *Peter Pinckney v KDG Mediatech AG* (Case C-170/12). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0170
3. Court of Justice of the European Union. (2020). *Constantin Film Verleih GmbH v YouTube LLC and Google Inc.* (Case C-264/19). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0264
4. Dynis, G. G. (2011). International legal concepts of global law, Internet law or cyberlaw and transformation of international law. Journal of the Kyiv University of Law, 2, 283.
5. European Parliament and Council of the European Union. (2000). *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive).* https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng
6. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC on the enforcement of intellectual property rights.* https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng
7. European Parliament and Council of the European Union. (2007). *Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II).* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007R0864
8. European Parliament and Council of the European Union. (2012). *Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Recast).* https://eur-lex.europa.eu/eli/reg/2012/1215/oj/eng
9. European Parliament and Council of the European Union. (2014). *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910
10. European Parliament and Council of the European Union. (2017). *Regulation (EU) 2017/1001 on the European Union trade mark.* https://eur-lex.europa.eu/eli/reg/2017/1001/oj/eng
11. European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Services Act).* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
12. Internet Corporation for Assigned Names and Numbers. (2020). *Uniform Domain-Name Dispute-Resolution Policy (UDRP).* https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-01-01-2020-en
13. International Organization for Standardization. (2012). *ISO/IEC 27037:2012 Information technology: Security techniques: Guidelines for identification, collection, acquisition, and preservation of digital evidence.*https://www.iso.org/standard/44381.html

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

14. Sabreen, A. (2023). Online courts and private and public aspects of open justice: Enhancing access to court or violating the right to privacy? The Age of Human Rights Journal, 20. https://doi.org/10.17561/tahrj.v20.7516
15. Susskind, R. (2020). Online court and the future of justice. Oxford University Press. https://doi.org/10.1093/oso/9780198838364.001.0001
16. Vasyliev, S. (2025). The Genesis of Online Dispute Resolution in Ukraine. *Public Administration and Law Review*, (3(23), 65–79. https://doi.org/10.36690/2674-5216-2025-3-65-79
17. World Intellectual Property Organization. (2017). *WIPO Overview 3.0: WIPO Panel Views on Selected UDRP Questions.*https://www.wipo.int/amc/en/domains/search/overview3.0/
18. World Intellectual Property Organization. (2025). *WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).* https://www.wipo.int/amc/en/domains/guide/

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

Conclusion

Based on the research results presented by the authors in this monograph, the following conclusions can be drawn:

1. The research was conducted and demonstrated that the rapid digital transformation of public administration elevates information security to a strategic priority for modern states. In the Ukrainian context, where digital modernization is closely linked to European integration, the establishment of a resilient and coherent e document management system was substantiated as essential for transparency, democratic governance, and the protection of citizens' rights. At the same time, it was identified that the existing system continues to face structural challenges, including legal inconsistencies, fragmented institutional responsibilities, limited technical and financial capacity, weak interoperability and coordination, and safeguards that are not fully proportional to current risks. These vulnerabilities were shown to increase exposure to cybercrime, espionage, unauthorized access, and data manipulation, which undermines trust and constrains the development of digital public services.

2. The intellectual property protection in corporate information flows should be treated as a governance and control problem rather than as a set of isolated legal declarations. It was found that protection effectiveness depends primarily on daily information handling, especially the ability to preserve confidentiality across functions, platforms, and external partners through disciplined classification, access governance, and boundary management. It was also established that digital transformation expands exposure by increasing the number of flow points, accelerating dissemination, and complicating traceability after incidents, which makes lifecycle continuity and "safe pathways" for legitimate sharing essential. A portfolio approach was substantiated as more resilient than reliance on any single legal mechanism, because coherent combinations of confidentiality controls, contractual duties, and complementary IP tools improve enforceability. Finally, it was shown that evidence readiness functions as a continuous organizational capability, and that scalable protection is achieved when confidentiality is operationalized as measurable behavior embedded in accountability and repeatable controls.

3. The contemporary intellectual property landscape, globally and in Ukraine, is undergoing structural transformation driven by digitalization, data centric business models, and the rapid diffusion of artificial intelligence and distributed technologies. It was established that classical doctrinal

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

foundations increasingly interact with technological realities that challenge conventional assumptions about authorship, originality, territoriality, infringement detection, and long term preservation, while platformized cross border markets amplify legal conflicts and cybersecurity risks. For Ukraine, the analysis indicated that effective modernization requires a hybrid legal technological model of IP governance in which legal reform, institutional oversight, cybersecurity standards, and interoperable registries function together, because neither legal instruments nor technical tools are sufficient in isolation. It was also demonstrated that emerging technologies create new risks yet offer modernization opportunities, provided that auditability, safeguards, and dispute resolution frameworks are embedded into implementation, especially given wartime vulnerabilities of digital infrastructures. Future research was defined around empirical assessment of stakeholder behavior under new rules, comparative evaluation of leading innovation economies, technological study of distributed systems for archival preservation, and interdisciplinary work integrating IP law, information science, cybersecurity, and computational methods. Overall, it was concluded that Ukraine's transition to a resilient and innovation oriented IP regime depends on integrated harmonization, institutional strengthening, and technological modernization that balances rights protection with digital openness.

