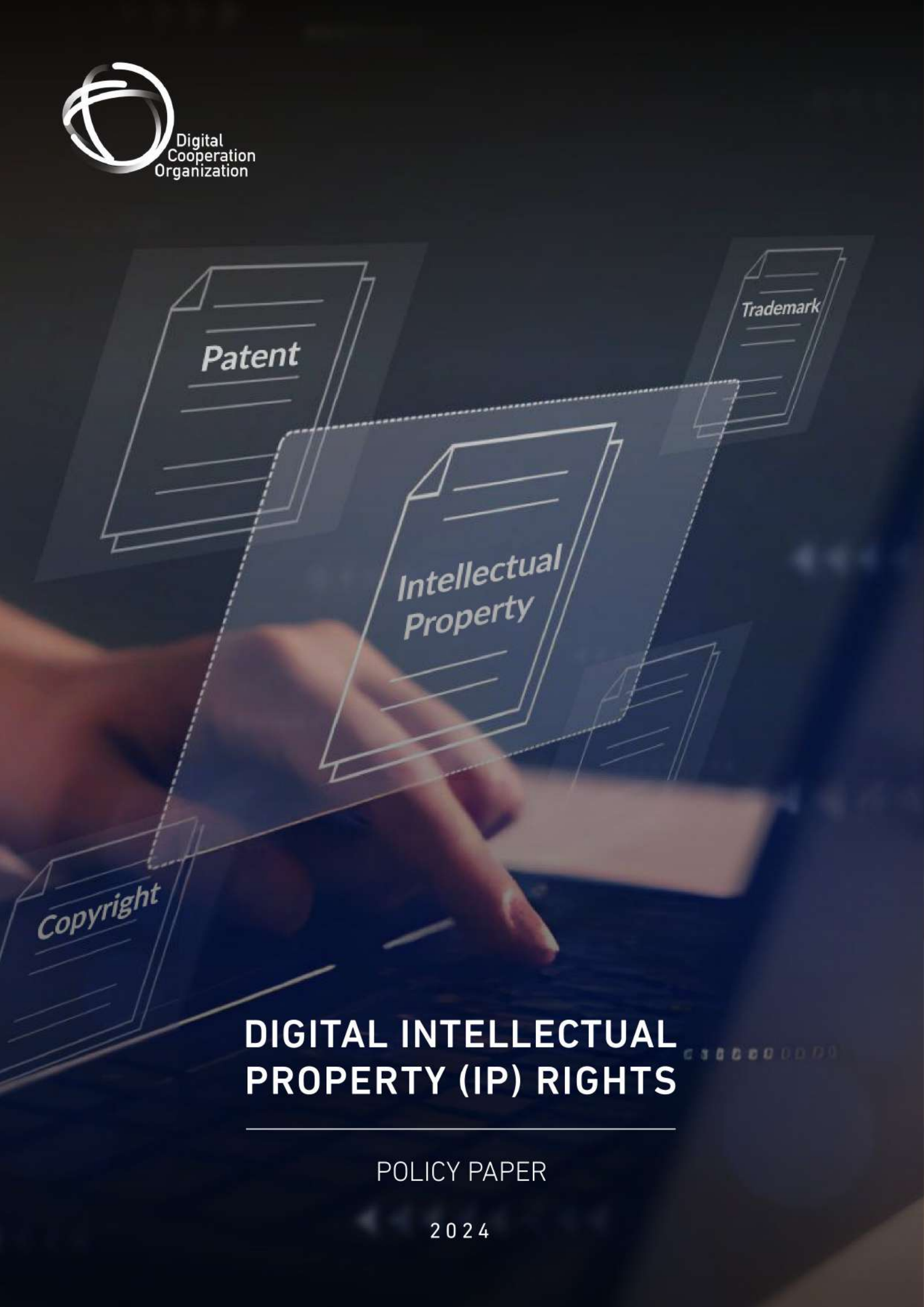
Digital Cooperation Organization




# DIGITAL INTELLECTUAL PROPERTY (IP) RIGHTS

POLICY PAPER

2024

# DOCUMENT DISCLAIMER

The following legal disclaimer ("Disclaimer") applies to this document ("Document") and by accessing or using the Document, you ("User" or "Reader") acknowledge and agree to be bound by this Disclaimer. If you do not agree to this Disclaimer, please refrain from using the Document.

This Document, prepared by the Digital Cooperation Organization (DCO). While reasonable efforts have been made to ensure accuracy and relevance of the information provided, the DCO makes no representation or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained in this Document.

The information provided in this Document is intended for general informational purposes only and should not be considered as professional advice. The DCO disclaims any liability for any actions taken or not taken based on the information provided in this Document.

The DCO reserves the right to update, modify or remove content from this Document without prior notice. The publication of this Document does not create a consultant-client relationship between the DCO and the User.

The designations employed in this Document of the material on any map do not imply the expression of any opinion whatsoever on the part of the DCO concerning the legal status of any country, territory, city, or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The use of this Document is solely at the User's own risk. Under no circumstances shall the DCO be liable for any loss, damage, including but not limited to, direct or indirect or consequential loss or damage, or any loss whatsoever arising from the use of this Document.

Unless expressly stated otherwise, the findings, interpretations and conclusions expressed in this Document do not necessarily represent the views of the DCO. The User shall not reproduce any content of this Document without obtaining the DCO's consent or shall provide a reference to the DCO's information in all cases.

By accessing and using this Document, the Reader acknowledges and agrees to the terms of this Disclaimer, which is subject to change without notice, and any updates will be effective upon posting.

# TABLE OF CONTENTS

# EXECUTIVE **SUMMARY**

# EXECUTIVE SUMMARY

In the age of rapid digital transformation, the protection of Digital Intellectual Property (IP) rights has emerged as a paramount concern, driving innovation, economic growth, and the evolution of digital ecosystems. With this concern, the Digital Cooperation Organization (DCO) has developed this policy paper, which is based on extensive analysis, research, and discussion with experts that participated in the DCO's Digital Space Accelerator (DSA) global roundtables in:

- **Riyadh – September 19, 2023**
- **Cape Town – November 15, 2023**
- **Geneva – December 7, 2023**

This policy paper explores the complex domain of Digital IP Protection, elucidating its pivotal importance, formidable challenges, stakeholders' roles, and crucial policy recommendations for the DCO Member States and beyond.

The paper emphasizes that Digital IP, encompassing digital patents, copyrights, trademarks, and trade secrets, represents a diverse range of creations born from human intellect. This includes inventions, literary and artistic works, designs, symbols, and digital assets such as software, algorithms, and databases, all of which play a crucial role in shaping the digital economy.

Central to the digital economy, Digital IP stands as a cornerstone of innovation and economic progress. It incentivizes creativity, fuels competition, encourages investments in research and development, and facilitates the monetization of digital assets, underpinning a vibrant digital marketplace. The paper emphasizes the importance of safeguarding Digital IP to fully realize its benefits to the digital economy.

The paper also discusses a myriad of challenges that Digital IP faces. These encompass navigating the complexities introduced by emerging technologies such as Artificial Intelligence, Blockchain, Internet of Things (IoT), and the immersive technologies (AR / VR / XR), grappling with cybersecurity threats that endanger digital assets and proprietary information, balancing IP rights with evolving data privacy concerns, and addressing the intricate legal framework surrounding copyright, tech patents, and data privacy laws, alongside ethical considerations in IP protection strategies.

The paper explores a diverse array of stakeholders of the digital IP ecosystem, each playing a crucial role in shaping, enforcing, and safeguarding Digital IP. From individual creators and innovators driving new IP assets to governments setting IP policies and enforcing laws, from legal professionals interpreting IP regulations to online platforms managing IP infringement issues, the paper highlights the importance of collaboration among these stakeholders for robust digital IP protection.

Reflecting on the global Digital IP landscape, the paper also underscores the need for international cooperation and alignment of IP frameworks across the DCO Member States, recognizing the interconnected nature of digital economies and the shared challenges in IP protection.

Drawing upon these insights, the policy paper proposes a series of policy recommendations and identifies steps that the DCO Member States can take towards implementing them. These include:

### 1. Harmonizing laws and adherence to international treaties and conventions

- Establishment of common strategy for accession to international treaties or conventions especially related to digital IP protection.
- Comparing and analyzing existing laws from different jurisdictions to identify best practices and develop tailored legislative and regulatory approaches to foster greater collaboration and innovation.
- Establishing consistent IP laws and standardized methodologies across regions to facilitate cross-border innovation and economic growth.

### 2. Raise awareness of IP protection in the DCO Member States

- Develop and agree on strategies for raising awareness on IP and Digital IP protection across the DCO Member States.
- Ensure the strategies and standards are socialized across the DCO Member States.
- Implement awareness and education campaigns on the importance of digital IP protection.

### 3. Develop IP Courts and Alternative Dispute Resolution (ADR) systems

- Develop IP Courts that have specialization to look into the digital IP matters.
- Invest resources in training the disciplines required in specialist IP courts.
- The establishment of Alternative Dispute Resolution ("ADR") systems and an emphasis on mediation, ideally with these systems being harmonized across all, or a subset of DCO Member States.

### 4. AI Regulation

- Develop strategies with guidelines on regulation of AI development and use, also include elements of regulation for training and use of AI in relation to the Digital IP rights.

### 5. Promote adoption of Digital Rights Management (DRM) technologies

- Promote the adoption of DRM technologies to protect Digital IP and prevent unauthorized access, distribution, and reproduction of copyrighted materials.
- Strike a balance so that DRM does not stifle creativity and innovation within the digital economy.

### 6. Data Rights

- Consider how best to protect rights in data, striking a balance between encouraging technological advancement and innovation on the one hand, and enabling businesses to protect the investment made by them in accumulating the valuable data that they hold, on the other.

### 7. Technology / software patents

- Investigate options on how best to deal with software patentability in a way that promotes innovation in the DCO economies.

### 8. Design data privacy regulations that cooperate with international standards whilst fostering innovation

- Harmonize data privacy principles across the DCO Member States and align them with international standards.
- Design data privacy regulations and compliance programs which have the same or similar standards to other data privacy regimes.

### 9. Incorporate fair/use dealing into copyright law

- Implement 'permitted use exceptions' into copyright frameworks so that innovation may continue to thrive within the digital economy without depriving the digital copyright creators of compensation and incentives to create.

This policy paper advocates for collective action from stakeholders to fortify Digital IP protection, stimulate innovation, and foster a digital economy that benefits society at large, underscoring the imperative of a harmonized and forward-looking approach to Digital IP governance.

# 1

# INTRODUCTION

# INTRODUCTION

Intellectual property ("**IP**") plays a significant role in driving innovation and economic growth by offering legal protection and financial incentives to creators and inventors, as well as those who provide funding for their work. However, the proliferation of powerful new technologies emerging in recent years poses numerous challenges to the protection and enforcement of IP rights under existing regimes. In a borderless world where innovation sets the pace of the digital economy, it is important for IP regimes to anticipate and monitor risks, responding to them appropriately to ensure there is a balance between enabling innovation and protecting creativity.

This policy paper identifies the main challenges facing IP in the digital world, including the impact of emerging technologies, cybersecurity and digital piracy on the protection and enforcement of IP rights. Our primary research consists of subject matter expert input from multiple roundtables and surveys. Produced over the span of six months, our secondary research sets out the legal frameworks which address issues of IP ownership, protection and enforcement in the digital context. Furthermore, this paper identifies possible areas for the DCO Member States to consider for improving digital IP protection.

The insights have been drawn together to produce our recommendations for the DCO Member States and beyond, which are designed to help develop robust and effective systems for protecting IP rights in the digital environment whilst still enabling IP to power innovation and fuel growth in the digital economy.

# 2

# DIGITAL IP AND ITS **IMPORTANCE IN THE DIGITAL ECONOMY**

# DIGITAL IP AND ITS IMPORTANCE IN THE DIGITAL ECONOMY

## a. What is IP?

According to the World Intellectual Property Organization ("**WIPO**")[1], Intellectual Property refers to intangible creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names, and images used in commerce. IP rights are rights which essentially grant creators legal protection over their creations for a designated period. During this period, the owner of the IP has the exclusive right to exploit the IP, meaning they can prevent others from selling, distributing, or otherwise using the IP. IP rights allow owners to monetize their IP (through licensing for example), with such monetization theoretically providing an incentive for continued innovation that benefits the public.

As Intellectual Property is intangible, it fundamentally differs from 'real' property, but given its cultural and economic significance, IP is in many ways treated like physical property. There are four main types of IP rights (as set out below), all of which can apply in both physical and digital contexts:

**1. Patents:** According to WIPO, a patent is an exclusive right granted for an invention, which can be a product or a process that generally offers a new way of doing something or provides a new technical solution to a problem. To obtain a patent, technical information about the invention must be disclosed to the public through a patent application.

**2. Copyright:** According to WIPO, copyright "is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings."

**3. Trademarks:** According to the United States Patent and Trademark Office, a trademark can be a word, phrase, symbol, design, or a combination thereof that distinguishes goods or services[2]. It functions as a recognition tool for customers in the marketplace, aiding them in distinguishing certain offerings from those of their competitors. The term 'trademark' encompasses both trademarks (utilized for goods) and service marks (used for services). Trademarks play a crucial role in identifying the origin of goods or services, providing legal protection to the brand, and acting as a defense against counterfeiting and fraudulent activities.

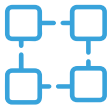
**4. Trade secrets:** According to the European Union ("**EU**"), a "trade secret is a valuable piece of information for an enterprise that is treated as confidential and that gives that enterprise a competitive advantage"[3].

## b. Digital IP – IP in the digital world

As outlined above, IP rights can protect both physical and digital assets. In this paper, the term "**Digital IP**" refers to IP in a digital context, for example where IP rights protect digital assets (including content created, stored, amended, shared and / or otherwise dealt with using technological means such as digital music files, artistic works, computer programs, films, images etc.). The proliferation of new technologies in recent times has raised numerous questions about the protection, enforcement, and ownership of Digital IP.

Digital IP is a key consideration in the development of emerging technologies. Examples include:

**1 Cloud computing:** The source code of the relevant software, licensing of software, creation and use of databases, and associated know-how on how to operate cloud computing infrastructure rely heavily on copyright laws, rights in data, and confidential information.



**2 Blockchain:** The technology is built on software whilst some distributed ledger technologies are protected by a mix of copyright, patents and trade secrets.


**3 Non-Fungible Tokens (NFTs) and Digital Assets:** NFTs are unique digital identifiers that are recorded on a blockchain and are used to certify ownership and authenticity. An NFT cannot be copied, substituted, or subdivided. The ownership of an NFT is recorded in the blockchain and can be transferred by the owner, allowing NFTs to be sold and traded. Digital assets rely on copyright works and trademarks being reproduced and proliferated through digital media to create revenue. Essentially, they are new forms of digital works, protected using existing copyright and/or trademark systems.

**4 Generative AI (GenAI):** The learning language models ("**LLMs**") central to GenAI require significant computing power and will run using copyright-protected software. The training of these LLMs requires vast amounts of input data, which often includes Digital IP such as online copyright works and databases, especially if sourced from web scraping. The outputs may be refined and combined with other materials to create new Digital IP assets, though they may require human input to qualify for legal protection.

**5 Data Licensing:** This enables massive amounts of information to be shared quickly and easily across borders in a digital medium to enable better calculations and assessments based on data, for example as used in financial institutions, mechanical engineering and civic planning (infrastructure and logistics).

**6 Spatial Technologies:** These technologies operate on software source code, which is protected by copyright, often featuring digital reproductions of copyright works such as artistic works, music, and film. Character likenesses and other trademarked images may also be reproduced (e.g., themed events in games like Fortnite, incorporating characters from various entertainment franchises such as comic books and animated shows).


**7 Streaming Services:** These are online platforms developed to enable copyright works such as films (e.g. Netflix) and music (e.g. Spotify) to be streamed to the public on a mass scale without the need for a physical copy of the relevant work.

