JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i4

Optimizing the Implementation of Digital Rights Management to Strengthen Copyright Protection in Digital Streaming Services in Indonesia

Rifa Elvaretta Khansa[1], Tasya Safiranita[2].
[1]Faculty of Law, Universitas Padjadjaran, rifa21001@mail.unpad.ac.id.
[2]Faculty of Law, Universitas Padjadjaran, tasya.safiranita@unpad.ac.id.

Corresponding Author: rifa21001@mail.unpad.ac.id[1]

Abstract: The rapid advancement of digital technology has significantly heightened the risk of copyright infringement in streaming services, making the implementation of Digital Rights Management (DRM) an essential mechanism for protection. This study aims to analyze the effectiveness of DRM regulations in safeguarding copyrights on digital platforms in Indonesia and to propose measures to enhance their enforcement. The research employs a normative juridical approach, focusing on an in-depth examination of Indonesia's Law No. 28 of 2014 on Copyright, alongside a comparative analysis of international cybersecurity regulations, particularly in the European Union (EU) and the United States (US), where DRM frameworks are more robust and extensively enforced. The findings of this study indicate that, first, while DRM is legally recognized in Indonesian regulations, its practical implementation remains vulnerable to cyberattacks and digital piracy. The existing legal framework remains general and lacks specificity in addressing the technical complexities of DRM protection for digital content. Second, comparative insights reveal that countries with more developed cybersecurity infrastructures, such as the EU and the US, provide more comprehensive protection through detailed legal frameworks and advanced technological measures that reinforce DRM enforcement. Based on these findings, this study recommends updating Indonesia's DRM regulations, strengthening cybersecurity infrastructure by adopting international best practices, and enhancing global cooperation to combat digital piracy through cross-border networks. These measures are essential to fortifying copyright protection in Indonesia's digital streaming landscape and ensuring a secure and sustainable digital economy.

Keyword: Digital Rights Management, Copyright Protection, Streaming Services, Cybersecurity, Digital Piracy.

INTRODUCTION

Intellectual Property (IP), formerly known as Intellectual Property Rights (IPR), is the right of ownership over works resulting from human intellectual abilities in the fields of science and technology. These works are intangible objects that are born from a combination of creativity, taste, and creativity, and contain economic and moral values. In a legal perspective,

the term intellectual property is always associated with ownership of various types of objects, both movable goods, immovable goods, tangible goods, and intangible. Juridically, intellectual property rights are categorized as personal property based on human natural rights, intellectual property rights are considered equivalent to other property rights, which can be defended from claims or control of unauthorized parties (Amirulloh & Muchtar, 2016). In Indonesia, the regulation on Intellectual Property has existed since 1840, when the Dutch colonial government introduced the first law on IP protection in 1844. This was followed by the passage of the Trademark Law in 1885, the Patent Law in 1910, and the Copyright Law in 1912 (Director General of IP, 2025). The 1945 Constitution also shows its appreciation of copyright protection for the Creator's creativity, precisely in Article 28 letter c Paragraph (1) and (2). In the article, it can be seen that everyone has the right to create and obtain material and moral benefits from the results of creativity. The creation can be in the form of tangible and intangible objects (Ramli, 2022). The development of IP in Indonesia is increasing rapidly along with technological advances and its impact on national trade. This has encouraged Indonesia to become a member of the World Trade Organization (WTO) and ratify the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPs) stipulated in the Agreement Establishing the World Trade Organization. This ratification is embodied in several national regulations, and Indonesia is bound to follow WTO provisions related to IP (Andrea, Permata, & Safiranita, 2020)

In addition to TRIPs, IP is regulated through various international conventions, such as the Paris Convention for the Protection of Industrial Property and the Convention Establishing the World Intellectual Property Organization, which Indonesia ratified through Presidential Decree No. 15 of 1997. Several other conventions, including the Patent Cooperation Treaty (PCT), Trademark Law Treaty, Berne Convention for the Protection of Literary and Artistic Works, and WIPO Copyright Treaty were also ratified in the same year (Julianti & Subekti, 2018). According to the WIPO Convention, the scope of IP includes two main elements, namely Industrial Property Rights, which include patents, trademarks, and industrial designs, and Copyright, which includes literary, musical, photographic, and cinematographic works (Andrea et al., 2020). Copyright is an exclusive right granted to creators or copyright holders for works in the fields of , art, and literature. Based on Law No. 28 of 2014 on Copyright (Copyright Law), copyright automatically arises once the work is realized in tangible form. These rights include moral rights and economic rights, where the creator has full control over how his/her work is used and derives economic benefits from such utilization.