4. The strengthening IP protection in the EU games sector requires operational governance that links harmonised legal rules with practical controls and evidence ready enforcement. It was established that the Information Society framework supports the protection of technological measures, while the DSM architecture and Article 17 related guidance reshapes platform responsibilities around licensing and user uploaded content management. It was also shown that trademark protection and trade secret governance remain decisive because brand integrity and confidential know how underpin competitive advantage in game development and distribution. In addition, civil enforcement instruments and rapid online mechanisms, including UDRP procedures, were identified as important for limiting reputational harm in cases of piracy, impersonation, and deceptive domain practices. Overall, it was concluded that a resilient model treats IP as a measurable capability set integrating rights clarity, technical and contractual controls, market integrity measures, and enforcement readiness, while preserving legitimate user creativity and trust.

5. The blockchain technology has significant potential to strengthen the protection and management of intellectual property rights, while its legal integration remains incomplete and uneven across jurisdictions. It was

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

demonstrated that distributed ledger systems can support evidentiary certainty by enabling immutable time stamping and verifiable record keeping that assists in establishing authorship, priority, and chains of title, which is particularly valuable in copyright and patent disputes where proof is decisive. The analysis also found that smart contracts can automate licensing, lower transaction costs, and improve the transparency of royalty distribution, especially in digital content markets. Comparative review indicated that although blockchain records may be accepted as evidence in some jurisdictions, there is still no harmonized framework defining their legal effect, and regulatory initiatives that reference blockchain often remain fragmented and under specified, particularly regarding tokenized assets and decentralized ownership patterns. It was further established that the legal status of NFTs remains ambiguous, since courts and policymakers continue to struggle with fitting token based transactions into traditional categories of copyright and property. Practical evaluation confirmed that blockchain can enhance traceability and support anti counterfeiting efforts, yet it cannot independently verify originality or prevent piracy, and therefore functions primarily as a complementary evidentiary and transactional tool within a broader protection ecosystem. The study also demonstrated that core doctrinal principles, including territoriality, registration requirements, and the originality standard, are not replaced by blockchain records, but instead require interpretive alignment and explicit statutory anchoring for legal certainty. Finally, it was concluded that the most effective pathway is a hybrid legal technological model in which blockchain is integrated with statutory regimes, contractual safeguards, and judicial oversight, supported by coherent legislative guidance, harmonized technical standards, and stronger international coordination to address cross border enforcement complexity.

6. The international aspects of IP protection are inseparable from contemporary assessments of business reputation because IP simultaneously provides legal defensibility and signals governance maturity. It was established that global instruments, including TRIPS and WIPO administered treaties, set baseline expectations and enable cross border protection pathways that influence how stakeholders interpret a firm's diligence, integrity, and compliance culture. The analysis also showed that cross border branding amplifies reputational exposure through counterfeiting, cybersquatting, and inadvertent infringement, which makes continuous monitoring and rapid response capacity decisive for trust preservation. Methodologically, it was substantiated that IP can be embedded in reputation assessment through indicators reflecting portfolio

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

robustness, enforcement performance, governance quality, and value linkage, with standards such as ISO 10668 and ISO 56005 supporting transparency and comparability across contexts. It was further found that in disputes, evidence quality and procedural readiness shape whether reputational harm escalates or is reframed as a resilience narrative grounded in effective governance. Overall, it was concluded that firms that operationalize IP due diligence, build robust contract architectures, and maintain digital enforcement capabilities are better positioned to protect intangible assets and sustain stakeholder trust across jurisdictions.

7. Legal protection of polygraph assessment methodologies is most robust when it is implemented as a portfolio that mirrors the layered structure of the underlying asset and its use context. Copyright protection is well suited to the expression of the methodology in tangible form, including manuals, training materials, structured reports, and software code, yet it does not grant exclusivity over the functional procedure itself or over methods of operation. This doctrinal limitation makes confidentiality a decisive layer in practice, because the competitive value of the methodology often resides in calibrated decision rules, scoring logic, procedural sequencing, and expert know how that can be replicated if disclosure occurs (World Intellectual Property Organization, 1996; World Intellectual Property Organization, 2025). Accordingly, trade secret protection and systematic know how governance become central, since the TRIPS framework and the EU Trade Secrets Directive converge on a coherent legal test based on secrecy, commercial value, and reasonable protective steps, while also attaching liability to unlawful acquisition, use, or disclosure, including breaches of confidentiality and use limitation obligations (World Trade Organization, 1994; European Parliament and Council, 2016). Within this portfolio logic, contracting and enforcement readiness operationalize rights and determine their practical effectiveness, because the design of licensing scope, role based access controls, audit trails, and rapid evidence preservation strongly influences whether remedies can be pursued without expanding disclosure of the very information that must remain confidential (European Parliament and Council, 2004; European Parliament and Council, 2016).