**8 Online Marketing:** Trademarks, copyright-protected software and database rights are used in the retail sector to provide bespoke advertisements based on people's online profile and activities.

**9 Digital Twins Technology:** The sensors and interfaces used for Digital Twins run on software protected by copyright, and digital twins usually also involve other copyright-protected works (such as images and literary materials), confidential information, licensed data streams, and other databases.

**10 3D-Printing / 3D-Scanning:** Scanning and printing technology and the printing materials may be patent-protected, and both processes will use software protected by copyright. Images, data, and know-how can be licensed for use by others to build on and enhance initial efforts or to create new and unexpected items. Without licensing of scanned or printed materials, there is a risk that unauthorized 3D-printing and/or 3D-scanning could infringe rights (including IP rights) in original works, for example by 3D-printing copies of protected design articles after 3D-scanning them.

## c. Importance of Digital IP for the digital economy

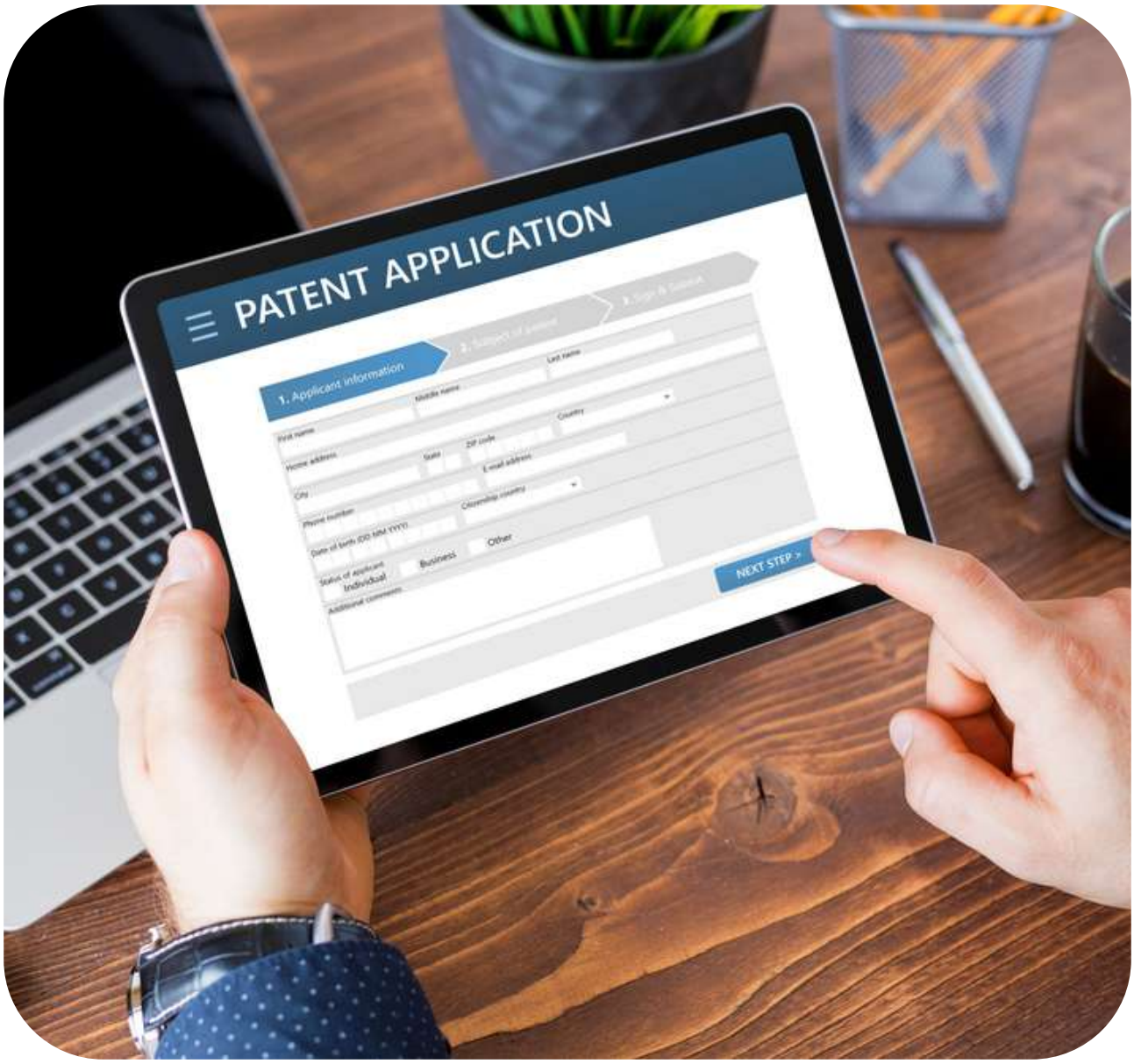
The state of the digital economy presents both opportunities and challenges in the current global economic landscape. Digital IP is central to a country's success in the digital economy due to its role in sharing knowledge and driving growth through innovation, but without effective protection measures the risk of Digital IP being infringed is always present.

Today's economy is data-driven, so it is crucial to safeguard any innovation which may provide a competitive advantage. Digital IP protection allows businesses to both protect and maximize economic potential from their ideas. Digital IP not only drives innovation, protects the creator's investments, and spurs healthy competition; it also fosters collaboration, allowing different players to leverage each other's experience, knowledge, and resources to develop the best solutions for the relevant market.

Effective Digital IP protection provides an incentive to invest in research and development in technological innovation. Hence, countries with effective and robust legal frameworks for Digital IP protection inspire investor confidence, encouraging them to make investments in these geographies and jurisdictions[4]. Fundamental factors that contribute to a country's attractiveness from an investment perspective include: (i) commitment to the rule of law; (ii) robust protection of IP, including Digital IP, and (iii) the provision of a favorable IP tax regime and innovation incentives schemes.

Strong and effective IP, and especially the Digital IP protection systems, are therefore key to attracting both domestic and foreign direct investment[5]. This investment can boost the economy of the recipient country by creating jobs, generating revenue, and fueling economic growth.

However, given the rapid proliferation of new technologies, it is challenging to develop and implement universal regulations, legal systems, and / or frameworks that encompass all the nuances of emerging technologies while keeping up with the pace of technological advancement. In many instances the application of existing IP systems to the digital world, and approaches to the new technological paradigm is proving to be unfit for purpose. International collaboration to harmonize the scope and protection of Digital IP is therefore increasingly important.



# 3 DIGITAL IP PROTECTION: WHAT ARE THE BIGGEST **CHALLENGES TO ADDRESS?**

# DIGITAL IP PROTECTION: WHAT ARE THE BIGGEST CHALLENGES TO ADDRESS?

The challenges facing the effective protection of Digital IP today are numerous, as **it has become increasingly difficult to use traditional methods of IP protection for Digital IP**. Some key challenges include:

a. Rapidly developing emerging technologies.

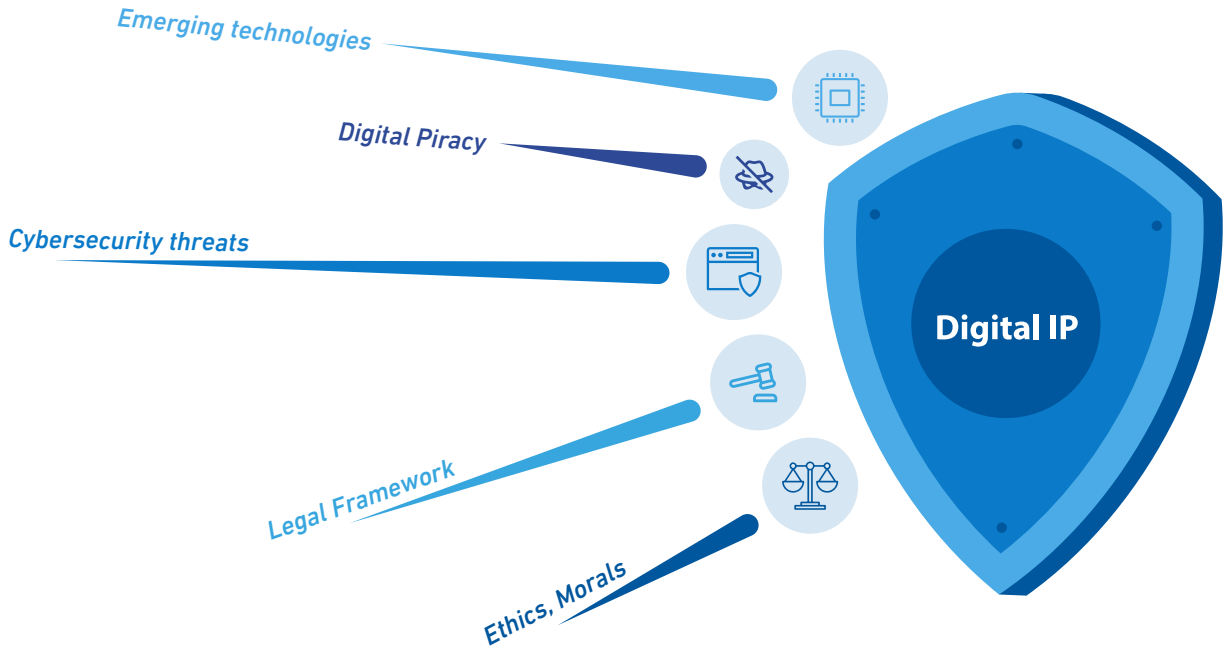
b. Cybersecurity threats.

c. Digital Piracy.

d. Inadequate legal frameworks:

- Copyright infringement and fair- use / dealing.
- Rights in data.
- Technology / software patents.
- Data privacy.

e. Ethical, policy, and moral considerations.




## a. Emerging technologies

### i. Artificial Intelligence ("AI")

To grasp the impact that AI has had in the field of IP, we must revisit Alan Turing's famous question: Can machines think?

In 1950, the British mathematician[6], a key contributor to the invention of the programmable computer, posed this fundamental question in an essay titled 'Computing Machinery and Intelligence'[7]. His essay has sparked ongoing debates among philosophers and computer scientists, and this decades-old question continues to shape the field of AI.

Even though machines can now accomplish tasks that were once deemed uniquely human, the inquiry into whether they genuinely 'think' or possess consciousness persists. AI technologies, especially machine learning algorithms, possess the ability to generate, augment, and utilize Digital IP in diverse manners. Some systems can produce original content like music, art, or literature, sparking questions about whether there is any Digital IP in this content and, if so,

who would own it? For example, if a machine generates a piece of music, should it benefit from copyright protection and, if so, should the copyright be owned by the machine's designer, the AI developer, or the machine itself?

Other systems, particularly Generative AI[8] ("**GenAI**"), have also ushered in a new wave of possibilities and complexities. GenAI has instigated transformative shifts, exemplified by text generators, which can draft essays, scripts, and poems, and even outperform humans in complex medical and legal exams at a pace which surpasses human capabilities. GenAI can also swiftly produce remarkable artwork, often mirroring the styles of renowned artists with exceptional precision, seemingly outperforming human counterparts in terms of both quality and speed.

The transformative impact of GenAI on content creation inevitably raises questions around Digital IP protection and, particularly, ownership. The concept of 'originality', traditionally attributed to human beings in the creative process, is central to the issue of Digital IP ownership. Without human involvement in the creation of AI-generated works and inventions, copyright or patent protection may not be available. As AI systems can both assist humans in developing innovative ideas and generate ideas independently, should AI systems be legally recognized as inventors under patent law or authors under copyright law?

Some argue that AI systems lack the intentionality and creativity necessary for inventorship and, therefore, should not be considered inventors[9]. However, there are proponents of recognizing AI systems as inventors[10], as it could incentivize the development and utilization of AI in the innovation process.

As set out above, the swift progress and widespread use of AI across diverse domains poses substantial challenges for how Digital IP will be protected. As AI systems grow more proficient in generating creative content and inventions, legal frameworks must adapt to confront questions around Digital IP ownership. The resolution of this challenge hinges on striking a balance between encouraging innovation and creativity whilst simultaneously safeguarding the rights of human authors, inventors, and businesses.

### ii. Blockchain

Much like AI, blockchain technology presents numerous Digital IP-related opportunities and challenges.

Blockchain, a secure and unchangeable database of information, creates immutable digital assets that remain unaltered. It provides a transparent and decentralized record of information, granting immediate access and ensuring internal data integrity. These characteristics make blockchain highly attractive from a Digital IP management perspective. For example, the immutability of blockchain technology can help to establish originality and date of creation in a copyright work by preserving an unalterable, time-stamped record of the work's creation.

The use of blockchain technology could also enhance efficiency and authenticity in establishing ownership rights, mitigating counterfeiting, enabling licensing through Smart Contracts (which are digital agreements that are signed and stored on a blockchain network, and which execute automatically when the contract's terms and conditions are met), and registering trademarks. Blockchain, therefore, already has the potential to bolster the protection of Digital IP in several ways.

Notwithstanding these benefits, given that blockchain does not inherently validate the accuracy of the original information entered (instead only ensuring that the data on the ledger has not been compromised or altered),there must be a level of trust established between parties at the start to address any underlying questions about the authenticity of the original information in the blockchain[11].

The lack of harmonization in the treatment and regulation of Digital IP could also lead to conflicts among different countries regarding accepted usage of blockchain technology.

### iii. Internet of Things ("IoT")

With regards to IoT, it is anticipated that by 2025, its global economic impact will surge from €2.7 billion to €6.2 billion, driven by applications in healthcare, manufacturing, energy, urban infrastructure, security, vehicles, and agriculture[12]. By 2025, approximately 75.44 billion devices are expected to be connected to the internet worldwide.

The IoT enables rapid collaboration and information sharing, but also poses various challenges from a Digital IP perspective due to the complexity of interactions between connected devices and other smart objects:

**1. Patents:** There are questions around the patentability of IoT inventions and, given the rapid pace of innovation in this area and the requirement for interoperability of IoT-connected devices, a serious risk of any patents granted becoming quickly obsolete.

**2. Copyright:** Many devices used in IoT rely on complex software which is protected by copyright.

**3. Rights in data:** Due to the number of devices collecting data and the multiplicity of parties involved in IoT networks, issues relating to rights in, and the protection of data are of paramount importance.

### iv. Spatial technologies – Augmented Reality, Virtual Reality, Mixed Reality (AR, VR, XR)

NASA defines Virtual Reality ("**VR**") as "the use of computer technology to create the effect of an interactive three-dimensional world in which the objects have a sense of spatial presence" [13], whereas Augmented Reality ("**AR**") involves the real-time integration of information such as text, graphics, audio, and other virtual enhancements with real-world objects[14].

VR and AR pose major Digital IP challenges from a trademark and copyright perspective. There have been instances where registered trademarks and copyright works were used in VR and AR environments without permission from the relevant IP owner, creating the risk of confusion between physical and virtual marks among consumers, ownership disputes, and infringement of registered trademarks and copyright works.

An example of this includes the Hermès International vs. Mason Rothschild[15] case. Hermes filed a lawsuit against digital artist Mason Rothschild for trademark infringement and dilution of the 'Birkin' mark because the artist created a collection of non-fungible tokens ("**NFTs**") featuring variations of the Hermès Birkin bag, titled 'MetaBirkins,' and put them up for sale on online NFT platforms and markets. Hermès argued that Rothschild was encouraging others to create more NFTs claiming to be 'MetaBirkins' or variations thereof, ultimately infringing the registered trademark 'Birkin' and diluting the 'Birkin' and 'Hermès' brands. The court ruled that existing IP legislation applies to the metaverse, NFTs, and other digital assets. This decision, aside from being highly publicized, provides an invaluable insight into the protection of Digital IP. It is worth noting though, that cases like these are based on specific facts and circumstances, and also on the approach of the courts in specific jurisdictions, so there may be other decisions in the future which do not follow this judgment.