Digital streaming services are platforms that allow users to access and enjoy multimedia content, such as music, movies, videos, or live broadcasts, online without having to download the content to their devices. The content is played live over the internet, allowing users to watch or listen instantly on various devices, such as mobile phones, computers, or televisions.

In today's growing digital era, streaming services have become the main platform for the distribution of digital copyright content such as music, movies, books, and so on. With its ease of access and wide selection of content, the popularity of this service continues to increase, both in Indonesia and globally. Changes in information and communication technology have also resulted in the absence of boundaries ((Ramli, 2020)borderless) . The most popular streaming service provider platforms in the world today are in the fields of music (Spotify, Apple Music, Joox) and cinematographic works such as movies, drama series, documentaries (Netflix, Disney+, WeTV, and so on). By 2022, 66 million people in Indonesia will consume three billion hours of content from streaming services every month (Faisal, 2024). Not only are International digital streaming platforms popular in Indonesia, local streaming platforms are also growing. Some of them are iFlix, PT Vidio.com, Mola TV, and Langit Musik. These streaming platforms offer diverse content, from live sports, movies and local TV shows that are increasingly attracting the interest of Indonesians. Copyright is a very important aspect for

creators and copyright holders in protecting the exclusive rights to the works they have created (Kusno, 2017). In the case of digital streaming services, copyright serves to prevent the illegal use, reproduction, or distribution of content that may harm the copyright holder. Digital copyrighted works have various advantages over traditional works, such as easier distribution and publication (Kharisma, Hakim, & Mustafa, 2024).

However, this convenience also increases the risk of copyright infringement, such as the ease of copying content, the speed and ease of dissemination, and the ease of manipulating works (Kharisma et al., 2024). In reality, infringement is currently rampant, such as the piracy of movies uploaded to illegal streaming sites or platforms without the permission of the copyright holder, and the distribution of newly released music albums through file-sharing sites or peer-to-peer applications without compensation to artists and producers. In addition, there are also cases where excerpts of movies or television series are freely shared on social media such as Facebook, YouTube, or TikTok without a valid license, which not only infringes copyright but also reduces economic rights for content creators or copyright holders. In other words, this kind of activity harms a lot of people.

In the midst of this rampant infringement, legal protection for copyright holders has become increasingly urgent. Digital Rights Management (DRM) emerges as one of the technological solutions to address this problem by limiting access and unauthorized use of digital content. DRM or commonly called security technology is an access control technology used to protect copyright and control the use of digital content, such as music, movies, software, and other digital data. DRM allows publishers and copyright holders to regulate what can and cannot be done with a medium, including restrictions on the duplication, use, and distribution of the content (Adrian, 2009). This technology is often integrated with encryption and watermarking to prevent piracy and illegal use. In practice, DRM gives full control to the copyright owner to determine who has the right to access or use digital content, and restricts access only to authorized users (Nasution, M., & Virgono, 2016)

Some examples of DRM used in the music industry include technologies such as Apple FairPlay, which restricts songs downloaded from iTunes to only be played on certain Apple devices (Venkataramu, 2007), and Windows Media DRM, which is used by some music services to control access and usage of audio files (Wang & Shen, 2009). In the movie industry, DRM is applied through technologies such as UltraViolet and Widevine, which are used by streaming platforms such as Netflix and Amazon Prime Video to ensure that movies and television shows can only be watched by authorized users with compatible devices. , in the e-book industry, DRM technologies such as Adobe Digital Editions are used by publishers and digital booksellers to limit the number of devices that can be used to read e-books and prevent unauthorized printing or copying (Kim & Leung, 2021)

When it comes to digital streaming services, DRM plays a very important role in protecting copyright and preventing infringement of digital works. Streaming services rely on DRM to control access to copyrighted content, ensuring that only licensed users can enjoy available movies, music, or television shows. By restricting unauthorized copying, distribution, and use of content, DRM helps prevent piracy and illegal use that can harm copyright holders. Through DRM, streaming platforms can regulate content access based on subscription or purchase, giving content owners complete control over the distribution and use of their works. In light of this, it is necessary to understand how the current rules and implementation of DRM in Indonesia can ensure effective legal protection for copyright holders. While DRM offers a technological solution to prevent copyright infringement, its effectiveness is highly dependent on existing legal and regulatory support.

METHOD

This research uses a normative juridical method to evaluate the application of Digital Rights Management (DRM) in protecting copyright in digital streaming services in Indonesia.