8. The EU's legal regulation of artificial intelligence is being shaped as an integrated framework in which the AI Act is closely connected with Directive (EU) 2019/790 on copyright in the Digital Single Market. In this configuration, copyright compliance becomes a formal governance obligation for providers of general purpose AI models, who must adopt a clearly defined policy that takes into account the Directive's "reservation of rights" mechanism. This shifts responsibility beyond purely technical

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

transparency or labelling requirements and toward internal organizational and legal procedures for handling rights holder claims, including licensing options and, where justified, restricting or removing the use of protected works. The synergy between the AI Act and the DSM Directive does not rewrite copyright law directly, but it creates a compliance infrastructure that sets a minimum standard of good faith conduct in the AI market through transparency and documentation expectations. For Ukraine, this model serves as a practical benchmark for future AI regulation and for IP harmonization within the European integration trajectory. It implies that rights holders should prepare to use training data summaries for risk identification and evidence building, while AI providers should implement machine readable labelling and structured compliance processes that balance disclosure duties with protection of trade secrets. Finally, effective implementation depends on workable harmonized standards, so that these mechanisms operate as functional, unified tools rather than remaining declaratory.

9. Online IP litigation should be treated as a coordinated enforcement strategy because digital infringement spreads quickly across platforms and jurisdictions, while evidence can be erased or recreated with minimal effort. Effective outcomes depend not only on the legal merits of the claim, but also on early sequencing: rapid containment, immediate preservation of proof, reliable attribution, and precisely targeted remedies that match the actor and the operational leverage point. A robust approach combines forum selection with evidence packages suitable for adversarial scrutiny and uses both liability focused actions and disruption measures against intermediaries where appropriate. Overall, procedural discipline and operational readiness, including coordinated work across legal, security, and business functions, enable litigation to shift from episodic takedowns to sustained deterrence and protection of intangible value.

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

References

1. 100 mist – krok vpered. Monitorynh vprovadzhennia instrumentiv elektronnoho uriaduvannia, yak osnovy nadannia administratyvnykh posluh v elektronnomu vyhliadi [100 Cities – A Step Forward. Monitoring the Implementation of E-Governance Tools as the Basis for Providing Administrative Services in Electronic.
2. Akimov, O. O., Andrusiak, M. V. & Rusetskyi, R. Y. (2025). Tools for enhancing personnel security under martial law: an interdisciplinary approach to polygraph application. *Efficiency of Public Administration*, *1*(82/83), 86–93. https://doi.org/10.36930/508211
3. Akimov, O., & Andrusiak, M. (2025). Professional standardization of polygraph examiner's psychophysiological competencies in the context of ukraine's national security. *Society and Security*, (2(8), 72–79. https://doi.org/10.26642/sas-2025-2(8)-72-79
4. Bajwa, R., & Meem, F. T. (2024). Intellectual Property Blockchain Odyssey: Navigating Challenges and Seizing Opportunities. URL: https://arxiv.org/html/2410.08359v1
5. Berne Notification No. 169. [Berne Convention for the Protection of Literary and Artistic Works]. Accession by Ukraine. URL: https://surl.li/cwovek
6. Bilyk, P. (2024). *AI Act: A new era of artificial intelligence regulation in Europe*. Liga Zakon: Analytics. https://surl.lt/xrykty
7. Blockchain and Intellectual Property. (2019). URL: https://www.wipo.int/en/web/cws/blockchain-and-ip
8. Blockchain technologies and IP ecosystems: A WIPO white paper. (2022). URL: https://surl.li/kgsezu
9. Brittain, B. (2024, May 20). *OpenAI loses fight to keep ChatGPT logs secret in copyright case*. Reuters. https://surl.li/kwewyy
10. Bryntsev, O. V. (2016). "Electronic Court" in Ukraine: Experience and prospects [Monograph]. Kharkiv: Pravo.
11. Claeys, A. S., Cauberghe, V., & Vyncke, P. (2010). Restoring reputations in times of crisis: An experimental study of the situational crisis communication theory and the moderating effects of locus of control. *Public Relations Review, 36*(3), 256–262. https://doi.org/10.1016/j.pubrev.2010.05.004
12. Clark, B. (2018). Blockchain and IP Law: A Match made in Crypto Heaven? URL: https://surl.lt/ukevhm

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

13. Concept for the Development of E-Government in Ukraine. (2010). URL: http://zakon2.rada.gov.ua/laws/show/2250-2010-%D1%80/ed20110926
14. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.108. [E-resource]. – Access mode: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
15. Coombs, W. T. (2007). Protecting organizational reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*, 163–176. https://doi.org/10.1057/palgrave.crr.1550049
16. Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. https://rm.coe.int/1680afae3c
17. Court of Justice of the European Union. (2009, July 16). *Infopaq International A/S v Danske Dagblades Forening* (Case C-5/08) [Judgment]. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62008CJ0005
18. Court of Justice of the European Union. (2013). *Peter Pinckney v KDG Mediatech AG* (Case C-170/12). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0170
19. Court of Justice of the European Union. (2014). *Nintendo Co. Ltd and Others v PC Box Srl and 9Net Srl (Case C-355/12).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0355
20. Court of Justice of the European Union. (2020). *Constantin Film Verleih GmbH v YouTube LLC and Google Inc.* (Case C-264/19). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62019CJ0264
21. Danilchenko, O. (2017). Blokchejn: yurist iz mashiny [Blockchain: Lawyer in the Car]. [YURIST&ZAKON. 2017. № 21]. URL: http://uz.ligazakon.ua/magazine_article/EA010438
22. Data as an IP Asset. (2023). URL: https://surl.li/ogsheh
23. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. URL: https://surl.lu/bpozhj
24. 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'). URL: https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

25. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). URL: https://surl.li/vpnsdn
26. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal L 281. 23/11/1995. - P. 0031-0050.
27. Directive 98/34/EC Of the European Parliament and of the Council of 22 June 1998 on the laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services // Official Journal L 204. 21.7.1998. – P.37
28. Djamane, D. (2025). Smart Contracts: Global Perspectives and Legal Realities – Part 2 - Daily Jus URL: https://surl.lt/nmgknb
29. Dorigo, L. (2022). Smart Contracts work – but do they hold up in court? | Pestalozzi Attorneys at Law. URL: https://surl.li/mndszc
30. Dubov, D. Dubova S. (2006). Osnovy elektronnoho uriaduvannia. Navchalnyi posibnyk [Fundamentals of electronic governance. Textbook]. [Kyiv: Tsentr navchalnoi literatury]. –176p.
31. Dynis, G. G. (2011). International legal concepts of global law, Internet law or cyberlaw and transformation of international law. Journal of the Kyiv University of Law, 2, 283.
32. ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection. (2023) URL: https://surl.li/nivgkp
33. Epic Games. (2025). *Fan Content Policy*. Retrieved December 14, 2025, from: https://www.epicgames.com/site/en-US/fan-art-policy
34. EUIPO connects to TMview and DesignView through blockchain. URL: https://surl.li/hvhixr
35. EUR-Lex. (2018, June 11). *Enforcement of intellectual property rights* (summary). https://eur-lex.europa.eu/EN/legal-content/summary/enforcement-of-intellectual-property-rights.html
36. European Commission. (2021). *Guidance on Article 17 of Directive (EU) 2019/790 on copyright in the Digital Single Market* (COM/2021/288 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0288
37. European Parliament & Council of the European Union. (2016, April 27). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free*

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://surl.lu/offgny

38. European Parliament & Council of the European Union. (2019, April 17). *Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC*. Official Journal of the European Union, L 130, 92–125. https://surl.li/mdoooy
39. European Parliament & Council of the European Union. (2024, June 13). *Regulation (EU) 2024/1689 on artificial intelligence (AI Act)*. Official Journal of the European Union, L 1689. https://surl.li/ylettv
40. European Parliament & Council. (1996). *Directive 96/9/EC of 11 March 1996 on the legal protection of databases*. https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng
41. European Parliament & Council. (1998). *Directive 98/71/EC of 13 October 1998 on the legal protection of designs*. https://eur-lex.europa.eu/eli/dir/1998/71/oj/eng
42. European Parliament & Council. (2001). *Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
43. European Parliament & Council. (2004). *Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights*. https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng
44. European Parliament & Council. (2009). *Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs*. https://eur-lex.europa.eu/eli/dir/2009/24/oj/eng
45. European Parliament & Council. (2012). *Regulation (EU) No 386/2012 of 19 April 2012 on entrusting the Office for Harmonization in the Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R0386
46. European Parliament & Council. (2015). *Directive (EU) 2015/2436 of 16 December 2015 to approximate the laws of the Member States relating to trade marks (recast)*. https://eur-lex.europa.eu/eli/dir/2015/2436/oj/eng
47. European Parliament & Council. (2016). *Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

48. European Parliament & Council. (2017). *Regulation (EU) 2017/1001 of 14 June 2017 on the European Union trade mark (codification).* https://eur-lex.europa.eu/eli/reg/2017/1001/oj/eng
49. European Parliament & Council. (2019). *Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0770
50. European Parliament & Council. (2019). *Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market*. https://eur-lex.europa.eu/eli/dir/2019/790/oj/eng
51. European Parliament & Council. (2022). *Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065
52. European Parliament & Council. (2024). *Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
53. European Parliament and Council of the European Union. (1996, March 11). *Directive 96/9/EC on the legal protection of databases*. *Official Journal of the European Communities*, L 77, 20–28. EUR-Lex. https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng
54. European Parliament and Council of the European Union. (2000). *Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive).* https://eur-lex.europa.eu/eli/dir/2000/31/oj/eng
55. European Parliament and Council of the European Union. (2001, May 22). *Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society*. *Official Journal of the European Communities*, L 167, 10–19. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2001/29/oj/eng
56. European Parliament and Council of the European Union. (2004, April 29). *Directive 2004/48/EC on the enforcement of intellectual property rights*. *Official Journal of the European Union*, L 157, 45–86. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0048
57. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC on the enforcement of intellectual property rights.* https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

58. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC of 29 April 2004 on the enforcement of intellectual property rights*. https://eur-lex.europa.eu/eli/dir/2004/48/oj/eng
59. European Parliament and Council of the European Union. (2004). *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (Text with EEA relevance)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048
60. European Parliament and Council of the European Union. (2007). *Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II)*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007R0864
61. European Parliament and Council of the European Union. (2009, April 23). *Directive 2009/24/EC on the legal protection of computer programs (codified version)*. *Official Journal of the European Union*, L 111, 16–22. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2009/24/oj/eng
62. European Parliament and Council of the European Union. (2012). *Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Recast)*. https://eur-lex.europa.eu/eli/reg/2012/1215/oj/eng
63. European Parliament and Council of the European Union. (2014). *Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910
64. European Parliament and Council of the European Union. (2016, June 8). *Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. *Official Journal of the European Union*, L 157, 1–18. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng
65. European Parliament and Council of the European Union. (2016). *Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*. https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