In summary, emerging technologies have posed a variety of Digital IP challenges[16]. As each new technology engages different IP rights, the Digital IP issues and considerations are unique to each technology, use case and the relevant applicable law within a given jurisdiction. This makes it difficult to introduce effective overarching legal systems and frameworks because the issues must be addressed on a technology-by-technology basis. Further, **the pace of technological advancement results in the piecemeal building of sometimes inadequate policies and regulations relating to Digital IP, as the law struggles to keep up**.

## b. Cybersecurity

In the digital age it is easier than ever to store and share massive amounts of information, including valuable data. As organizations increase interconnectivity among their technologies and devices during their digital transformation, vulnerabilities to cyber threats have inevitably risen (especially with the digitalization of valuable corporate information including IP). As the methods of cybersecurity protection have become more sophisticated, so too have the methods used by cybercriminals to bypass such protection, leading to an ever-escalating technological arms race.

All IP is potentially valuable, but trade secrets in particular are highly valuable because they encompass proprietary information whose value relies on its confidentiality and secret nature. Trade secrets often confer a competitive advantage which is a key driver of revenue and growth to a business, so the consequences of such information losing secrecy are potentially devastating. Instead of robbing a physical safe which contains secret documents, cybercriminals actively target businesses to acquire this sort of valuable information by breaking through cybersecurity protection. If cybercriminals are successful in accessing sensitive and valuable Digital IP in this manner, it can then be sold, shared or otherwise exploited for lucrative criminal returns.

Theft of Digital IP not only jeopardizes businesses but also poses significant risks to the global economy and national security. Consequently, cybersecurity has emerged as a pivotal consideration in the safeguarding of Digital IP for businesses, public institutions, and private individuals.

The most common cybersecurity threats to Digital IP are:

**1. Data breaches:** Cybercriminals target sensitive Digital IP, including trade secrets, research and development data, or customer lists.

**2. Insider threats:** Disgruntled employees or collaborators may steal or leak Digital IP, either for personal gain or to harm the business.

**3. Phishing attacks:** Cybercriminals employ social engineering tactics to deceive employees into disclosing sensitive information or granting access to the business's network, targeting the Digital IP stored therein.

**4. Industrial espionage:** Competitors or other malicious actors may target businesses to steal valuable Digital IP or sabotage operations.

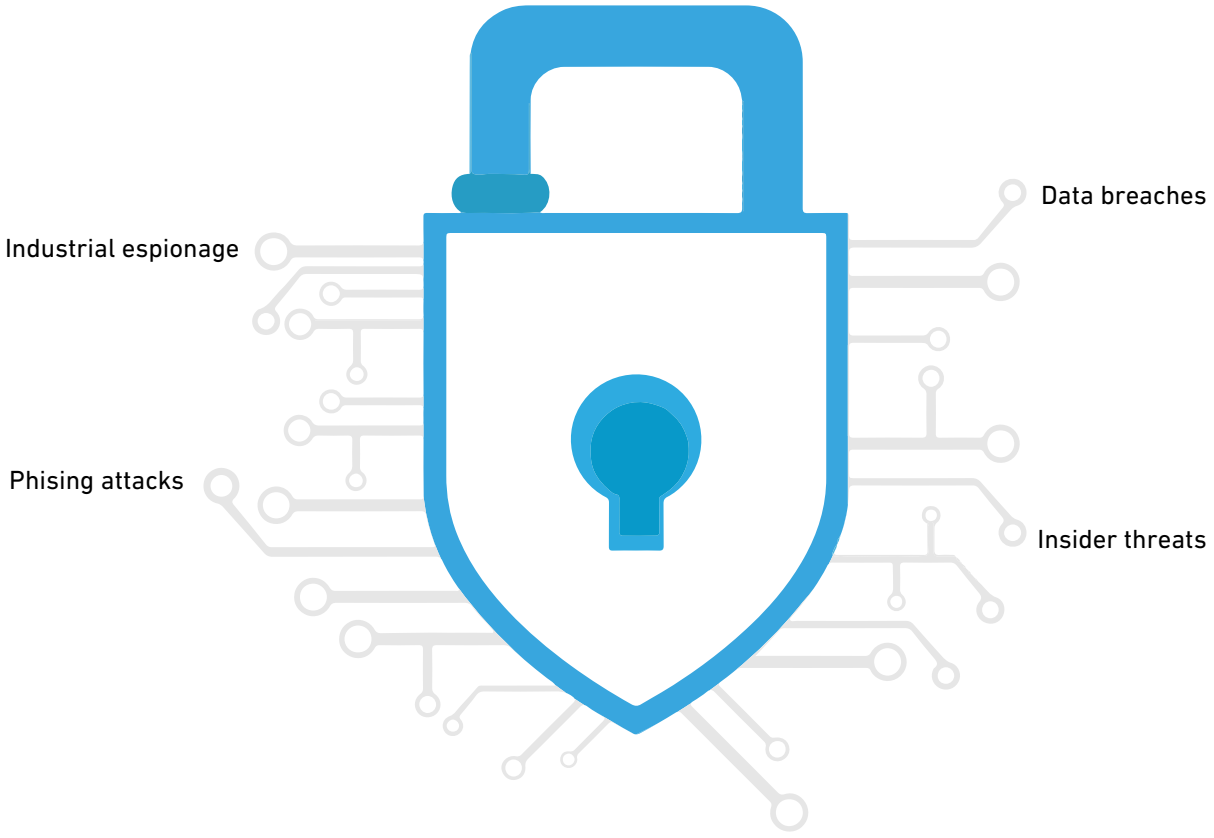



Figure 2: Most common cyber-attacks to Digital IP

The adoption and implementation of robust cybersecurity strategies is key to mitigate these cybersecurity threats[17]. This involves assessing underlying risks and conducting security audits to ensure adequate data encryption and secure communication. Additionally, the value of implementing multi-factor authentication and access control measures has been emphasized, along with monitoring networks and devices for suspicious activities. These are just a few of the cybersecurity strategies recommended to protect Digital IP.

As an example, one of the most significant cyberattacks occurred in the USA through a cybersecurity breach of SolarWinds Orion software[18], impacting both government agencies and private companies. The cyberattacks, initiated in September 2019, infiltrated the computing networks of SolarWinds, a company specializing in network management software. The threat actor injected test code into SolarWinds' "Orion" network management suite, specifically into a file included in SolarWinds's Orion software updates. Unaware of the compromise, SolarWinds distributed these updates to its customers. The hidden code created a 'backdoor,' allowing the threat actor remote access to infected computers. Cybersecurity researchers believe the threat actor used a sophisticated computing infrastructure to remotely exploit the networks and systems of SolarWinds' customers who had downloaded the compromised software updates. Given the federal government's widespread use of the Orion software for network monitoring purposes, the incident enabled the threat actor to breach infected agency information systems. Approximately 18,000 customers received the compromised software update, with a smaller subset of high-value customers, including the federal government, being specifically targeted for espionage purposes.

**The potentially huge scale of disruption and embarrassment resulting from such attacks is why it is important to deploy effective cybersecurity measures to protect Digital IP.**

## c. Digital Piracy

Digital piracy involves the illicit reproduction, distribution, or utilization of Digital IP like software, music, movies, games, e-books...etc. without the consent of the Digital IP owner. Such unauthorized use often infringes copyright (and possibly trademark) laws and involves various unauthorized online activities enabled by the internet and other digital technologies. Digital piracy constitutes an infringement of the Digital IP rights of creators, publishers, and owners, and can result in financial losses and legal ramifications.

There are various types of digital piracy:

**Illegal File Sharing:** This refers to the unauthorized sharing and distribution of Digital IP content over a network or the internet. It involves the dissemination, sale, or publication of copyrighted and protected content to the public, typically via the internet, compact disks, or external storage devices.

**Torrenting**[19]**:** While it serves as a tool for free online data sharing, torrenting is also a symbol of piracy and copyright law violations. The term 'torrenting' specifically describes the act of downloading and uploading Digital IP content (such as movies, music, or books) using a peer-to-peer network such as BitTorrent without permission, enabling users to share large files, often containing copyrighted content.

**Streaming video piracy:** This involves the illicit distribution, reproduction, or sharing of video content online without the copyright owner's authorization. This form of piracy includes the unauthorized streaming of movies, TV shows, live sports events, and other video content through illegal online platforms or services. Perpetrators typically utilize websites, apps, or social media channels to provide Digital IP content without the necessary copyright licenses or agreements.

**Computer software piracy:** This refers to "the use and or distribution of copyrighted computer software in violation of the copyright laws or applicable license restrictions. Common forms include end user piracy and counterfeiting. End user piracy occurs when an individual or organization reproduces and / or uses unlicensed copies of software for its operations by making more copies of the software than it is licensed for. Counterfeiting is the illegal duplication or distribution of software."[20]

**E-book piracy:** This involves the unauthorized distribution and sharing of copyright-protected digital books without the consent of the copyright owner or publisher, for example through uploading e-books to file-sharing websites, distributing copies through email, or sharing them on peer-to-peer networks[21].

**Game piracy:** This refers to the unauthorized copying and distribution of digital games[22], which includes the downloading or distributing of unauthorized copies of video games, often involving cracked versions that bypass digital rights management (**DRM**) protections.

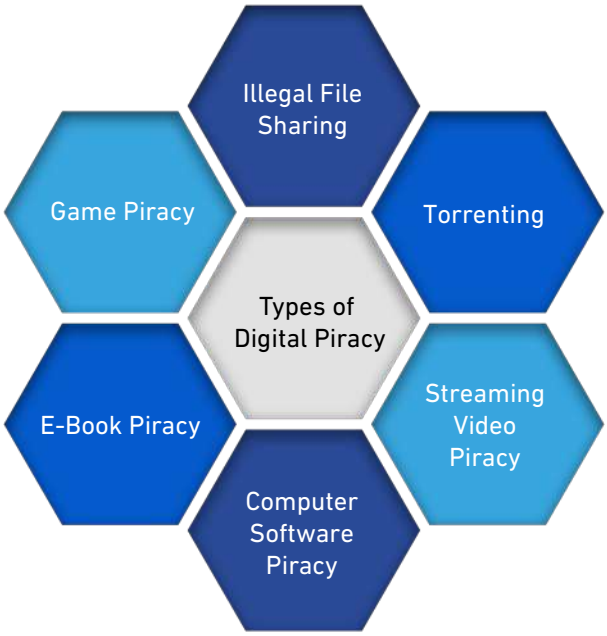



Figure 3: Types of digital piracy

One of the major issues related to digital piracy concerns consumer awareness about the practice and its illegality. For example, a recent study indicates that approximately 25% of viewers believe that using pirated sports services is justified[23].

There are several tools that have been developed to mitigate the risks of digital piracy. One such example is DRM technology. Efforts to combat digital piracy also involve taking legal action against infringing websites and individuals, increasing public awareness about the repercussions of piracy, and promoting legal alternatives such as streaming services and digital marketplaces for accessing content legally.

Digital piracy has various detrimental effects. Firstly, it leads to significant economic losses for businesses, creators, and the associated job market. The expected revenues from the sales of products or services can be significantly impacted by digital piracy.

It also diminishes the market value of Digital IP since it creates the perception among consumers that they can easily obtain Digital IP for free. Additionally, the quality of products and services is sometimes compromised, especially in the case of counterfeit products.

**Addressing digital piracy requires a collaborative effort involving governments, law enforcement agencies, industry stakeholders, and consumers. Increasing awareness, implementing strong legal measures, embracing technological innovations, and fostering international cooperation are essential steps in combating piracy and safeguarding Digital IP.**

Given the breadth of challenges to the protection and enforcement of Digital IP highlighted in this section, it is important that robust legal frameworks are in place to mitigate the above risks and ensure that Digital IP can be recognized, protected, commercialized and enforced easily. The effectiveness of Digital IP protection methods in tackling digital piracy issues should be continuously monitored and evaluated in light of the latest threats arising from advances in technology too.

## d. Legal Framework

In the past, we have seen a gradual expansion of the scope of protection afforded by IP rights as the law has evolved to try and keep up with the pace of technological advancement. Below, we examine how legal frameworks could be improved to incentivize innovation in the DCO Member States and beyond, whilst also protecting and rewarding creativity by sufficiently protecting Digital IP, with a particular focus on copyright, rights in data, technology / software patents and data privacy.

### i. Copyright*

**Copyright infringement and fair use / fair dealing**

As detailed in **Appendix A**, copyright owners have various exclusive rights over their copyright works, such as the right to copy, distribute copies (including electronically) and adapt the work. Doing any of these things without permission from the copyright owner will constitute copyright infringement. Copyright can also be infringed if someone deals with infringing copies of a work; i.e., by storing, importing and / or selling these copies.

There are exceptions which apply in specific circumstances to allow some uses of copyright works which would otherwise constitute infringement, such as criticism and review, private copying, non-commercial research...etc. These exceptions vary by jurisdiction, so international protection and enforcement of copyright can be difficult, especially in an online world where works can be shared across borders instantly.

Questions to consider include:

- How should copyright infringement and exceptions be treated in relation to emerging technologies?
- Are the existing Digital IP frameworks (especially with regards to copyright) adequate to allow technologies to grow and develop whilst providing sufficient protection to rightsholders?
- Should specific technologies be treated in a specific way under existing Digital IP frameworks (especially with regards to copyright)?
- Would a new approach be better – for example, specific defenses against copyright infringement for certain types of work when used in a specific way?
- Could the exceptions to infringement be harmonized regionally or globally in relation to certain technologies (to avoid confusion and make protection, use, and enforcement easier)?

In some countries, legal frameworks provide a defense to copyright infringement which is applicable in certain specific circumstances where use of the work is deemed to be 'fair' (i.e., where the overarching benefit of society necessitates priority over the rights of the copyright owner). Those countries that do have such defenses have enacted provisions very differently.

---

* Please refer to **Appendix A** for general background information on copyright law.

English law, for example, has the concept of '**fair dealing**'. There is a two-step test to establish whether fair dealing may apply:

***Step One – What purpose is the copyright work being used for?***

The list of purposes includes:

- Criticism and review
- Quotation
- Reporting current events
- Parody, caricature, and pastiche
- Research and non-commercial private study; and
- Text or data mining for non-commercial research

In order for the defense to apply, the use of the copyright work must be for one of the listed relevant purposes. The list of specific purposes has evolved over time, but the general principle appears to be that uses for non-commercial or cultural / journalistic reasons should be permitted.

***Step Two – Is the dealing in the work "fair"?***

Fairness is not legally defined, but the following are examples of considerations that will be considered when assessing fairness:

- How much of the copyright work has been used (considering both the quality and quantity of what has been used)?
- Does the infringing use interfere with the legitimate interests of the creator of the work (for example by preventing the creator from receiving remuneration for use of their work)?
- Is the use financially motivated or non-commercial? The use is more likely to be considered fair if the motivation for use is non-commercial

The assessment of whether a potentially infringing use is fair will take into account all relevant factors.

In contrast, the application of the principle of '**fair use**' under US law is different. 'Fair use' also attempts to strike a balance between protection for rightsholders and use that should be permitted, but there are some key differences between the fair use and fair dealing defenses:

- The list of fair use purposes is not definitive (unlike fair dealing), and so there can be less certainty in how and when the defense may apply.
- The factors to be considered when assessing whether a use is fair are:
  - Purpose and character of use
  - Nature of the work
  - The amount used and substantiality of what has been taken from the original work; and
  - The effect of the use on the potential market value of the original work

Fair use is fundamentally and intentionally more general and less specific than fair dealing, and therefore is more open to interpretation when assessing the potential application of the defense (which may make it better suited to accommodating new uses of Digital IP, specifically copyright works, through emerging technologies).

## ii. Rights in data

### Value of data to emerging technologies

Raw data may not be protected as an IP right as such, but it still has enormous value to technological development – consider the vast variety of useful information a company will have on its employees, customers, markets, past dealings, business practices, know-how relating to challenges faced in the past…etc. Then consider how powerful technology, which enables these insights to be combined and shared amongst different entities, could be.