The normative analysis method is conducted by reviewing relevant Indonesian laws and regulations, including Law No. 28 of 2014 on Copyright (Copyright Law) and other regulations related to copyright protection and the use of DRMs. This process involved inventorying and analyzing the content of these regulations to identify the strengths and weaknesses in the current legal framework. This research also compares DRM regulations in Indonesia with similar regulations implemented in other countries that have been more advanced in regulating cybersecurity and copyright protection, such as countries in the European Union and the United States. This comparison aims to provide an overview of the effectiveness of existing regulations and identify measures that can be adapted from international policies.

A literature study was also conducted to collect secondary data from online library data research, including scholarly journals, books, legal articles, and industry reports that discuss DRM and copyright protection in digital streaming services, others. In the early stages of the research, relevant sources were identified and selected through academic databases such as Google Scholar, JSTOR, ResearchGate and so on. After the search process was completed, selection and analysis were carried out to obtain study references that were in line with the focus of this research.

The results of this desk research are combined with normative analysis to provide a comprehensive theoretical view of DRM implementation and the legal framework in Indonesia. This method allows the research to conduct an in-depth analysis of the effectiveness of DRM regulations and provide practical recommendations to strengthen copyright protection policies in the digital era. With this approach, it is hoped that this research can make a significant contribution to understanding and addressing the challenges faced by copyright holders in protecting their works in the evolving era of digital streaming services. The research method is designed to provide a comprehensive overview of DRM implementation and its regulatory effectiveness in protecting copyright in Indonesia, as well as to explore possible improvements in the existing regulations.

RESULTS AND DISCUSSION

The Effectiveness of Legal Regulations in Indonesia related to Digital Rights Management (DRM) in Providing Preventive and Repressive Protection for Copyright Holders against Infringement of Rights on Digital Platforms

In Indonesia, Copyright is specifically regulated in Law Number 28 of 2014 (Copyright Law), but there are also supporting regulations related to Copyright such as Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Government Regulation Number 56 of 2021 concerning Management of Royalties for Copyright of Songs and/or Music, and others. Copyright is the exclusive right of the creator that arises automatically based on the declarative principle after a work is realized in a tangible form without reducing restrictions in accordance with the provisions of laws and regulations (Government of Indonesia, 2014a). The meaning of exclusive rights in this case includes the ability to duplicate a work or give permission to other parties to do the same, in accordance with applicable legal provisions. The Copyright Holder is the Creator as the owner of the Copyright, the party who receives the right legally from the Creator, or other parties who receive further rights from the party who receives the right legally (Government of Indonesia, 2014a). Copyright holders have full authority to exploit their creations, including the right to authorize or prohibit the use, distribution, or reproduction of their works by other parties.

The exclusive authority and rights in Copyright include Moral Rights and Economic Rights, where moral rights are rights that are permanently attached to the creator and cannot be eliminated, even though copyright has been transferred to other parties through various legal means (Daud, 2024). These rights include the right to include or not include the creator's name, use aliases, change the work according to norms, change the title, and protect the work from

distortion or acts that damage reputation. This moral right cannot be transferred while the creator is still alive, but its implementation can be transferred after the creator dies through a will or other legal means (Government of Indonesia, 2014b). Meanwhile, economic rights are rights owned by creators or copyright holders to obtain economic benefits from their creations, both through personal use and use by other parties based on license agreements. This right covers various forms of commercial utilization, such as publishing, duplicating, translating, adapting, arranging, distributing, performing, announcing, communicating, and renting the work (GoI, 2014c). Copyright holders who are not creators do not have all the full exclusive rights, but are only entitled to economic rights. Nonetheless, these economic rights still provide significant protection, as they allow the copyright holder to commercially exploit the work, such as through publishing, duplicating, distributing, and licensing to third parties (Mulyani, Lestari, W, & Tedjosaputro, 2024).

The creations protected by the Copyright Act as stated in Article 40, include a variety of works in the fields of , art, and literature. These works include books, pamphlets, lectures, teaching aids, songs and music, dramas, fine arts such as paintings and sculptures, architectural works, maps, batik art, photography, cinematographic works, translations, adaptations, data compilations, video games, and computer programs (Government of Indonesia, 2014d). From this explanation, Copyright is closely related to cybersecurity, especially in the protection of digital content in the era of rapidly developing information technology. With the increasing distribution and accessibility of copyrighted works through digital platforms, the risk of copyright infringement also increases, including through piracy and dissemination of illegal content. Cybersecurity plays an important role in protecting copyright by ensuring that digital works, such as music, movies, software, and written works, are not copied, accessed, or distributed unlawfully. Cybersecurity technologies, such as encryption, firewalls, and intrusion detection systems, can be used to protect servers and databases that store copyrighted content from unauthorized access and cyberattacks.