66. European Parliament and Council of the European Union. (2017). *Regulation (EU) 2017/1001 on the European Union trade mark.* https://eur-lex.europa.eu/eli/reg/2017/1001/oj/eng
67. European Parliament and Council of the European Union. (2022). *Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Services Act).* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
68. European Union Intellectual Property Office. (2019). *The risks posed by counterfeits to consumers: A qualitative study*. https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers/2019_Risks_Posed_by_Counterfeits_to_Consumers_FullR_en.pdf
69. European Union Intellectual Property Office. (2019). *The risks posed by counterfeits to consumers: A qualitative study.*https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2019_Risks_Posed_by_Counterfeits_to_Consumers/2019_Risks_Posed_by_Counterfeits_to_Consumers_FullR_en.pdf
70. European Union. (2002). *Council Regulation (EC) No 6/2002 of 12 December 2001 on Community designs.* https://eur-lex.europa.eu/eli/reg/2002/6/oj/eng
71. European Union. (2016). *Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation)*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
72. For the first time in ukraine, copyright is registered for works that include AI-generated images. (2024). URL: https://surl.li/cvslic
73. Fortune Media. (2025, January 29). *World's most admired companies*. https://fortune.com/ranking/worlds-most-admired-companies/ Fortune
74. Harasym, O. R., Komova, M. V., & Lytvyn, V. V. (2010). Orhanizatsiia zakhyshchenoho elektronnoho dokumentoobihu v merezhakh elektronnoho uriaduvannia [Organization of Secure Electronic Document Workflow in E-Governance Networks]. URL: https://lnk.ua/q462yyO4J
75. Hasselbalch, G. (2029). *A human-centric approach to AI: The EU Ethics Guidelines for AI*. DataEthics. https://surl.li/frmohg
76. Hayashi Y., Johoka Shakai (1969). Hado no Shakai Kara Sofuto no Shakai e [The Information Society: From Hard to Soft Society]. Tokyo: Kodansha Gendai Shinso, 1969. 209 p.
77. Hohn-Hein, N. (2022). EU IP Office launches first blockchain-based

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

IP register, Anti-Counterfeiting Blockathon Forum. URL: https://surli.cc/leegiq
78. ICANN. (2020). *Uniform Domain Name Dispute Resolution Policy (UDRP)*. https://www.icann.org/resources/pages/policy-2012-02-25-en
79. Intellectual Property (Stanford Encyclopedia of Philosophy). URL: https://plato.stanford.edu/entries/intellectual-property/
80. Intellectual Property Rights and Distributed Ledger Technology with a focus on art NFTs and tokenized art. (2022). URL: https://surl.li/yttfdp
81. International Organization for Standardization, & International Electrotechnical Commission. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection: Information security management systems: Requirements.* ISO. https://www.iso.org/standard/27001
82. International Organization for Standardization, & International Electrotechnical Commission. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection: Information security controls.* ISO. https://www.iso.org/standard/75652.html
83. International Organization for Standardization. (2010). *Brand valuation: Requirements for monetary brand valuation (ISO 10668:2010)*. https://www.iso.org/standard/46032.html
84. International Organization for Standardization. (2012). *ISO/IEC 27037:2012 Information technology: Security techniques: Guidelines for identification, collection, acquisition, and preservation of digital evidence.*https://www.iso.org/standard/44381.html
85. International Organization for Standardization. (2020). *Innovation management: Tools and methods for intellectual property management: Guidance (ISO 56005:2020)*. https://www.iso.org/standard/72761.html
86. Internet Corporation for Assigned Names and Numbers. (2020). *Uniform Domain-Name Dispute-Resolution Policy (UDRP).* https://www.icann.org/en/contracted-parties/consensus-policies/uniform-domain-name-dispute-resolution-policy/uniform-domain-name-dispute-resolution-policy-01-01-2020-en
87. Internet Corporation for Assigned Names and Numbers. (2020). *Uniform Domain-Name Dispute-Resolution Policy*. https://www.icann.org/resources/pages/uniform-domain-name-dispute-resolution-policy-01-01-2020-en