Data has long been recognized as a valuable business asset that can be exploited through licensing and sale. However, data also needs protection to maintain its value (or the advantage it provides to its owners and authorized users).

Some industries have long-established data sharing and licensing practices, for example in the financial services and healthcare sectors. but with the advent of more advanced technology and computing capability, it is now possible to aggregate and analyze massive amounts of information to uncover insights which would not have been otherwise considered.

Data, and rights in data, are more important than ever because they fuel so much of what emerging technologies can achieve. The balance between their protection and ease of use should be a key area of focus when devising Digital IP policies which will foster the further development of technology and innovation.

### Data rights and IP

There is a patchwork of IP and related rights which protect certain elements of data in some jurisdictions, such as:

- Literary copyright in the original selection and arrangement of information in a database.
- Right in the content of a database (often depending on the investment made in gathering, verifying, and presenting the information in the database); and
- Confidential information and trade secrets (assuming the information in the database qualifies)…etc.

These rights are not harmonized internationally (other than in the EU) so extra time and attention is often required when dealing with data rights to ensure that the required rights are properly protected through data rights licensing frameworks.

## iii. Technology / software patents

### Patents in general

Patents grant monopoly rights in inventions for a limited period. To be registered and receive patent protection, a patent application must disclose how the invention works.

The rationale behind this requirement is broadly that the inventor is incentivized by the monopoly of a registered patent, whilst society may benefit from the understanding of how the invention works. Once the period of monopoly protection ends, other parties may bring products and services which make use of the invention into the market for the benefit of all.

For a patent to be granted, it must be novel, inventive and capable of industrial application. The process of registering a patent is often lengthy and expensive.

**Patents in software and emerging technology**

In many countries, patent protection is generally not available for an "invention" which solely comprises a computer program or method of doing business as such. Patenting such software was seen as anti-competitive and likely to stifle innovation.

That said, some jurisdictions have introduced rules permitting software patents in situations where it can be proved that the software invention has a technical effect or solves some sort of technical problem. However, the approach to whether a computer program may qualify for protection is not harmonized and can differ significantly between jurisdictions and regions. Issues of patent ownership have also been a hot topic recently. In several jurisdictions, there has been a noteworthy refusal to grant patent protection in respect of "inventions" created solely by an AI "inventor". For example, the respective US, UK and European patent offices refused to register an invention Stephen Thaler claimed was created by his DABUS AI system[24].

### iv. Data Privacy

The new ideas springing from developments in technology and innovation have the potential to improve living standards and enhance our ability to meet challenges we continue to face. The balance between enabling innovation and protecting individual rights is arguably most keenly fought in relation to data privacy. Some jurisdictions and regions have historically preferred a lighter touch approach to data privacy regulation and enforcement, but with the advent of the GDPR in Europe (and in particular its requirements for compliance by data controllers and potentially significant fines for non-compliance) data privacy has become much more of a priority for technology stakeholders. It seems that approaches to innovation which sacrifice data privacy are now less likely to be supported.

Developing technologies and increasing computing capability means more data, including personal data, is being used in the development and deployment of emerging technologies e.g. big data, training of LLMs for GenAI, digital twins gathering sources of information to model outcomes etc.

Emerging technologies promise big opportunities for how personal data can be used, but also big risks if personal data is misused or otherwise compromised. Robust privacy capabilities and enhancements can be an attractive feature to technology stakeholders wishing to raise finance or other backing.

## e. Ethical, political, and moral dimensions

The ethical, political, and moral dimensions of IP protection in the digital age are both complex and challenging. The rapid advancement of technology leads to new questions challenging ethics, politics, and morality every day. Considering the diversity of countries within the DCO framework, these challenges become even more pronounced, making it difficult to establish a unified view of the issues:

**Balancing innovation and public interest.** On one hand, IP protection promotes investment in innovation, research, and development. On the other, reconciling this innovation with access to goods and services of public interest that are subject to IP rights is a question that lacks easy or immediate answers. This issue was especially prominent during the pandemic, particularly in the context of the discussion around vaccines for COVID-19.

**Global harmonization.** Harmonization can be sought through international agreements, treaties, or standards, which can be transposed into the national legal systems of each signatory state. Given that in the online world, Digital IP threats potentially know no borders, the solutions require a clear understanding of the challenges that individual countries face in tackling Digital IP infringement.

**Fair use.** It is important to weigh up the rights of the copyright owner against the public interest in the use of copyright works and to strike the right balance. In this regard, DRM systems need to be reconciled with user rights.

**Countering the digital divide.** Any discussion of Digital IP protection should not promote exclusion or hinder access to technologies, especially for the most vulnerable members of society.

**Fair compensation.** Compensating the creators of these works or inventions is of paramount importance, not only in strengthening the digital economy but also from the perspective of remunerating the labor and effort invested by individuals.

**Awareness raising.** Raising awareness around the economic and social impacts of practices such as counterfeiting and piracy of Digital IP which deprive creators of the opportunity to commercialize their products and services is key and should not be overlooked.

# 4

# STAKEHOLDERS AND THEIR ROLE IN THE **DIGITAL IP ECOSYSTEM**

# STAKEHOLDERS AND THEIR ROLE IN THE DIGITAL IP ECOSYSTEM

## a. Stakeholders

There are various stakeholders in the IP ecosystem (as set out below), and balancing the competing interests of these stakeholder groups when making decisions on issues such as the development, regulation, protection, and enforcement of Digital IP can be challenging:

**Individual Creators and Innovators.** This category encompasses the individuals and / or organizations responsible for generating the content, ideas, or inventions that form the basis of Digital IP. They are often the primary victims when it comes to issues of IP infringement (including infringement of Digital IP). It is important to develop a Digital IP system which protects and rewards their innovation and creativity.

**Businesses and Corporations.** The investments made by companies in research, development and innovation should be protected, and their concerns around protecting their Digital IP from infringement, theft, and counterfeiting heard. This can only be achieved through proper consultation with this group in relation to the scope of Digital IP protection.

**Governments, Government Agencies, Decision-makers, Policymakers and Courts.** This category covers the public entities responsible for creating and enforcing laws and regulations relating to the protection of IP. They are involved in establishing legal frameworks, addressing issues related to IP infringement and creating forums in which IP disputes can be effectively heard and managed. A well-functioning Digital IP regime will require the engagement of Digital IP experts by these entities.

**Intellectual Property Offices ("IPOs").** IPOs can be quasi-government agencies, or organizations responsible for granting and regulating IP Rights within a specific jurisdiction. Some of the key functions and responsibilities of IPOs include granting and registering IP rights; conducting registered IP searches; assisting in legal processes by providing documentation related to registered IP rights and aiding in legal actions against IP infringement; collaborating with international organizations such as the WIPO and other countries' IPOs to harmonize IP regulations; and monitoring IP trends. Their role in protecting Digital IP is of paramount importance.

**Citizens.** Citizens are important stakeholders not only because they access the digital content which underpins Digital IP, but also because they are often the targets of security breaches and the counterfeit goods and digital piracy markets.

**Legal professionals.** This category encompasses lawyers, patent attorneys, and other legal experts who specialize in IP law. They are experts in legal matters relating to the protection of IP and can offer key insights into the practical application of the law and any gaps in the legal framework that need to be filled, including in relation to Digital IP.


**Internet Service Providers ("ISPs") and "Online Platforms",** notably the **large digital** platforms, including social media companies, who dominate the digital space. These (typically private) organizations play a crucial role by implementing policies to tackle the infringement of Digital IP, taking down infringing content, and cooperating with law enforcement agencies. Regulatory and legislative developments should consider their influence and role in protecting Digital IP.

**Non-Governmental Organizations ("NGOs").** Various NGOs work to combat piracy, counterfeiting, and infringement. These entities are typically consulted by governments during the policy-making and legislative processes. They raise awareness of, and lobby for IP protection and will therefore be key in shaping developments in the Digital IP sphere.

**Educational Institutions and Research Units.** These organizations are significant because they are involved in research, development, and innovation, and because their educational communities frequently use resources subject to IP protection. They frequently partner with businesses and government agencies on initiatives pertaining to developments in the field of Digital IP protection.

**International Organizations,** notably the WIPO and trade organizations contribute to the development of international standards, treaties, and agreements related to Digital IP protection, fostering global cooperation in the field. They are therefore central to discussions around the development of legal and regulatory frameworks aimed at ensuring the effective protection of Digital IP in the online environment.


Figure 4: Digital IP protection - stakeholders

## b. Specific Role of Online Platforms

As outlined above, online platforms, including social media networks, play a crucial role in the protection of Digital IP. Given that the influence of the Online Platforms often supersedes the influence of the public bodies tasked with tackling issues of Digital IP infringement and enforcement, their cooperation is crucial.

Firstly, they can implement content moderation policies to identify and remove content which infringes Digital IP, such as copyrighted material, trademarks, counterfeit goods, and pirated content. This area has seen notable advancements. Algorithms and digital fingerprinting technologies can now be utilized to identify and prevent the unauthorized distribution of copyrighted materials, such as music, movies, books, and software found online. This ensures that creators are not deprived of potential sales and revenue. Similarly, in the field of trademark protection, trademark owners can report unlawful conduct, leading to the takedown of listings or profiles that infringe their trademarks, thereby safeguarding brand identities.

In addition, the Online Platforms' data analytics capabilities allow them to identify patterns associated with the infringement of Digital IP. This enables them to proactively tackle potential issues by monitoring user behavior, and to detect unusual patterns that could indicate counterfeit sales or other infringements of Digital IP.

Online Platforms can enforce contractual clauses pertaining to technological security measures directly without relying on public mechanisms such as judicial orders or intervention from law enforcement authorities. For example, Online Platforms can independently remove copyright-protected content from their platform without the involvement of any public body. Today, online platforms hold immense significance in this field, leading to what some experts refer to as 'technological asymmetry'[25], signifying a significant departure from traditional offline boilerplate contracts.

The enforcement of traditional contracts often relies on the role of public authorities in ensuring compliance with the rights and obligations agreed between parties. In the digital realm, online platforms, through their internal systems, assume a quasi-legislative function, where the platform's architecture becomes a mode of regulation. Online platforms can directly exercise their rights through a quasi-executive function.

This type of private enforcement arises from the fact that the Online platforms can exercise a great deal of control over their users, representing a form of self-regulation and reducing the involvement of public actors in safeguarding and enforcing Digital IP rights, particularly in cases related to copyright. The balancing of this role with the need to safeguard the public interest is a highly complex matter, particularly as the economic, social, cultural, and political realities which are relevant to specific users will vary from place to place.

Some of the largest Online Platforms in the e-commerce sector such as Alibaba, Amazon, and eBay have already taken proactive measures. They have harnessed technology and developed sophisticated Digital IP protection systems. Leveraging advanced computing technologies and big data, these players have established vigilant monitoring and Digital IP infringement notification systems[26].

# 5

# DIGITAL
# IP LANDSCAPE

# DIGITAL IP LANDSCAPE

## a. Global trends

To date, there has been no harmonized global approach to the protection of Digital IP, and countries are at different stages in the development of regulatory frameworks which aim to address the key challenges outlined in this policy paper.

Comprehensive details of the approaches taken by (i) various key global players and (ii) DCO Member States to ensure the protection of Digital IP in an increasingly digitized world are set out in **Appendix B.** However, by way of a summary, some key trends at a global level include:

**AI Regulation:** The regulation of AI is high on legislative agendas, as countries attempt to strike the right balance between promoting innovation and putting in place appropriate guardrails to ensure responsible use. For example, the EU AI Act is set to be the world's first comprehensive AI law, which seeks to impose different rules depending on the level of risk posed.

**Digital IP Ownership:** We have recently seen an influx in cases dealing with issues of Digital IP ownership, particularly in relation to AI-generated digital assets. There is no uniform, global approach to this issue, and the outcomes have varied by jurisdiction. For example, in China, the Beijing Internet Court recently ruled that an AI-generated picture qualifies as a copyrightable work. In the field of patents, the UK Supreme Court recently ruled that AI cannot be an 'inventor' for the purpose of establishing patent ownership, as under the relevant legislation, an 'inventor' must be a 'natural person'.

**Bargaining Frameworks:** Ensuring that content creators are fairly compensated for the publication of their digital content on Online Platforms has been a hot topic in recent years. Australia has led the way in the field with its News Media Bargaining Code, which requires Online Platforms to negotiate fair prices with news publishers to ensure that they receive just compensation for the use of their content, and Canada is following suit with its Online News Act.

## b. Trends across the DCO Member States and opportunities for improvement

As expressed earlier, there has been no harmonized global approach to the protection of Digital IP, and digital IP rights have recently come into the limelight with the emergence of new technologies like AI. While the DCO Member States, in general, are still in the process of devising frameworks for the Digital IP, many they have taken significant strides towards strengthening their conventional IP protection and enforcement regimes. There is a good room for these conventional IP regimes to be adapted and applied to the digital reality. Some of the key initiatives implemented by the DCO Member States in this regard are set out in the table next page.

| Member States | Examples of policy initiatives implemented by the DCO Member States<br>Initiatives |
|---|---|
|  Bahrain | Reduction of official fees for patent registration for individual applicants |
|  Bangladesh | Copyright Bill 2023 |
|  Cyprus | New Trademarks Law (2019) |
|  Djibouti | Member of international treaties related to IP (e.g. Paris Convention for the Protection of Industrial Property) |
|  The Gambia | National Intellectual Property Policy & Strategy |
|  Ghana | Contracting party to most international IP treaties and a member of the African Regional Intellectual Property Organization (ARIPO) |
|  Greece | Greek Law 2121/1993 on Intellectual Property |
|  Jordan | Digital Rights Management (DRM) and Technological Protection Measures (TPM) legislation |
|  Kuwait | New copyright law (Law 75 on Copyright and Related Rights) |
|  Morocco | Member of the Hague Agreement Concerning the International Registration of Industrial Designs |
|  Nigeria | Contracting party to the Convention on Cybercrime (Budapest Convention) |
|  Oman | Law of Copyrights and Neighboring Rights |
|  Pakistan | Intellectual Property tribunals through the Intellectual Property Organization of Pakistan Act |
|  Qatar | Involvement in international treaties managed by WIPO |
|  Rwanda | Nationwide awareness campaign focused on Intellectual Property ("The Meaning of Intellectual Property in your daily Life") |
|  Saudi Arabia | Saudi Authority for Intellectual Property (SAIP) |

Notwithstanding these efforts, following are examples (non-exhaustive) of areas that have been identified for the DCO Member States to consider for improving IP protection in the digital context:

While included in the related laws, **Bahrain**[27] is yet to implement a Collective Management Organization to create a system beneficial for users and holders of copyright and related digital IP rights.

In **Bangladesh,** the more comprehensive copyright protection regime was introduced by the Copyright Bill 2023. However, newspapers, magazines, digital platform content, and public speeches have not been included in its scope[28]. These can be added to provide them with appropriate legal copyright protection.

**Cyprus** is particularly concerned about the regulation of AI and its impacts on IP rights. The Cypriot government approved a National AI Strategy in 2020[29], but it is expected that EU AI Act will assist in refining and implementing the national strategy by addressing some of the risks and challenges in this field.

**Djibouti** is a member of various IP treaties such as the Paris Convention, however, since the country does not have domestic laws governing the copyright protection of Digital IP, there is an opportunity to create robust legal framework to match the needs of a prosperous digital economy.

In **The Gambia**, key gaps identified within the context of IP, that are equally applicable to the Digital IP, include the need for: integration of IP into national and sectoral development policies, a comprehensive IP framework, enhancement of institutional mechanisms for policy coherence, accession to legal and international commitments, development of administrative capacity and enhancement in generation and protection of IP assets. Furthermore, there are opportunities related to increasing awareness of IP, improving enforcement of IP rights, and proper utilization of IP in areas where the country has a competitive edge, including distinctive products, traditional knowledge, and creative industries[30].