All States, including Indonesia, have an obligation to protect copyrighted works, especially those that are digital-based, through effective legal enforcement and protection against copyright infringement. The presence of digital technology does not mean that all existing laws must be drastically changed. Instead, the rule of law must be adjusted and applied appropriately to ensure that technological advances do not undermine the basic principles of Copyright (Irawati, 2019). Departing from this, experts in the fields of internet technology and law continue to try to offer various solutions to overcome legal problems that arise in this digital era. In an effort to provide protection for copyrighted works, both internet technology experts and legal experts work together to develop technology that is able to protect copyright from various forms of abuse that may occur due to rapid technological advances. One innovation that has been produced by these technology experts is the development of security technology to protect digital content from illegal or unauthorized actions. Security technology, namely Digital Rights Management (DRM), is a security system designed to protect creative works Irawati, 2019).

In the Copyright Law, the norms regarding DRM have been elaborated, namely in Article 6 which regulates "Copyright management information" and "Copyright electronic information." Copyright management information includes methods or systems that can identify the originality of the substance of the work and its creator, as well as information codes and access codes. Meanwhile, Copyright electronic information includes data about the creation that appears electronically related to the announcement of the creation, the name of the creator, the copyright holder, and the period and conditions of use of the creation. This article supports the implementation of DRM by providing a legal framework that protects digital copyright management information. It ensures that information, such as the name of the creator, the copyright holder, and the terms of use of the work, may not be altered or deleted without authorization (Riswandi, 2016). This principle is very important in the application of DRM

because it maintains the integrity and authenticity of copyright information when content is published or distributed in digital form. This protection applies not only to new creations, but also to works that were previously protected in analog form and then converted into digital format.

Then there are other articles in the Copyright Law that recognize DRM as a "security technology" used to protect copyrights on digital works. As in Articles 52 and 53 of the Copyright Law, which regulate the prohibition of damaging or eliminating technological means used as security technology, except for the interests of national defense and security or other lawful reasons.

These articles directly recognize DRM as a legitimate "means of technological control" to protect copyright in the digital realm, provide a legal basis for the application of this technology to prevent illegal use or copying, and support DRM by establishing protections for the hardware and software used in storing and protecting digital copyrights, such as encryption and secure server settings.

The government's authority to monitor infringement of copyright and related rights through information technology is set out in Article 54 of the Copyright Act. DRM plays an important role in supporting this oversight by controlling access, distribution, and use of copyrighted digital content (Mikafa, Hariandja, & Nail, 2022).

Through DRM, the government can monitor and prevent the dissemination of illegal content digitally. In , this article also encourages cross-country cooperation to strengthen efforts to prevent copyright infringement on digital platforms. Under Article 54, the Minister of Communications and Digital (Menkomdigi) has a legal basis to prevent and eradicate illegal acts of piracy, including digital piracy.

The government, through Menkomdigi, actively blocks hundreds of links containing pirated content and illegal streaming services without a license. In this effort, the National Cyber and Crypto Agency (BSSN) also plays an important role by providing cyber security that supports digital content protection. BSSN works closely with Menkomdigi to secure information technology networks and infrastructure to prevent illegal access and cyberattacks on platforms that protect digital copyrights

Furthermore, Law Number 1 Year 2024 on the Second Amendment to Law Number 11 Year 2008 on Electronic Information and Transactions (ITE Law), has provided a legal basis for the regulation of electronic activities in Indonesia, including the protection of digital content that can be related to DRM.

Where in Article 5 to Article 8 recognizes that electronic information and documents are valid evidence, and their management must be carried out in a way that ensures the integrity, authentication, and security of the data. DRM in this case can be seen as a technology that helps ensure that digital information, including copyrighted content, is processed, stored, and accessed securely in accordance with the provisions of the law.