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

88. Kim, P. H., Dirks, K. T., & Cooper, C. D. (2009). The repair of trust: A dynamic bilateral perspective and multilevel conceptualization. *Academy of Management Review, 34*(3), 401–422. https://doi.org/10.5465/amr.2009.40631887
89. Korzhevskyi, I. (2025). A Conceptual Approach to Enhancing Enterprise Economic Security Under the Influence of Business. *Economy and Society*, (73). https://doi.org/10.32782/2524-0072/2025-73-121
90. Korzhevskyi, I. (2025). Methodological Approaches to Assessing Corporate Reputation and Economic Security of Enterprises. *Economics, Finance and Management Review*, (3(23), 106–118. https://doi.org/10.36690/2674-5208-2025-3-106-118
91. Krat, V. (2024). *Will artificial intelligence rule the "authorial" world: A judge's thoughts on the nature of AI regulation*. Supreme Court: Expert discussion "Sui generis right to protect AI 'creations'". https://surl.li/dcbbek
92. Kyrylenko, A. (2024). Ukrainian IP Office registers works incorporating AI-generated content protected under new sui generis right - The IPKat. URL: https://surl.li/gzujju
93. Law of Ukraine "Pro elektronni dokumenty ta elektronnyi dokumentoobih" [On Electronic Documents and Electronic Document Management] (2003). (No. 851-IV). URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
94. Lee, E. (2023) NFTs as Decentralized Intellectual Property. URL: https://illinoislawreview.org/wp-content/uploads/2023/08/Lee.pdf
95. Len, G. D., & Mann, E. C. Benefits and Considerations of Protecting Your IP With Blockchain Technology. (2025). URL: https://surl.lu/zzqvsv
96. Levi, S. D., & Ghaemmaghami, M. (2025). Copyright Office Weighs In on AI Training and Fair Use | Skadden, Arps, Slate, Meagher & Flom LLP. URL: https://surl.li/hztxut
97. Li, C. (2025). Japan unveils 2025 IP strategy to climb global innovation rankings | Asia IP. URL: https://surl.lt/eienqg
98. Lince, T., Little, T., &Diakun B. (2021). EUIPO approves blockchain platform; NFT trademark mystery; SHOP SAFE Act hearing set – news digest. URL: https://surl.li/gqzhxf
99. Maidannyk, L. (2024). *Towards the EU: Legislative changes in Ukraine regarding copyright*. *Yuridichna Gazeta*, 3(781). https://surl.li/avlhyw

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

100. Marchenko V. V. Elektronne uriaduvannia v orhanakh vykonavchoi vlady: administratyvno-pravovi zasady [Electronic Governance in Executive Bodies: Administrative and Legal Basis] : Monograph / V. V. Marchenko. – Kharkiv: Panov, 2016. – 444p.
101. Marchenko, V., & Dombrovska, A. (2025). GLOBAL SOLUTIONS FOR SAFEGUARDING INTELLECTUAL PROPERTY: HOW BLOCKCHAIN REVOLUTIONIZES DIGITAL RIGHTS MANAGEMENT. *Public Administration and Law Review*, (2(22), 81–89. https://doi.org/10.36690/2674-5216-2025-2-81-89
102. Marchenko, V.. The Evolution of Information Security Framework in Ukraine: European Integration and Legal Perspectives. In *International conference on Economics, Accounting and Finance*. Retrieved from https://conf.scnchub.com/index.php/ICEAF/ICEAF-2024/paper/view/806
103. Markets in Crypto-Assets Regulation (MiCA). (2025). URL: https://surli.cc/iknsyg
104. Masuda, Y. (1980). The information society as a post-industrial society. World Future Society.
105. McGowan, B. (2025). Deepfake threats to companies. URL: https://surl.li/aygtyg
106. Meta. (2025, October 25). *Privacy Policy*. https://www.facebook.com/privacy/genai
107. Mihus, O. (2024). STRENGTHENING INTELLECTUAL PROPERTY PROTECTION IN THE EU: IT LAW AND ITS IMPACT ON THE COMPUTER GAMES INDUSTRY. *Public Administration and Law Review*, (4(20), 20–34. https://doi.org/10.36690/2674-5216-2024-4-20-34
108. Ministry of Digital Transformation of Ukraine & Office of the Ombudsman of Ukraine. (2024). *Human rights in the age of artificial intelligence: Challenges and legal regulation*. https://surli.cc/dhwont
109. Ministry of Digital Transformation of Ukraine. (2024, January). *Guidelines for responsible use of artificial intelligence for media*. https://surl.li/ejekki
110. Ministry of Digital Transformation of Ukraine. (2024). *Glossary of terms in the field of artificial intelligence*. https://surl.li/pucezu
111. Ministry of Digital Transformation of Ukraine. (2024). *White paper on the regulation of artificial intelligence in Ukraine: Vision of the Ministry of Digital Transformation (Consultation version)*. https://surl.li/vgnrns

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

112. Ministry of Digital Transformation of Ukraine. (2025, July). *Guidelines for responsible use of artificial intelligence for legal professionals*. https://surli.cc/qrmood
113. Ministry of Economy and WIPO sign Memorandum of Cooperation. URL:https://surl.li/plmgvj
114. Ministry of Economy of Ukraine, Intellectual Property and Innovation Office. (2024, November). *Guidelines on responsible use of artificial intelligence: Intellectual property issues*. https://surli.cc/tbvymf
115. Moille, C. (2025). France Takes Pioneering Step in Recognizing Blockchain Time-Stamping as Proof of Authorship in Intellectual Property. URL: https://surl.lt/vtmrui
116. Mojang Studios. (2025). *Minecraft usage guidelines.* Retrieved December 14, 2025, from: https://www.minecraft.net/en-us/usage-guidelines
117. Naisbitt, J. (1982). Megatrends: Ten new directions transforming our lives. Warner Books.
118. Non-Fungible Tokens and Intellectual Property: A Report to Congress. (2024). URL: https://surl.li/jcrygm
119. OECD. (2021). *Illicit trade: Misuse of e-commerce and online platforms for trade in counterfeits.* OECD Publishing. https://www.oecd.org/en/publications/illicit-trade-misuse-of-e-commerce-and-online-platforms-for-trade-in-counterfeits_07d1032d-en.html
120. OECD. (2025). *Mapping the global trade in fakes: Global trends and enforcement challenges.* OECD Publishing. https://www.oecd.org/en/publications/mapping-the-global-trade-in-fakes_8b2be95f-en.html
121. OpenAI. (2025, October 25). *Terms of Use*. https://openai.com/uk-UA/policies/usage-policies/
122. Organisation for Economic Co-operation and Development, & European Union Intellectual Property Office. (2025). *Mapping the global trade in fakes: Global trends and enforcement challenges*. OECD Publishing. https://www.oecd.org/en/publications/mapping-the-global-trade-in-fakes_8b2be95f-en.html
123. Organisation for Economic Co-operation and Development. (2021). *Illicit trade: Misuse of e-commerce and online platforms for trade in counterfeits*. OECD Publishing. https://www.oecd.org/en/publications/illicit-trade-misuse-of-e-commerce-and-online-platforms-for-trade-in-counterfeits_07d1032d-en.html