**Ghana's** basic legal framework can be improved to include various IP rights, especially the essential ones related to the digital economy. The DCO membership could serve as a catalyst for developing a stronger legal framework.

In **Greece,** intellectual property is governed by the Greek Law 2121/1993 on Intellectual Property. Different articles of the law were amended from time to time to keep adapting it to the ongoing developments in IP and copyright domains. The most recent amendment with regards to emerging technologies, and relevant to the Digital IP (L. 4961/2022) was made in 2022 whereby 3D printed works were included in the definition of works protected by intellectual property (L. 2121/1993)[31]. In particular, computer-aided design files (CAD files) were also protected, provided they contain source code. 3D printers were also added as material carriers of digital reproduction, the use of which accords to the creators of works a reasonable remuneration. There is further room to adapt the legislation to cater for additional IP protection requirements that arise with emerging technologies. Additionally, it is expected that EU AI Act will assist in addressing some of the risks and challenges associated to the IP implications of AI in Greece.

In **Jordan**, there is an opportunity to strengthen Research and Development (R&D) and IP-specific tax incentives, as well as to combat the high levels of copyright infringement, particularly online [32]. There is a significant room for improvement on the Digital IP protection in Jordan, given that The Software Alliance ("**BSA**") estimates suggest that 55% of software in Jordan is pirated [32].

**Kuwait's** IP protection regime can benefit significantly by enhancing the country's participation in international IP related treaties and focusing on developing laws and regulations specific to the Digital IP protection.

One of the factors that significantly boosted **Morocco's** position in international rankings was its ratification of all the Acts that together constitute the Hague Agreement. However, there is also a recognized need for legal reforms in the design rights environment [32].

**Nigeria** has opportunity to improve on developing Technological Protection Measures ("**TPM**") and DRM legislation prohibiting the use, sale, manufacture, and distribution of circumvention devices employed for copyright infringement purposes. On a broader scale, piracy is rampant and poses substantial risks for rightsholders in enforcing Digital IP rights. According to BSA estimates, the software piracy rate in Nigeria stands at 80%, [32] a figure that has remained virtually unchanged over the past decade.

There is an opportunity for **Oman** to enhance capacity on IP protection regime, particularly in relation to its judicial system. Local courts sometimes struggle with trademark infringement cases due to shortage of expertise and experience in this field [33]. The capacity building is especially important in the context of emerging technologies and their impact on the Digital IP.

**Pakistan** is currently in the process of reforming its national IP framework, including statutory laws concerning patents, copyright, and trademarks [32]. The government and parliament of Pakistan are actively engaged in a comprehensive program aimed at national IP rights reforms. The reforms need to take Digital IP protection into consideration.

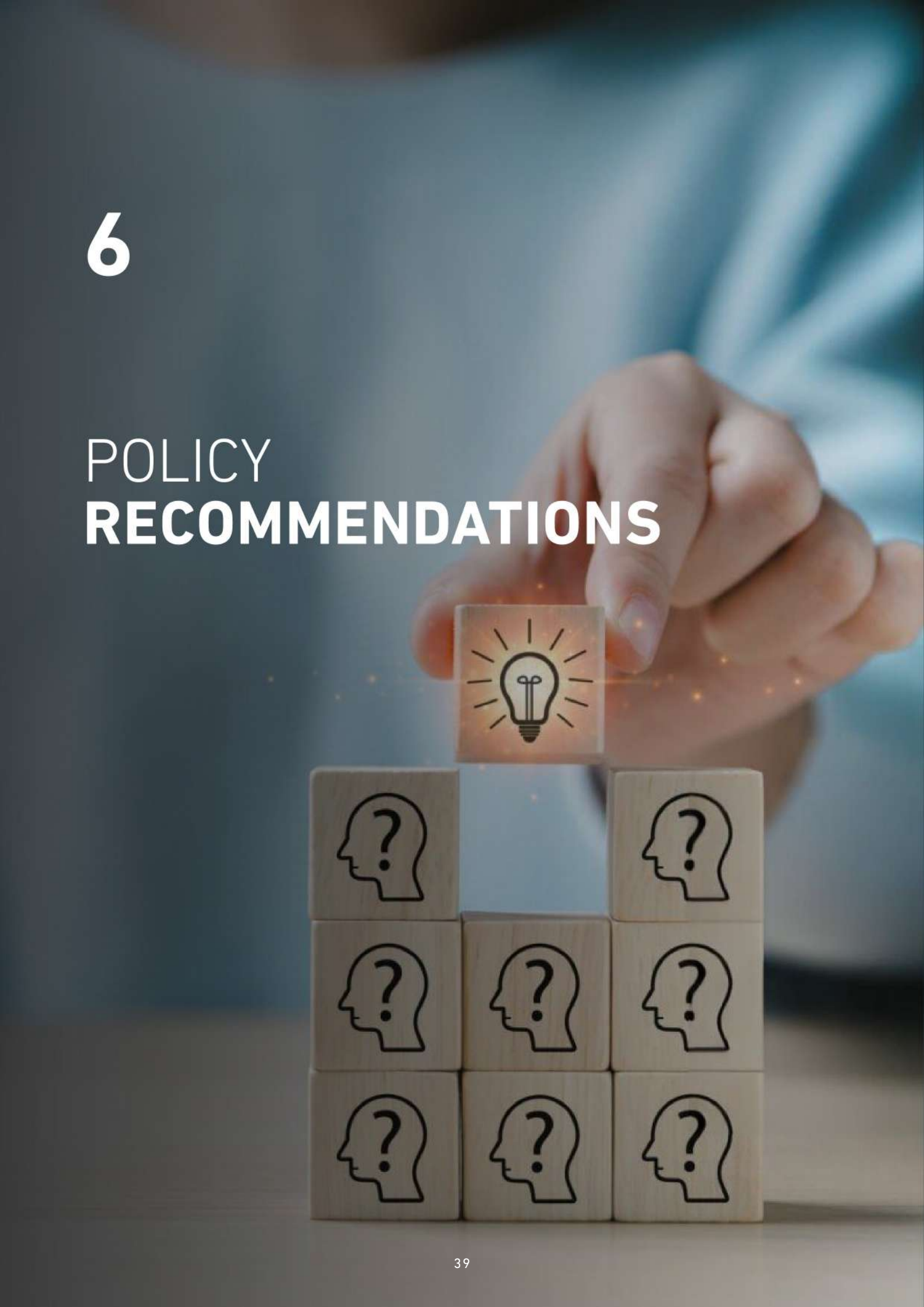
**Qatar** established a law on industrial designs in 2002 [27]. The implementing regulations for this law still need to be developed in order to bring the law into effect. In 2020, a new Law on the Protection of Industrial Designs was enacted, replacing the previous legislation. The law has not been publicly released, and its implementing regulations are yet to be issued. It is expected that the law and its implementing regulations include specific articles of the Digital IP protection.

While **Rwanda** excels in fostering an innovation-friendly environment, there is a need for improvement in the Digital IP management [34]. Rwanda is actively working to raise awareness about the importance of this topic, with a particular focus on increasing women's participation in technological advancements, artistic developments, and successful businesses [35]. Currently, structural barriers are resulting in gender disparity in IP registration, with only 15% of total IP records in Rwanda attributed to women [36].

**Saudi Arabia** has an opportunity to work on guaranteeing the reciprocity of IP registration with other states. This means ensuring the same scope of IP protection that companies might expect in countries like the United States and other Western markets. Currently, most rights should be registered in the country, under local laws. For example, a US trademark registration or US patent does not provide protection in Saudi Arabia [37].

# 6

# POLICY **RECOMMENDATIONS**



# POLICY RECOMMENDATIONS

Ideally, a global approach to Digital IP that fosters innovation should consider all relevant stakeholders. International treaties have historically played a significant role in IP, although they have not always addressed all IP (especially the Digital IP) issues comprehensively. National jurisdictions also have a role to play. Below, some recommendations will be presented to strengthen the protection of Digital IP, always with the aim of accelerating its contribution to the digital economy.

Please note these recommendations are offered based on expert opinions and experiences of how collaboration between stakeholders can help advance the development of the IP ecosystem, including in relation to Digital IP. The recommendations are not intended to be definitive, and it may be that there are different or amended steps which may be more favorable in a given context (whether geographical, regional, to do with a specific form of Digital IP or Online Platform etc.). However, we hope they will be useful in at least adding to the considerations about how best to enhance the protection and productivity of Digital IP through policy.

## *Recommendation 1: Harmonization of laws and adherence to international treaties and conventions*

### *Summary of recommendation*

This recommendation involves the following steps:

- **Establishment of a common strategy** for accession to **international treaties or conventions related to Digital IP protection,** particularly in the digital space.
- **Benchmarking laws:** Comparing and analyzing existing laws from different jurisdictions to **identify best practices and develop tailored legislative and regulatory approaches to foster greater collaboration and innovation.**
- **Harmonizing laws:** Establishing consistent IP laws and standardized methodologies across regions to facilitate cross-border innovation and economic growth.

### *Context*

The international sources for IP protection include conventions and treaties administered by the WIPO, the UNESCO Universal Copyright Convention, the World Trade Organization ("**WTO**") Agreement on Trade-Related Aspects of Intellectual Property Rights ("**TRIPS**"), and other treaties related to IP. The two main IP Protection Conventions are the Berne Convention and the Paris Convention. There are some DCO Member States that are parties to some of these conventions, but there is no common regional strategy. Given the significance of these treaties and conventions in the field of IP protection, we believe that one of the recommendations should focus on the accession to existing and future international treaties and conventions that are especially relevant to the Digital IP protection, in a coordinated manner amongst the DCO Member States.

Each of the above aspects of this recommendation emanated from the global roundtables that the DCO held throughout 2023. The establishment of a common regional strategy for accession to international treaties or conventions was discussed at all three roundtables (Riyadh, Cape Town, and Geneva), whilst benchmarking and harmonizing laws emerged from discussions held in Cape Town and Geneva.

The recommendation involves building a methodology to assess the benefits and potential limitations of accession to relevant treaties, followed by formulating a common agreed approach across the DCO Member States as to which international treaties or conventions related to IP protection, particularly in the digital space, the DCO Member States should accede to. Stakeholders will need to collaborate on writing and sharing a document setting out the agreed approach following their collaboration. Benchmarking laws would be carried out by comparing and analyzing existing laws from various jurisdictions to identify best practices and develop customized solutions to achieve the goals of the DCO Member States (for example, cross-border collaboration and innovation in the digital space). Finally, this recommendation entails harmonizing laws by establishing consistent and uniform Digital IP laws across the DCO Member States to facilitate cross-border innovation and economic growth. Together, these steps will establish a standard for IP protection (including in respect of Digital IP) across the DCO Member States' jurisdictions

Within this recommendation, the discussions in Geneva also highlighted the importance of ensuring the creation and maintenance of a fine balance between protecting Digital IP and empowering innovation (including by reducing the regulatory burden on start-ups as a result of onerous compliance with legal frameworks).

### *Action points for stakeholders*

- **The DCO:** The DCO General Secretariat can play a role in coordinating and encouraging collaboration, seeking to generate support for this recommendation across the DCO Member States.
- **Governments and IPOs:** The DCO Member States' governments and IPOs need to agree on a common regional strategy for acceding to the IP conventions and treaties, as well as to legislate for harmonized IP laws.
- **International / inter-governmental IP organizations:** Notwithstanding the above, support from the entities such as WIPO can be sought utilizing their knowledge of IP regimes in different jurisdictions, providing guidance, facilitating discussion and dialogue between governments and IPOs to negotiate and agree the above steps.
- **Legal Experts:** IP experts in each DCO Member State could undertake the benchmarking exercise, guided by government and /or IPO instructions on how to strike a balance within the strategy to reward IP creation but in a way that does not fetter ongoing collaboration and innovation.

## *Recommendation 2: Raise awareness of IP protection in the DCO Member States*

### *Summary of recommendation*

This recommendation involves the following steps:

- **Develop and agree strategies for raising awareness on Digital IP protection** across the DCO Member States.
- **Ensure the strategies and standards are socialized across the DCO Member States.**
- **Implement awareness and education campaigns.**

### *Context*

The aspects of this recommendation follow on from the first recommendation above. The DCO Member States will individually (and perhaps collectively) embark on awareness raising campaigns to ensure as many stakeholders as possible are aware of the relevant national and / or regional Digital IP strategy. The DCO Member States could share experiences of how best to raise awareness of this Digital IP strategy so that the successes of, and potential improvements to, the awareness campaign can be evaluated. The awareness campaign can be iterated accordingly over time to ensure it remains fit for purpose.

### *Action points for stakeholders*

- **The DCO:** The DCO General Secretariat will be key in facilitating discussions between the Member States about the awareness campaign. The DCO could also coordinate and bring together global and respective national legal IP experts from the DCO Member States to discuss this topic. The DCO General Secretariat can also be key in facilitating and coordinating the socialization of the awareness raising strategy by bringing governments and IPOs within its Member States together.

- **Governments:** The DCO Member States governments are probably best placed to formulate strategies on how to run effective campaigns to raise awareness about national and regional IP strategies, especially focusing on the Digital IP. Governments should draw up plans for the campaign, including budgets, timelines, media for the campaign advertisements and collaborations with other DCO Member States governments. Once campaign details are finalized, the government should make sure the campaign is run efficiently (which may involve working closely with IPOs), with clear operational accountability for implementation and delivery of its various aspects.
- **NGOs and educational institutions:** These stakeholders may be able to assist with broadening the reach of the awareness raising campaign and should also feed in key findings from their own research on what the most effective strategies may be, i.e. how best to raise awareness within certain demographics such as students of a certain age in a specific country etc. NGOs may also play a key part in reaching marginalized communities who the public sector bodies are unable to reach as this is part of their expertise.
- **IPOs:** The IPOs are generally best placed to help with delivering awareness raising campaigns and training materials (such as online portals, podcasts, videos etc.) which are aimed at assisting stakeholders to make the best possible use of their Digital IP as these activities are typically within their remit and they should have the required expertise (or ability to call upon it). IPOs should work together with national governments accordingly.

### *Recommendation 3: Develop IP Courts specializing in the Digital IP matters and Alternative Dispute Resolution (ADR) systems*

#### *Summary of recommendation*

This recommendation involves the following steps:

- **Develop specialist IP Courts with expertise on the Digital IP matters amongst other IP issues.**
- **Invest resources in training the disciplines required in specialist IP courts.**
- The **establishment of** Alternative Dispute Resolution **("ADR") systems and an emphasis on mediation,** ideally with these systems being harmonized across the DCO Member States.

#### *Context*

Countries that rank higher in terms of IP protection have specialized courts in their legal systems, both at the trial and appellate levels [38]. Some specialized courts have jurisdiction over specific types of IP issues, (such as patent disputes, the validity of IP rights etc.) and some serve as trial courts, whilst others function as appellate bodies with the authority to review cases on appeal and overturn decisions made by lower courts. The advantages of having specialized IP courts include enhancing the quality of justice available to IP rightsholders and enabling these courts to effectively keep up with and adapt to the dynamic developments in IP law.

There should ideally be universal access to IP courts, with a simple and proportionate approach to the costs associated with resolving IP disputes. This could be achieved by establishing a small claims court (similar to the Intellectual Property Enterprise Court [39] in the UK) for certain types of IP disputes, meant to be resolved within a set period of time and without full trials. Additionally, it is important to ensure that there are enough judges and other legal professionals with the required IP expertise, understanding of the Digital IP nuances, and experience to preside over such courts. However, there may also be a need to streamline the judicial system for more complex IP disputes to ensure that the cost is not an initial barrier to seeking justice for IP infringement.

As well as an education system which can produce eminent lawyers, judges and other academics in the legal field (which will need to be funded, whether through public or private means), an IP ecosystem which enables specialized IP courts, cognizant with today's Digital IP implications, to function as intended will also require (i) an IPO staffed with technical specialists, and (ii) channels of communication encouraging the sharing of knowledge with IP courts in other jurisdictions. Technical specialists need to understand the Digital IP aspects of technologies being registered / disputed so that they can provide expert guidance in the first instance to other stakeholders on fundamental aspects of the IP courts system without requiring those stakeholders to contact the IP courts themselves. Communication with other IP courts is important to ensure that good ideas and practices are proliferated whilst anything which does not work can be improved or removed from the IP court system.

In situations involving IP disputes, resorting to court action is not the sole solution. ADR systems have gained increasing importance over time, not only due to the drawbacks of litigation – which range from uncertain outcomes to time and cost implications – but also because of the flexibility, generally lower costs, confidentiality, and the expertise of those involved in ADR. Therefore, ADR processes have gained widespread popularity with recent legislation, especially within the EU, encouraging the use of ADR (for example, the 2019 EU copyright directive [40] mandates EU countries to include a voluntary ADR procedure in their laws and the EU Trademark Regulation [41] (Regulation EU 2017/1001) promotes ADR for conflicts involving EU Trade Marks (EUTMs) and designs). In addition, the European Union Intellectual Property Office (EUIPO) has been tasked with establishing a Mediation Centre [42]. Including ADR within the scope of the specialized IP court system seems to be a way of ensuring the approach to dispute resolution will be up to date and in line with developments in other parts of the world, which is a key consideration for confidence in enforcement of Digital IP.

***Action points for stakeholders***

- **The DCO:** The DCO General Secretariat, in collaboration with other specialized international organizations could play a role in facilitating discussions between the DCO Member States in relation to the establishment of specialized IP courts focused on the Digital IP issues (which include ADR systems) and harmonized approaches to training the expertise required in the court, IPOs, legal education systems etc. In particular, the DCO could convene meetings and / or other forms of collaboration between stakeholder groups (including legal and IP professionals, government legislators, IPOs, industry bodies and rights / creators' groups) so that the parameters for how specialist IP courts should operate within the DCO Member States can be agreed, ideally resulting in agreed common features for a harmonized approach.

- **Governments:** Once parameters for the operation of IP courts have been agreed, it is the responsibility of the respective national governments of the DCO Member States (working closely with their IPO) to implement IP courts in their jurisdiction. The governments would also be responsible for deciding how to invest resources to establish the other elements of the IP court system, including funding for training of Court / IPO staff and investment in legal education for future IP experts.
- **Legal IP experts:** These stakeholders will be using the IP courts and largely operating its functions, so they will play a key role in the success of the IP courts, as well as in the development and use of ADR mechanisms. Legal experts will have experience of how disputes arise and are resolved (both with positive and negative experiences for clients and IP practitioners) so their participation in delivering an effective suite of ADR mechanisms is crucial. To the extent the legal IP experts already have information which may be helpful in developing ADR mechanisms, this should be shared with governments and IPOs along with other insight on what to prioritize in ADR based on experiences to date.
- **IPOs:** Once parameters for operation of IP courts and ADR mechanisms have been agreed, IPOs will need to work with the national governments of the DCO Member States to (i) implement IP courts and ADR mechanisms in their jurisdiction and (ii) spread awareness of their existence and remit(s). IPOs will also need to develop training for their staff on the new IP court and ADR systems.
- **Creators, consumers, businesses, SMEs, Online Platforms:** Representative bodies for each of these stakeholder groups (who are likely to use IP courts and ADR for IP disputes) should submit documented evidence and insights on their experiences in using the existing court systems within a DCO Member State to resolve IP disputes (including those relating to Digital IP) and what changes would improve the courts and dispute resolution mechanisms to persuade their respective groups to use them more. In particular, the submissions from these representative groups should include (i) considerations on what challenges the current position poses for resolution of the Digital IP disputes within their demographic for the relevant DCO Member States, (ii) which of these challenges could be solved or improved through the proposed specialized IP courts and ADR mechanisms, and (iii) what challenges would not be addressed by the proposed specialized IP courts and ADR mechanisms.

## *Recommendation 4: AI regulation*

### *Summary of recommendation*

This recommendation involves the following steps:

- Developing a **strategy with guidelines on the regulation of AI development and use.**

### *Context*

As previously mentioned, the impact of emerging technologies, including AI, significantly affects Digital IP rights. We have provided examples from Europe, the United States, and China in **Appendix B** as to how AI is being regulated in those territories. Despite the different approaches, there is a common thread: seeking regulation, starting with guidelines or recommendations for use of AI that place humans at the center of these developments

The main conclusion from the discussions held at the Riyadh roundtable in September 2023 was that a strategy on guidelines for use of AI should be developed, with the relevant stakeholders who would be impacted by the guidelines (including governments, international organizations, businesses, corporations, SMEs, big technology companies and Online Platforms) and need to be involved in the development process. Stakeholders' input would feed into the planned strategic guidelines, and these would be circulated and iterated over time to reach an agreed initial set of AI guidelines. These guidelines will probably be broad enough to address various issues in the context of AI regulation, but eventually these will develop in enough detail to also include elements of regulation for use of AI in relation to IP rights (including Digital IP rights) in the future.

The key focus of stakeholder input will be on the risks associated with use of AI, in particular the identification of (i) areas where AI may be deployed without significant risks (where AI innovation can continue without the need for very stringent guidelines) and (ii) areas where the risks are significant enough to warrant a more cautious approach. Ideally these risk assessments would be shared and agreed upon amongst the DCO Member States to enable further collaboration and development of AI technology to benefit them and the DCO.

### *Action points for stakeholders*

- **The DCO:** The DCO General Secretariate could provide the Member States with robust policy tools which could provide actionable guidelines to govern the development, deployment, and use of AI systems, with a focus on embedding ethics in AI by design. The DCO plays a role in facilitating discussions between the Member States in relation to the development of AI strategy and sharing / collating relevant information on a regional level to assess how proposed guidelines may help / hinder relevant DCO Member States.
- **Governments:** The DCO Member States' governments should develop national strategies for regulation of AI. To do so, they should establish an action plan and timeline so that the strategy can consider what is happening around AI regulation in other parts of the world as well as what specific challenges need to be met in the relevant DCO Member States or region(s). Specifically, the governments should convene meetings of interested stakeholder groups (consumers, creators, companies, SMEs, Online Platforms, educational institutions, NGOs, IPOs, legal experts), asking the questions and collating

the responses to ensure views from across the stakeholder spectrum on the benefits and risks of AI regulation are considered. Governments will ultimately be responsible for producing guidelines / rules on use of AI following this process.

- **Legal experts:** These stakeholders will be needed to work closely with the government on the risk assessments and development of guidelines following collection of information from the various stakeholders by the government. This is because the guidelines and any potential new regulations or amendments to existing regulation and / or industry practice (such as codes for use of AI in specific fields etc.) need to consider the legal consequences stemming from misuse of AI.
- **IPOs:** IPOs will need to assist their national governments in collating evidence and conducting the risk assessment (especially regarding IP) for uses of AI prior to deciding how to regulate.
- **International / inter-governmental IP organizations:** These stakeholders, such as WIPO, can support by providing their knowledge of AI regulatory regimes in different jurisdictions, providing guidance, facilitating discussions and diplomatic dialogue between governments to enable collaboration on harmonizing aspects of AI regulation within the DCO Member States.
- **Online Platforms, creators, consumers, businesses, and SMEs (especially in the technology space):** Each of these stakeholder groups will be impacted by the decisions on how to regulate AI within the DCO Member States. Each of these representative groups should therefore prepare and share with national governments documented evidence to support its views on (i) areas where AI use should be regulated more stringently and (ii) areas where such regulation should be more light-touch; in each case with the overarching aim of encouraging innovation and investment in the digital economy whilst providing a satisfactory level of regulatory oversight.

## *Recommendation 5: Promote adoption of Digital Rights Management (DRM) technologies*

### *Summary of recommendation*

This recommendation involves the following steps:

- **Promote the adoption of DRM technologies** to protect Digital IP and prevent unauthorized access, distribution, and reproduction of copyrighted materials.
- **Strike a balance so that DRM does not stifle creativity and innovation within the digital economy.**

### *Context*

DRM systems offer several advantages for content creators, distributors, and consumers in the Digital IP landscape. These technologies encrypt digital content, thus preventing unauthorized access, copying, or distribution and safeguarding Digital IP to ensure it is not used without permission. DRM also enables the enforcement of copyright laws by controlling how digital content is used, restricting actions like copying, printing, or sharing, and ensuring that only authorized users can access the content. Additionally, DRM facilitates secure distribution and monetization of Digital IP, helping content owners generate revenue through sales, rentals, or subscriptions.

The implementation of DRM technologies to protect the rights of creators should be balanced against permitted uses of works protected by IP rights, including through exceptions such as fair use (see below), so that other creators and innovators who wish to use works protected by IP rights in ways which are permitted are able to do so without an onerous administrative or financial burden. If this burden is too great, then the adoption of DRM may risk stifling creativity and innovation within the DCO Member States.

The views of relevant stakeholders (including consumers, creators, any companies who publish content online, Online Platforms, legal experts, international organizations, and IPOs) should be sought by the government of each DCO Member States in response to a consultation on how DRM works and how it could be improved. The consultation should seek to understand what improvements each stakeholder would most want to see manifested in a new DRM approach which would boost use of Digital IP and economic growth.

### *Action points for stakeholders*

- **The DCO:** the DCO General Secretariat could facilitate discussion amongst stakeholders within a Member States, as well as across the DCO Member States, to ensure that there is as broad a representation of views as possible on what would constitute effective DRM measures to grow the digital economy.
- **Governments and IPOs:** The governments of the respective DCO Member States would be responsible for assessing responses from stakeholders and deciding on how to approach DRM, with IPOs supporting based on their experiences dealing with infringement issues to date. Once an approach is decided upon, there could be an awareness campaign run by government in conjunction with creators, consumer and business representative organizations, IPOs and Online Platforms to get the positive message about DRM protecting

creators and fostering innovation in front of as many people as possible. If DRM needs to be enshrined in any legislation or regulation (for example to stipulate that efforts to circumvent DRM will constitute infringement of copyright, or to establish situations in which DRM can be circumvented for certain types of use which are permitted on policy grounds) then the governments will need to consider where to add such additional measures in conjunction with legal IP experts before drafting the amendments.

- **Online Platforms:** To the extent DRM can run online, these stakeholders will need to agree to adopt those measures and practices as required to monitor and ideally report infringing use. This may require agreements to behave in this manner between Online Platforms and creators themselves and / or the representative bodies for creators in relation to certain Digital IP rights.
- **Legal experts:** Expert support from IP and technology law specialists will be needed to advise on appropriate changes to the legal landscape to ensure DRM technology strikes a balance between effective protection of IP rights and enabling innovation. Legal experts will also assist national government legislators and policy departments to draft any required legislation to enshrine the new standard of DRM protection in law.
- **Creators and companies who publish content online:** As the main aim is a DRM system which encourages creativity whilst protecting IP rights, it is crucial to involve creators and businesses who publish Digital IP content in the consultation process to ensure their views are documented and considered. Relevant representative organizations should approach the government with their prepared evidence and insights to ensure they are captured as part of this exercise.
- **Consumers and international organizations:** Each of these stakeholder groups should prepare and share with government documented evidence to support its views on how best to deploy and improve DRM technology to stimulate innovation whilst still protecting IP rights.

## *Recommendation 6: Data rights*

### *Summary of recommendation*

This recommendation involves the following steps:

- **The DCO Member States should consider how best to approach data rights.**

### *Context*

As set out in the policy paper, data usage is a key part of technological development as all emerging technologies rely heavily on the power and value of data. The DCO Member States should consider how best to protect rights in data, striking a balance between encouraging technological advancement and innovation on the one hand, and enabling businesses to protect the investment made by them in accumulating the valuable data that they hold, on the other.

The DCO Member States should individually, and on a collective basis, consider what features should be present in an optimized data rights system to encourage growth of the digital economy. Part of this consideration should include the question of how data rights would be best protected as IP, whether under existing IP rights frameworks or by implementing a dedicated data right and associated policies for licensing and sharing the data which makes it easy to use and share for collaboration.

For example, this could include:

- a framework setting out standardized data formats.
- easy methods for data holders to opt-in or out of certain uses.
- an easy system to monitor data use and ensure rightsholders get paid accordingly.
- transparency of reporting and where data goes and how it is used etc.

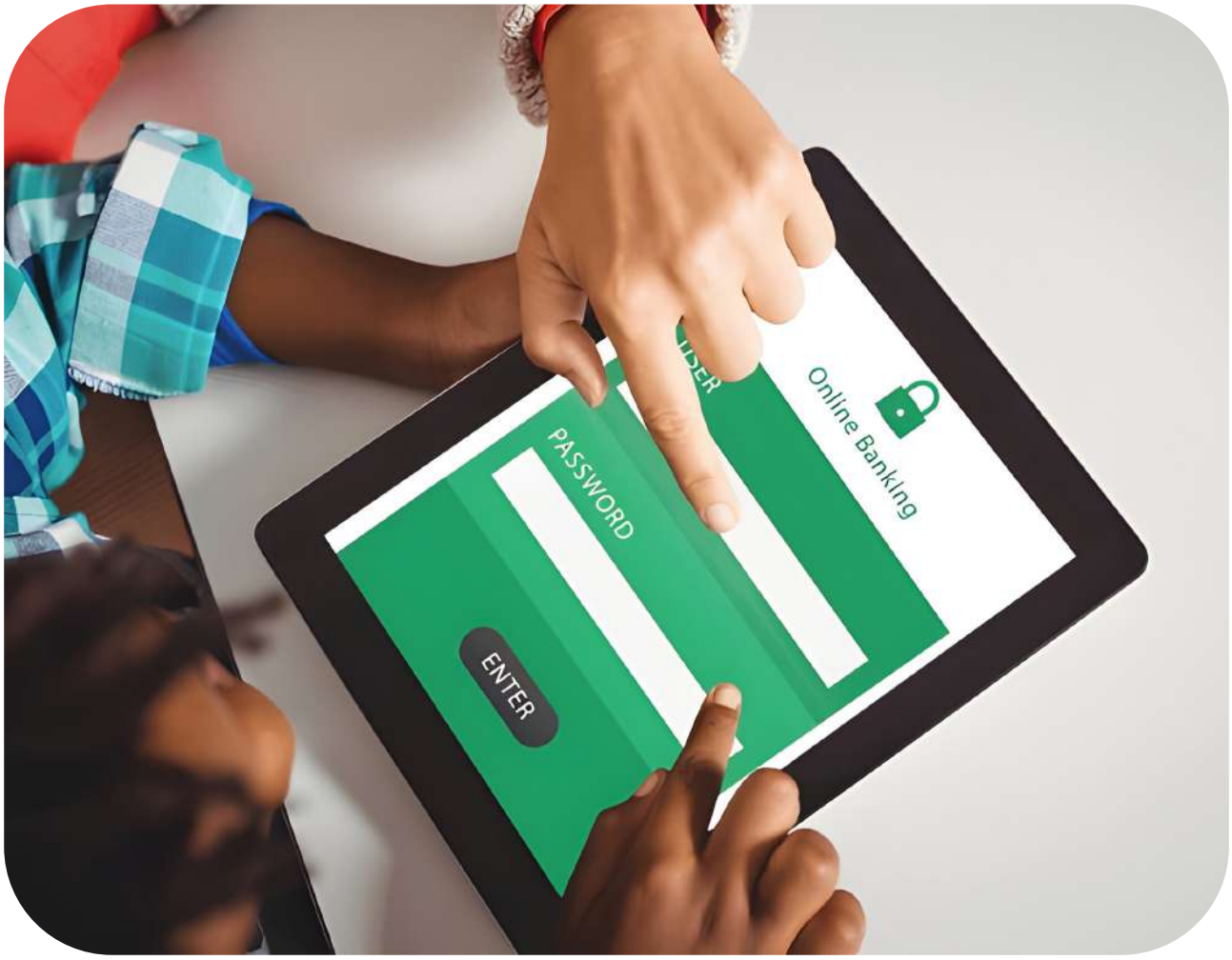
This type of approach could enable more open development of technology, especially in certain sectors where access to industry data can be a barrier for less established stakeholders (such as financial services and healthcare).