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

124. Oxford Insights. (2022–2024). *Identifying risks in public contracts: Generative AI and the Company Analysis Tool*. https://surl.li/nfgyye
125. Pascoe, C., Quinn, S., & Scarfone, K. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Papers, NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
126. Preparing for the Ukraine-European Commission negotiating: copyright. URL: https://nipo.gov.ua/en/ua-mock-session-7-d2-en/
127. Ramalho, A. (2021). *Intellectual property protection for AI-generated creations*. Routledge. https://surl.li/lfskzy
128. Ramos, A. (2022). The metaverse, NFTs and IP rights: to regulate or not to regulate? URL: https://surl.li/ycypcv
129. Rechardt, L. (2015). Streaming and Copyright: a Recording Industry Perspective. URL: https://surl.lu/vdwavt
130. Reggianini, E. (2025). Standardizing On-chain IP Rights Management. URL:https://surl.li/dxyajr
131. Reputation Institute. (2016, March 22). *2016 Global RepTrak® 100: The world's most reputable companies*. https://www.rankingthebrands.com/PDF/Global%20RepTrak%20100%20Report%202016%2C%20Reputation%20Institute.pdf
132. Reuters. (2025, July 15). *Roblox launches IP licensing platform, partners with Netflix, Lionsgate.* https://www.reuters.com/business/media-telecom/roblox-launches-ip-licensing-platform-partners-with-netflix-lionsgate-2025-07-15/
133. Rindova, V. P., Williamson, I. O., Petkova, A. P., & Sever, J. M. (2005). Being good or being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal, 48*(6), 1033–1049. https://doi.org/10.5465/amj.2005.19573108
134. Roblox. (2025-a). *Roblox Terms of Use.* Retrieved December 14, 2025, from: https://en.help.roblox.com/hc/en-us/articles/115004647846-Roblox-Terms-of-Use
135. Roblox. (2025-b). *License Manager Terms.* Retrieved December 14, 2025, from: https://en.help.roblox.com/hc/en-us/articles/42542704086548-License-Manager-Terms
136. Rosati, E. (2022). The missing link: How blockchain technology can help protect IP owners and consumers. URL: https://surl.li/pngeso
137. Rose, A. (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. URL: https://surl.li/sdrxzm

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

138. Rose, A. (2020). Blockchain: Transforming the registration of IP rights and strengthening the protection of unregistered IP rights. URL: https://surl.li/inkqba
139. Rota, D., & Douglass S. M. (2024). Don't Forget About NFTs! USPTO and USCO Issue Joint Study on the Interplay Between NFTs and Intellectual Property. URL: https://surl.li/vlyuzq
140. Roth, E. (2025, November 12). *Roblox is opening up its IP licensing platform. The Verge.* https://www.theverge.com/news/819407/roblox-is-opening-up-its-ip-licensing-platform
141. Rubryka. (2024, September 24). *Solutions from Ukraine: Ukrainian IP Office grants copyright to AI-generated images for first time*. https://surl.li/czcath
142. Sabreen, A. (2023). Online courts and private and public aspects of open justice: Enhancing access to court or violating the right to privacy? The Age of Human Rights Journal, 20. https://doi.org/10.17561/tahrj.v20.7516
143. Savchuk, V., & Tsurkan, O. (2025). Legal Landscapes: Ukraine – Intellectual Property. URL: https://surl.li/crdlvh
144. Schmalenberger, A. (2022). Smart contracts in the Data Act. URL: https://surl.li/xybtvw
145. Shakhatreh, H. (2024). Comparison of Commercial Dispute Resolution Mechanisms in Jordan and the Middle East. *Public Administration and Law Review*, (2(18), 51–66. https://doi.org/10.36690/2674-5216-2024-2-51-66
146. Shakhatreh, H. J. M. (2023). Development of E-Commerce within the Framework of Compliance with Financial Law. *Financial and Credit Activity Problems of Theory and Practice*, *4*(51), 429–439. https://doi.org/10.55643/fcaptp.4.51.2023.4123
147. Shakhatreh, H., & Ababneh, E. M. (2023). The main ways of leaking commercial secrets and measures to protect them. *Economics, Finance and Management Review*, (2), 76–82. https://doi.org/10.36690/2674-5208-2023-2-76-82
148. Sharp, A. J. & Lobel, O. (2023). Smart Royalties: Tackling the Music Industry's Copyright Data Discrepancies through Blockchain Technology, Smart Contracts, and Non-Fungible Tokens. URL: https://surl.li/cfjdvc
149. Somal, S. (2025). The Increasing Threat of Cyber Espionage and Its Impact on Trade Secret Protection. URL: https://surl.li/zgdecf