### *Action points for stakeholders*

- **Governments:** Input from various stakeholders (consumers, businesses, academics, SMEs, Online Platforms, legal experts, international groups, IPOs and NGOs) will need to be collated by the government of each DCO Member States in order to decide (i) on the features of an ideal data rights system which would foster innovation whilst still protecting valuable rights in data, and (ii) what aspects of the current IP system may work for data and what may be best addressed through a new dedicated data right.

  Once evidence is gathered and opinions have been sought by government from stakeholders (consumers, creators, businesses, and online platforms) on how best to implement the features identified as necessary for an effective data rights system, it will be for government to decide what approach to follow and draft and publish a data rights policy and associated laws/regulations accordingly.

- **IPOs:** The IPOs in each DCO Member State will need to work with their national government legislators to draft the new data rights policy guidance and any associated legislative documentation.
- **Legal experts:** Expert support from IP and data law specialists will be needed by government legislators and policy departments to draft the required guidelines / policies / regulations / legislative amendments following the government consultations.
- **DCO:** The DCO General Secretariat could facilitate discussion amongst stakeholders and collaboration amongst Member States on a harmonized approach to data rights and Digital IP, as well as support the Member State governments individually to establish their data protection approaches.
- **Consumers, businesses, academics, SMEs, Online Platforms, international groups and NGOs:** Each of these stakeholder groups should prepare and share with the respective DCO Member States' governments its documented evidence to support its views on what (if any) changes to the data rights regime in their DCO Member States would be effective in stimulating innovation whilst still protecting rights in data. In particular, these representative groups should (i) include considerations on what challenges the current position poses for innovation and protection of data rights within their demographic for the relevant DCO Member States, (ii) what proposed changes to the ways in which data rights may be protected would solve these challenges, and (iii) what current benefits of the existing position they would want to preserve in light of any further changes.



## *Recommendation 7: Technology / software patents*

### *Summary of recommendation*

This recommendation involves the following steps:

- The DCO Member States should **investigate** whether facilitating software patentability would promote innovation in their economy.

### *Context*

We set out in the policy paper how (i) a patent provides the patent owner with a monopoly right in return for disclosure about how their invention works, and (ii) that software patents are available in some countries where software produces a technical effect in order to solve a technical problem.

The key question is what would make it easier to protect new technological inventions and encourage further innovation to boost the digital economy in the DCO Member States – maintaining the current position with little or no protection for software patents, protecting software which has a unique technical effect, broadening situations in which software patents may be available, or instead creating a new IP right (one which is easier and cheaper to obtain than a patent and also perhaps does not grant a monopoly right or last as long as a patent, and allows for use of GenAI in its inventive process)?

The question should be researched by key stakeholders including creators, businesses, IPOs, legal experts, the government, Online Platforms, and other innovative technology companies. The DCO Member States can then make decisions on how to best protect rights in technology based on the evidence gathered.

### *Action points for stakeholders*

- **Governments:** Input from various stakeholders (creators, businesses, academics, SMEs, Online Platforms, legal experts, IPOs, and NGOs) will need to be collated by the government of each DCO Member State in order to decide on how best to protect rights in technology whilst also incentivizing innovation.

  Once input is gathered, it will be for each government to decide what approach to follow and to draft and publish proposed amendments to existing patent laws or creation of new rights in software-based inventions.

- **IPOs:** IPOs could assist governments in the above steps.

- **Legal experts / academics:** Expert support from IP and technology law specialists will be needed to advise on appropriate changes to patent law, as well as to assist government legislators and policy departments to draft the proposed amendments to patent legislation.

- **Creators:** As one of the key points to address is whether software patents stimulate creativity, it is crucial to involve inventors and creators in the consultation process to ensure their views are documented and considered. Relevant representative organizations should be identified and communicated with by the government / IPOs accordingly to capture this valuable insight.

- **DCO:** The DCO General Secretariat could facilitate discussion amongst stakeholders and collaboration amongst Member States on a harmonized position to technology / software patents and support the Member States governments to establish possible individual approaches.
- **Online Platforms / big technology businesses:** Each of these stakeholder groups should prepare and share with the government their views on software patents. These representative groups should (i) include considerations on what challenges the current position poses for innovation and protection of software within their demographic for the relevant DCO Member States, (ii) what proposed changes to the ways in which software innovations may be protected would solve these challenges, and (iii) what current benefits of the existing position they would want to preserve in light of any further changes.

### *Recommendation 8: Design data privacy regulations that cooperate with international standards whilst fostering innovation*

#### *Summary of recommendation*

This recommendation involves the following steps:

- Design **data privacy regulations and compliance programs** which have the same or similar standards to other data privacy regimes (e.g. GDPR).
- **Harmonize with international standards of data privacy protection.**

#### *Context*

The policy paper has already referred to the increased importance of data privacy rights in the context of technological innovation, particularly since the advent of the GDPR. Individuals are becoming increasingly aware of their rights and empowered to actively prefer technologies which respect their privacy rights.

A consistent approach to data privacy should be attractive to technology stakeholders wishing to use data processing services from within the DCO Member States, as uncertainty on the legality of processing in a certain jurisdiction can be very disruptive – for example, the uncertainty surrounding the lawful methods by which personal data may be transferred from the EU and the UK to the USA caused much consternation amongst stakeholders who had to be prepared for the transfer method to change (as it has done on numerous occasions) and to manage the potential impact on their operations.

Alternatively, the DCO Member States may choose to have lower compliance standards (either across the board or to relax them only in relation to certain types of personal data processing / specific sectors...etc.) to attract innovators who wish to experiment with technologies in ways that may normally fall foul of more restrictive data privacy regulations.

There will need to be evidence gathering and research to inform the policy decision on whether to be consistent with international privacy standards or to deviate in certain aspects to attract innovation and investment. The input from educational institutions, the DCO Member States, and regional registries tasked with regulating data privacy issues (the equivalent of the Information Commissioner's Office in the UK for example) as well as consultations with consumers, businesses and Online Platforms should be sought.

Whatever approach is ultimately pursued by each DCO Member States, the advantage of having similar standards and approaches to other jurisdictions and regions is that it will be easier for most data processing systems used by stakeholders in the digital economy to interact without fear of breaching compliance obligations (for example in terms of e-commerce, sharing individual records for staff / students / patients, relocation services...etc.). These advantages are only further enhanced by harmonizing data privacy laws with other jurisdictions, which can help support the international scaling capability of technologies (making it easier to work with personal data in relation to emerging technologies across borders) whilst allowing the DCO Member States to be compliant with international standards of privacy regulation.

By contrast, in areas where innovation may be perceived to be impeded by onerous data privacy obligations, it may be advantageous to promote a different standard of privacy rights in order to attract innovation and investment. The risk of this approach is falling out of step with other jurisdictions, which may make it more difficult to work globally using personal data.

*Action points for stakeholders*

- **Governments:** The DCO Member States should seek views from stakeholders as set out above through a consultation process. Once views have been provided, government legislators will need to draft the required new regulations and other documentation, working closely with legal experts and IPOs to do so.
- **Legal experts:** Privacy and digital IP experts will be key in expounding views on what may best achieve the goals of this recommendation, as well as working closely with government legislators on drafting new privacy regulations.
- **The DCO:** The DCO General Secretariat could facilitate discussions amongst stakeholders and cooperation amongst Member States on a harmonized approach to data privacy rights once the governments have established their approach as above. The General Secretariat could develop standardized privacy principles for its Member States to form basis of a harmonized data privacy framework amongst them.
- **Online platforms, consumers, businesses and educational institutions:** These stakeholders have a large part to play in providing evidence in response to the government consultation to support their insights on how data privacy regulation should be harmonized with and / or deviate from other standards (such as GDPR). Each of these stakeholder groups should be encouraged to document what changes to data privacy regulation would enable innovation to flourish within the relevant DCO Member States or region whilst still providing a desired level of privacy protection, as this will be very useful when the new legislation and associated documentation are prepared.
- **Regulatory bodies:** As well as feeding into the consultation run by government, the regulatory bodies with the responsibility of regulating use of personal data within each DCO Member State need to be familiar with the details of the approach which their respective governments decide to adopt, the ways in which it accords with, and deviates from, data privacy regulations in other jurisdictions and regions. They will also need to prepare guidance for individual data subjects and organizations (both data processors and data controllers) who will need assistance in knowing what their rights and obligations under the new data privacy regime are. The regulatory bodies should also consider whether forming a supranational governance body would be helpful, both in terms of sharing best practices and emerging knowledge and to liaise more effectively with other regional data privacy governance bodies (such as the European Data Protection Board) [43].

## *Recommendation 9: Incorporate fair / use dealing into copyright law **

### *Summary of recommendation*

This recommendation involves the following steps:

- **Assessment of fair / use dealing.**
- **Implementation of desired copyright exceptions.**

### *Context*

The DCO Member States should consider and implement permitted use exceptions into copyright frameworks so that innovation may continue to thrive within the digital economy without depriving copyright creators of compensation and incentives to create.

This will require evidence to be gathered and communicated to demonstrate that the benefits associated with the exceptions would be applicable in the relevant Member State, possibly through economic research commissioned by government and / or IPOs. There would also need to be a consultation to understand potential impacts / benefits from creator, consumer, business and Online Platform points of view.

Once evidence and feedback has been gathered, the DCO Member States should decide how to implement the required changes into law, for example by drafting new legislation or amending existing laws. Once this decision is taken it will be for the DCO Member States to draft the exceptions into law accordingly.

### *Action points for stakeholders*

- **Governments:** Governments should seek views from expert stakeholders (academics, legal experts, IPOs) as well as business and consumer groups (including consumers, creators, businesses, SMEs and Online Platforms) on the potential impacts of implementation of these exceptions. Once views from stakeholder groups have been canvassed, Governments will need to work with IPOs and legal experts to decide to what extent they should implement fair use / fair dealing into copyright law. Once this has been decided, Governments will need to introduce amendments to copyright law in order to effect the agreed changes.
- **Legal experts:** Legal IP experts will be key in providing views on what may best achieve the goals of this recommendation, as well as working closely with government legislators on drafting new copyright exceptions into law.
- **The DCO:** The DCO General Secretariat could facilitate discussion amongst stakeholders and cooperation amongst Member States on a harmonized approach to copyright exceptions once the governments have established their approach as above.
- **IPOs, NGOs and academic representatives from higher education institutions:** Each of these expert stakeholder groups should provide its views to governments as part of the evidence-gathering process. These views should include evidence to support conclusions as well as insight on the benefits which the exceptions could bring (including any required conditions to maximize these benefits) and any potential negative impacts of adopting the exceptions to the digital economy within the relevant DCO Member States.

* See pages 17-19 for the distinction between the two concepts.

- **Consumers, creators, businesses, SMEs and Online Platforms:** Each of these stakeholder groups should participate in the consultation process and share evidence to support its views on how proposed amendments to the copyright exceptions will impact it. The evidence gathered should include considerations of how best these exceptions may be implemented to boost innovation and use of Digital IP within the respective stakeholder group.

# 7

# CONCLUSION

# CONCLUSION

An effective Digital IP landscape is fundamental to achieving a prosperous and thriving digital economy and should be a priority for the DCO Member States.

The research conducted over the past few months, as well as the roundtables that took place, have led to the conclusion that improvements to existing laws should be made, along with the reinforcement of international and institutional cooperation. This will enable the building of a suitable landscape and ecosystem within the DCO Member States and regions for Digital IP to flourish and for new technologies to meet its economic, cultural and societal potential.

Emerging technologies, particularly AI, have been identified as one of the key challenges for Digital IP management. This conclusion was drawn from surveys distributed to participants in the roundtables the DCO conducted which overwhelmingly indicated the urgent need to pay greater attention to this technology and to build the necessary foundations for increased regulation of its use, considering the impact it has on copyright and other forms of Digital IP.

This policy paper also highlights the importance of involving various stakeholders in discussions around approaches to Digital IP protection. International organizations, creators, businesses and corporations, governments and public entities, IP offices, legal and IP professionals, ISPs and Online Platforms, citizens, NGOs, and educational institutions and research units should all be part of the response to the challenges identified in this paper.

Significant gaps remain in the legislative and regulatory frameworks of the DCO Member States. The aim of the policy recommendations set out in Section VI above is to contribute to greater promotion and protection of Digital IP rights in the DCO Member States, safeguarding their differences whilst fostering an environment which supports acceleration towards a more prosperous digital economy.

# APPENDIX A

## Copyright - Background

### *Idea and Expression Dichotomy*

The basic overarching principle of copyright is that it does not protect ideas or concepts in and of themselves, no matter how creative or original. Instead, it protects the creative expressions of those ideas, which need to be recorded or fixed in some way e.g. written down or recorded in some medium. So, for example, copyright would not protect the idea of a story featuring a group of people scaling a mountain together, but it could protect a book, manuscript, or screenplay which has been written and which includes this as part of its plot.

This concept is fundamental to copyright and is sometimes referred to as the "idea / expression dichotomy". It has been cited in cases where claimants have tried to claim copyright in ideas which they may not have expressed in any meaningful form, such as ideas for elements of literary plots or musical melodies.

### *Historically Identified Copyright Categories*

It is commonly accepted in most jurisdictions worldwide that copyright protection subsists in specific categories of copyright works. By the 1980s, the main types of copyright work seemed settled, having been shaped further by the technological developments of the preceding decades:

- Literary works (such as books, software, and databases);
- Dramatic works (including dance and mime);
- Musical works (distinguished from words or motions set to music);
- Artistic works, such as paintings, sculptures, and photographs;
- Sound recordings;
- Films.

Further technological developments mean there are now new types of work to consider.

### *Authorship and Exclusive Rights*

The author of a copyright work is the person who creates it. The author (or the owner of a copyright work if the ownership has been transferred from the author) has the exclusive right to prevent others from doing certain things in relation to their work, such as:

- Reproducing the work
- Distributing copies of the work to the public
- Communicating copies of the work electronically to the public
- Adapting the work.

Although many jurisdictions do not have a copyright register, it is important to know who the author or owner of a work is as unauthorized use may infringe their copyright.

***Duration of Protection***

Copyright duration is usually measured as the life of the author plus a set number of years depending on the type of copyright work. There is a tension between the protection of authors and the duration of the copyright term for works, as it can be argued that too long a term stifles innovation by preventing usage of copyright works – for example, the estates of deceased artists who have ongoing copyright in the works of the artist may refuse to allow usage of works for training image generation AI models.

Although copyright law has been stretched to accommodate computer programs in the form of software, the pace of technological development may mean that existing copyright durations for software as a literary work no longer align with the rationale for protection, i.e. that it rewards the creativity of the author without impacting innovation. As software code can be written and deployed quickly and at scale, does it make sense to protect it in the same way as a book which can take an author years to write?

***How can the existing legal copyright framework incorporate emerging technologies?***

To ensure the continued development of innovative technologies and other creative works which benefit society, it is worth considering how the existing legal framework for copyright could be adapted to enhance the protection of Digital IP in emerging technologies. For example, should technological works be protected as literary copyright works just because they are underpinned by software? Would it make for a better copyright framework if certain types of work were protected differently on their own terms, for example:

- software as a standalone copyright work (not a form of literary work);
- data created from ongoing monitoring and reporting and / or combined with other data sources protected as its own data right (instead of via a collection of various rights that vary by jurisdiction including literary copyright in the selection and arrangement of a database, sui generis database rights which protect the contents of a database, confidential information etc.);
- works created using GenAI having specific standalone protection.

GenAI poses many questions about how the existing copyright framework may be changed and arguably improved. Unless all materials used in training data for a GenAI model have been licensed, there is a risk that the training of the GenAI model may infringe copyright or breach relevant contractual terms, especially if the training data has been scraped from the internet or otherwise collated indiscriminately. Also, most jurisdictions do not currently grant copyright protection to works which have been created solely by GenAI, even though some of the musical, artistic and literary outputs from GenAI models are comparable to what humans can create. These issues raise the following questions:

- Should there be an exemption allowing the use of certain types of copyright / data works to train GenAI models? How could this be balanced against the rights of the copyright / data owners?
- If there were a specific copyright-type regime in place for the protection and use of such GenAI works, would it foster creativity by giving people the incentive to use these technological tools and create things they would not otherwise have been able to?
- Should such works have a shorter duration of protection and be more freely available for use by others without permission?

- Should there be a register of works and authors/owners and the prompts used to generate certain works (and a record of the datasets used to train the relevant GenAI models)?

Spatial technologies engage copyright in several ways, starting with the software code that underpins the technology. The key considerations are how to treat the Digital IP used within the technology, for example the user-generated content that may be created and shared within a metaverse platform, the branded goods which may be advertised therein and the music, films, video games and literary and artistic works which may be created and / or uploaded and shared on a platform. The terms of the relevant technology platform provider usually state that users must have the right to use copyright works, and these terms may also give broad rights to the platform holder in relation to user-generated content, but could this approach be improved?

- Could the use of copyright works in the metaverse and other digital technologies be licensed collectively (in the same way music and artistic works are licensed and revenues are shared out through collective management organizations)?
- Could user-generated content be protected in its own right?
- Similarly, should there be a new approach to Digital IP in artistic works / films / books etc.?
- Does it make sense for Digital IP assets to benefit from the same protection as physical copyright works, when sharing and copying them is near-instantaneous and normally inexpensive?

## APPENDIX B

### Trends in the Digital IP Landscape

*Global*

Before delving into the detail of what measures countries have adopted to enhance their Digital IP protection regimes, it is worth mentioning the International IP Index [44]. This index creates a roadmap for economies aiming to enhance innovation and creativity through more effective IP standards by assessing them on the strength and effectiveness of their IP frameworks. The geographical coverage includes some DCO Member States such as Morocco, Jordan, Saudi Arabia, Ghana, Nigeria, Kuwait, and Pakistan (ranked in that order in latest index). Interestingly, Morocco recorded the largest improvement in its overall score at 2.5%. The countries leading this index are the United States, United Kingdom, France, Germany, Sweden, and Japan, followed by the Netherlands and Ireland.

Indeed, the **United States** has implemented various measures aimed at bolstering the protection of Digital IP. This includes legislation such as the Digital Millennium Copyright Act, which establishes guidelines for addressing online copyright infringements. Additionally, the United States is a key promoter of international agreements and treaties designed to strengthen global IP protection, such as the Anti-Counterfeiting Trade Agreement.

In 2022, the White House Office of Science and Technology Policy published a blueprint for an AI Bill of Rights (the "**Blueprint**"), which shared a non-binding roadmap for the responsible use of AI. The Blueprint outlined five fundamental principles (safe and effective systems; algorithmic discrimination protections; data privacy; notice and explanation; and human alternatives, consideration, and fallback) designed to steer and regulate the proficient advancement and deployment of AI systems, paying special attention to the inadvertent repercussions of AI on civil and human rights. The Blueprint envisages a system of self-regulation in the private sector involving, in particular the oversight and creation of products and services through a consumer rights-oriented approach. Acknowledging the need for clear public guidance, in 2023, the U.S. Copyright Office [45] issued a policy statement setting out its procedures for reviewing and registering works incorporating AI-generated content. This policy outlined:

- the human authorship requirement;
- the application of the human authorship requirement;
- guidelines for submitting U.S. copyright applications involving AI-generated content.

In the **European Union ("EU")**, the proposed EU AI Act mandates developers of AI tools to disclose the copyrighted materials they used in constructing their systems (European Commission, 2021). The EU has also implemented the Directive on Copyright in the Digital Single Market (the **"DSM Directive"**) [46], the purpose of which is to enhance the utilization of digital technologies and to facilitate cross-border access to, and use of works, ensuring the efficient functioning of the copyright market.

Under **China's** GenAI Regulation which took effect from July 2023, GenAI outputs must be tagged as AI-generated content. The Beijing Internet Court also recently issued a verdict in the country's first case addressing the copyrightability of AI-generated images. The court determined that an AI-generated picture qualifies as a copyrightable work involving human authorship. Consequently, the defendant was held liable for copyright infringement.

**Japan** has a robust IP protection and enforcement framework and holds the top spot in international rankings in this area. This framework includes the Patent Act, the Utility Model Act, the Design Act, the Trademark Act, the Copyright Act, and the Unfair Competition Prevention Act. In addition to this, there are various bodies responsible for the protection of IP rights, including the Japan Patent Office ("**JPO**"). The JPO is responsible for examining and granting patents, utility models and design rights, as well as handling copyright registration and administration. Japan is also a signatory to various IP treaties, such as the Paris Convention for the Protection of Industrial Property (the "**Paris Convention**") and the Berne Convention for the Protection of Literary and Artistic Works (the "**Berne Convention**").

When it comes to the intersection of Online Platforms and copyright issues, there are two key global players: **Canada** and **Australia**. Recently, the Canadian digital media regulator announced its intention to establish a framework for negotiations between news organizations and Online Platforms who wish to use their content, due to come into force this autumn. The goal is to implement mandatory bargaining by early 2025. Canada's Online News Act, part of a global trend aimed at requiring technology firms to pay for news, was enacted in June but has not yet been implemented. This development makes Canada the first country to follow the precedent set by Australia's News Media Bargaining Code, which requires Online Platforms to negotiate fair prices with news publishers to ensure they receive just compensation for the use of their content.

## The DCO Member States' IP initiatives

It is also worth highlighting some initiatives that have been implemented by the DCO Member States in the field of IP protection, particularly in the realm of Digital IP.

In September 2023, the Ministry of Industry and Commerce of **Bahrain** unveiled an initiative aimed at fostering innovation and protecting IP rights [47]. This included reducing the official fees for patent registration for individual applicants.

In 2023, the **Bangladesh** parliament passed the Copyright Bill 2023 with the goal of safeguarding the rights of original works in publications, film, digital media, drama, folklore, the arts, and audio recordings. This legislation supersedes the previous 'Copyright Act-2000' and is designed to uphold IP rights.

In recent years, **Cyprus** has made substantial advancements in modernizing its IP laws, aligning them with international standards. In 2019, Cyprus introduced a new Trademarks Law, replacing the outdated legislation from 1962. This new law brought Cyprus in compliance with the EU Trademark Directive, encompassing provisions for online trademark registration and the safeguarding of non-traditional trademarks.

**Djibouti** is a member of international IP treaties, such as the Paris Convention, indicating a commitment to international IP protection standards.

The Government of **The Gambia** [48] has recognized that IP serves as an effective policy tool for facilitating the transfer and use of foreign technologies and creative works and for encouraging fair competition, thereby promoting national social, cultural and economic development. In light of this, it has published its National Intellectual Property Policy & Strategy, aimed at establishing an IP system which harnesses the creative potential of Gambians while promoting sustainable, inclusive, and rapid social and economic development in order to support the transformation of the Gambian economy and the realization of its national vision.

**Ghana** is a contracting party to most international IP treaties and is a member of the African Regional Intellectual Property Organization ("**ARIPO**"), but has to align its domestic legal framework with international standards.

As part of the 2001 US-Jordan Free Trade Agreement, **Jordan** implemented DRM and Technological Protection Measures ("**TPM**") legislation. Article 55 of the Copyright Act explicitly prohibits the use, sale, manufacture, and distribution of circumvention devices (devices aimed at bypassing TPMs).

In 2019, **Kuwait** enacted a new copyright law, Law 75 on Copyright and Related Rights, introducing significant changes to the copyright regime, particularly relating to enforcement [49]. Notably, Article 36 grants designated officials broader administrative enforcement authority compared to the provisions in the previous Copyright Law. Additionally, Kuwait's National Library oversees the national copyright system and now provides rightsholders with the option to file copyright infringement complaints directly through an online portal.

**Morocco** became a member of the Hague Agreement Concerning the International Registration of Industrial Designs on March 13, 2020 (the "**Hague Agreement**"). The Hague Agreement is a global treaty that streamlines the registration process for industrial designs. By enabling creators to register their designs across multiple countries through a single application, the Hague Agreement simplifies the protection of various design elements, including an object's shape, surface, or ornamentation. It operates through a centralized system, offering a more efficient and accessible pathway for international design registration.

In 2022, **Nigeria** became a full contracting party to the Convention on Cybercrime (the "**Budapest Convention**"). The Budapest Convention fosters collaboration among nations to combat cybercrime, which frequently encompasses theft, counterfeiting, and the unauthorized distribution of Digital IP.

Since 2008, Royal Decree No. 65/2008 (the Law of Copyrights and Neighboring Rights) has been in force in **Oman** [51]. This legislation includes provisions aimed at protecting Digital IP.

**Pakistan** established IP tribunals through the Intellectual Property Organization of Pakistan Act 2012 (50). These tribunals were officially opened by the Federal Government of Pakistan in 2015, serving as specialized alternatives to the District Courts. The fundamental objective behind the creation of these IP tribunals was to establish a judicial mechanism capable of handling the technical and intricate aspects of IP laws. These tribunals were designed to ensure the swift, cost-effective, consistent, predictable, and high-quality adjudication of IP cases. Simultaneously, their establishment aimed to alleviate the litigation burden on the regular courts. The Federal Government of Pakistan also implemented new regulations under the Designs Rules in 2023.

**Qatar** has been engaging in WIPO international treaties and refining its domestic IP legal framework in an effort to create a favorable environment for attracting investment in knowledge-based sectors, in line with the Qatar National Vision 2030 [56].

In 2019, **Rwanda** organized a month-long nationwide awareness campaign focused on IP [52]. The campaign, titled "The Meaning of Intellectual Property in your Daily Life", had the primary objective of raising awareness about the importance of registering IP and the associated benefits. During this campaign, information on the advantages of protecting IP was shared, along with guidance on its commercialization and enforcement, addressing

the needs of rightsholders and innovators. In 2022, Rwanda gained recognition as one of the leading countries in the field of IP registration, securing the 3rd position in Sub-Saharan Africa and ranking 54th globally according to the International Property Rights Index [53].

Founded in 2018, the Saudi Authority for Intellectual Property ("**SAIP**") [54] oversees issues pertaining to the protection, regulation, and enforcement of intellectual property rights in **Saudi Arabia**. The SAIP's objective is to encourage local innovation and enhance the competitiveness of the national economy by assisting local businesses in strategically utilizing IP. As an autonomous IP authority with a global outlook, the SAIP is also striving to establish itself as an IP hub in the Middle East and North Africa region [55].

# BIBLIOGRAPHY


1 World Intellectual Property Organization

2 United States Patent and Trademark Office

3 European Union

4 The Way Forward for Intellectual Property Internationally, Stephen Ezell and Nigel Cory, 2019

5 The Rule of Law and IP Rights Protection: Key Factors In Attracting FDI To The US, Stefan Calimanu, 2023

6 The quest for the thinking computer, Robert Epstein, Boston University and the University of California, San Diego, 1992

7 The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life: Plus The Secrets of Enigma, B. Jack Copeland (editor), Oxford University Press, 2004

8 The Network Readiness Index 2022, Portulans Institute, 2022

9 IP in a world without scarcity, Mark. A. Lemley, 2015

10 Artificial Intelligence, Big Data and Intellectual Property: Protecting Computer-Generated Works in the United Kingdom, Ryan Abbott, 2017

11 The Role of Blockchain Technology in Intellectual Property Protection, Moroğlu Arseven, 2021

12 5G – The future of IoT, 5G Americas White Paper, 2019

13 IP Aspects of Augmented Reality and Virtual Reality Technologies, Ryan N. Phelan, Barrett Spraggins, David Pointer, and George Raynal, 2022

14 Gartner Glossary

15 Hermes vs. Mason Rothschild case, 2023

16 Study on the impact of AI on the infringement and enforcement of copyright and designs, EUIPO, 2022

17 Managing the risk of intellectual property cyber theft, Deloitte, 2017

18 Protecting your most valuable intellectual property from cyberattacks, Rose Cordero Prey, and Sandra L. Applebaum, 2021

19 https://vpnoverview.com/privacy/downloading/what-is-torrenting/

20 https://www.directives.doe.gov/terms_definitions/computer-software-piracy

21 https://goodereader.com/blog/e-book-news/how-an-e-book-is-pirated-its-implications-for-the-stakeholders-and-the-extent-of-the-problem

22 Digital Game Piracy: Analyzing the Illegal Distribution of Digital Games via BitTorrent, Anders Drachen; Rob Veitch; and Kevin Bauer, 2011

# BIBLIOGRAPHY


23 Charting Global Sports Piracy, Synamedia

24 The End of the Road for DABUS and Dr Thaler at the UK Supreme Court - Kluwer Patent Blog (kluweriplaw.com)

25 How platforms govern users' copyright-protected content: Exploring the power of private ordering and its implications, João Pedro Quintais, Giovanni De Gregorio, João Magalhães, 2023

26 https://www.wipo.int/wipo_magazine/en/2018/si/article_0006.html

27 EU – GCC Dialogue on Economic Diversification Gulf Cooperation Council (GCC) countries, European Union, 2021

28 https://bangladeshpost.net/posts/parliament-passes-copyright-bill-2023-120670

29 Digital Cyprus 2025

30 Intellectual Property Policy and Strategy of The Gambia 2018-2023

31 https://iclg.com/practice-areas/copyright-laws-and-regulations/greece

32 International Cover IP Index, U.S. Chamber of Commerce and Global Innovation Policy Center, 2023

33 Intellectual Property Rights in the Sultanate of Oman

34 https://www.newtimes.co.rw/article/6961/opinions/editorial/awareness-on-intellectual-property-could-empower-women

35 https://www.newtimes.co.rw/article/6975/news/rwanda/intellectual-property-day-what-rwanda-needs-to-do-better

36 https://www.cnbcafrica.com/media/6326619007112/

37 https://www.trade.gov/country-commercial-guides/saudi-arabia-protecting-intellectual-property

38 A closer look at specialized intellectual property courts, Jacques de Werra, 2019

39 Intellectual Property Enterprise Court - GOV.UK (www.gov.uk)

40 The 2019 EU Copyright Directive

41 The EU Trade Mark Regulation

42 Mediation Centre

43 What is the European Data Protection Board (EDPB)? - European Commission (europa.eu)

44 International Cover IP Index, U.S. Chamber of Commerce and Global Innovation Policy Center, 2023

45 Artificial Intelligence and Copyright, United States Copyright Office, 2023

46 DSM Directive

# BIBLIOGRAPHY


47 Official Gazette No. 3699, dated September 21, 2023

48 Intellectual Property Policy and Strategy of The Gambia 2018-2023

49 International Cover IP Index, U.S. Chamber of Commerce and Global Innovation Policy Center, 2023

50 Specialist IP tribunals in Pakistan, Naeema Sadaf and H. Zafar Iqbal, 2016

51 Law of Copyrights and Neighboring Rights, Oman

52 https://rdb.rw/rdb-in-nationwide-intellectual-property-awareness-campaign/

53 https://taarifa.rw/rwanda-is-3rd-top-for-intellectual-property-rights-protection-in-su-saharan-africa/

54 Saudi Authority Intellectual Property

55 Saudi Arabia gears up on IP, Yasser Al-Debassi, 2020

56 Qatar National Vision 2030

Digital Cooperation Organization

Follow us on

@dcorg | www.dco.org