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)

150. Susskind, R. (2020). Online court and the future of justice. Oxford University
Press. https://doi.org/10.1093/oso/9780198838364.001.0001
151. Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media.
152. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world. Penguin.
153. The Green Paper on the Electronic Governance in Ukraine. URL: http://etransformation.org.ua/2014/11/24/355/
154. The RepTrak Company. (2020). *2020 Global RepTrak: A decade of reputation leaders*. https://www.reptrak.com/wp-content/uploads/2022/04/2020-Global-RepTrak-Report.pdf
155. Toffler, A. (1980). The third wave. Morrow. URL: https://surl.li/qfsbhv
156. UANIPIO is in the process of integration with WIPO digital platforms. URL: https://nipo.gov.ua/en/integration-wipo-digital-platforms-ga-2025/
157. Vasyliev, S. (2025). The Genesis of Online Dispute Resolution in Ukraine. *Public Administration and Law Review*, (3(23), 65–79. https://doi.org/10.36690/2674-5216-2025-3-65-79
158. Verkhovna Rada of Ukraine. (2022, December 1). *Law of Ukraine "On copyright and related rights" (No. 2811-IX). https://surl.li/bnqgnt*
159. Walport, M. (2016). Distributed ledger technology: Beyond blockchain. UK Government Office for Science.
160. WCT Notification No. 30. [WIPO Copyright Treaty]. Accession by Ukraine. URL: https://surl.lt/hbopek
161. What is Intellectual Property? URL: https://surl.li/vgmkpj
162. Whiddington, R. (2024, August 15). *Artists have won a small victory in a potentially landmark artificial intelligence copyright case*. Artnet. https://surli.cc/heagsn
163. World Intellectual Property Organization. (1996, December 20). *WIPO Copyright Treaty (WCT)*. WIPO Lex. https://www.wipo.int/wipolex/en/treaties/textdetails/12740
164. World Intellectual Property Organization. (2017). *WIPO Overview 3.0: WIPO Panel Views on Selected UDRP Questions*.https://www.wipo.int/amc/en/domains/search/overview3.0/
165. World Intellectual Property Organization. (2019). *Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps". WIPO Magazine* (Issue 5/2019). https://shorturl.at/9IM2Q

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

166. World Intellectual Property Organization. (2019). *Protecting trade secrets: How organizations can meet the challenge of taking "reasonable steps". WIPO Magazine.* https://www.wipo.int/en/web/wipo-magazine/articles/protecting-trade-secrets-how-organizations-can-meet-the-challenge-of-taking-reasonable-steps-41043
167. World Intellectual Property Organization. (2025). *Copyright*. Retrieved December 15, 2025, from https://www.wipo.int/en/web/copyright
168. World Intellectual Property Organization. (2025). *Summary of the Berne Convention for the Protection of Literary and Artistic Works (1886)*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/ip/berne/summary_berne
169. World Intellectual Property Organization. (2025). *Summary of the Paris Convention for the Protection of Industrial Property*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/ip/paris/summary_paris
170. World Intellectual Property Organization. (2025). *Summary of the Madrid Agreement concerning the international registration of marks*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/registration/madrid/summary_madrid_marks
171. World Intellectual Property Organization. (2025). *Summary of the Patent Cooperation Treaty (PCT) (1970)*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/treaties/registration/pct/summary_pct
172. World Intellectual Property Organization. (2025). *Trade secrets*. Retrieved December 14, 2025, from https://www.wipo.int/en/web/trade-secrets
173. World Intellectual Property Organization. (2025). *WIPO Guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).* https://www.wipo.int/amc/en/domains/guide/
174. World Intellectual Property Organization. (2025). *WIPO guide to the Uniform Domain Name Dispute Resolution Policy (UDRP)*. Retrieved December 14, 2025, from https://www.wipo.int/amc/en/domains/guide/
175. World Intellectual Property Organization. (2025). *WIPO guide to the Uniform Domain Name Dispute Resolution Policy (UDRP).* Retrieved December 14, 2025, from: https://www.wipo.int/amc/en/domains/guide/

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

176. World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization). https://www.wto.org/english/docs_e/legal_e/27-trips.pdf Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177–186. https://doi.org/10.1016/S0363-8111(97)90023-0
177. World Trade Organization. (1994). *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) (Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization)*.https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm
178. World Trade Organization. (2025). *Agreement on Trade-Related Aspects of Intellectual Property Rights: Part III, enforcement of intellectual property rights*. Retrieved December 14, 2025, from https://www.wto.org/english/docs_e/legal_e/27-trips_05_e.htm
179. Xalabarder, R. (2002). Copyright: Choice of Law and Jurisdiction in the Digital Age. URL: https://surl.li/krkbzb

https://doi.org/10.36690/IPP ISBN 978-9916-9389-5-9 (pdf)

Intellectual property: protection in modern conditions

Monograph

Number of copies: 300
First printing: December 17, 2025
DOI: https://doi.org/10.36690/IPP
Distributed worldwide by ***Scientific Center of Innovative Research OÜ***
office@scnchub.com
Full text available online at https://scnchub.com

https://doi.org/10.36690/IPP
ISBN 978-9916-9389-5-9 (pdf)