Article 26 and Article 27 of the ITE Law, as well as other relevant articles, emphasize the need for electronic system security to protect personal data and prevent misuse of electronic information that may disturb public order and violate the law, including mechanisms to prevent illegal distribution of copyrighted digital content. DRM plays a role in controlling access to digital content and preventing acts of piracy or copyright infringement, in accordance with the principles of cybersecurity stipulated in the ITE Law

Regulations in Indonesia also regulate criminal sanctions for digital copyright infringement. Article 112 of the Copyright Law stipulates that for every person who unlawfully commits an act as referred to in Article 7 paragraph (3) and/or article 52 for Commercial Use, shall be punished with imprisonment of 2 (two) years and/or a maximum fine of Rp300,000,000.00 (three hundred million rupiah). This article prescribes punishment for any person who intentionally damages the means of security technology used to protect copyright for commercial purposes without permission

From the articles of regulatory provisions described above, especially in the Copyright Law, although it provides a legal framework for the protection of copyright management information and copyright electronic information through security technology such as DRM, its effectiveness is still considered less strong in protecting this security technology due to the nature of sanctions in the form of a complaint offense. Complaint offense means that acts of destruction, alteration, or removal of copyright management information can only be prosecuted if there is a complaint from the aggrieved party, in this case the creator or copyright holder (Jamba, 2015). This means that violations of DRM provisions, such as the removal or modification of copyright information for commercial purposes, will not automatically be processed by law enforcement officials unless there is a formal complaint filed by the rightful party.

As a result, this provision provides room for offenders to commit illegal acts without fear of immediate legal consequences, as there is no guarantee that every offense will be complained about or prosecuted. Complaint offenses are different from general offenses, where law enforcement can be carried out without the need for complaints from certain parties (Jamba, 2015). Thus, protection of DRM and other security technologies is less effective as it relies on the awareness and ability of copyright holders to report infringement, which is not always the case. This makes law enforcement against DRM infringement weaker and potentially does not provide sufficient deterrent effect for infringers.

Then related to Article 53 of the Copyright Law is not regulated regarding criminal sanctions, because there is a very broad public interest related to the regulation of security technology against a copyrighted work. However, this can also be considered a weakness in protecting security technologies such as DRM, which are applied to digital copyrighted works (Irawati, 2019).

In terms of technology, the way DRM works in protecting digital copyrighted works, especially in digital streaming services includes several techniques, namely (Sandra, Ra'fah, & Permana, 2023)

1. Encryption

DRM uses encryption to protect digital content, be it music, videos, or e-books. The encryption process involves cryptographic algorithms that scramble the content so that it can only be accessed by users who have the decryption key. In this case, the key is often integrated with the user's device, such as a smartphone or computer, and will only work if the device is authorized. In existing digital streaming services in Indonesia, DRM works by encrypting audio or video data so that the content can only be accessed by authorized users. When the user plays the content, the authorized device will decrypt the data and display it without compromising the quality. This encryption process involves cryptographic algorithms, such as Advanced Encryption Standard (AES), which ensures that the content cannot be accessed without a valid key. On streaming services like Spotify, Netflix, Fucking, this process takes place automatically when a user purchases or subscribes to content.

2. Public/Privacy Keys

It is a method that involves two cryptographic keys to unlock access to the content. The public key is used to encrypt the content, while the private key is used to decrypt the content on the authorized user's device. This process ensures that only the device or user in possession of the private key can access the content, while any other party attempting to access the content without the key will be denied .

3. Access Control

The use of access control limits the number of devices that can be used to access a single piece of content. For example, digital streaming services such as Sky Music or Amazon Video limit the number of devices that can be used to download or watch the same content. This is done to prevent the unauthorized spread of illegal content. In Indonesia, local streaming services also implement these access controls to ensure that only users who have subscribed or

paid can access the content. If a user tries to access the content through an unregistered device, they will be asked to re-authenticate or obtain an additional license.

4. Watermarking

Watermarking is a technique that embeds marks or information into content without destroying its original quality. Watermarks are usually invisible to users, but can be used by copyright holders to trace the origin of content and prevent illegal dissemination. In many cases, watermarks can help identify the source of copyright infringement if content is leaked to unauthorized parties. In Indonesia, this watermark technology is often used on streaming content to protect movies, TV shows, and music from illegal distribution

All of the above technologies work together to ensure that digital content can only be accessed by authorized users and prevent illegal copying. Streaming services in Indonesia, both local ones like Vidio.com, Mola, Iflix, Langit Musik, and global ones like Netflix, use DRM as an integral part of their content security.

The technology and methods used by DRM in streaming services in Indonesia do offer good copyright protection, but still have some weaknesses, both in terms of prevention and repression. The use of encryption and dynamic authentication keys can limit illegal access to content, but challenges arise from increasingly sophisticated piracy attempts. While encryption provides security during transmission, there are weaknesses when the content is decrypted at the user side, which can be exploited by unauthorized parties (Nasution et al., 2016). DRM provides good control over content distribution, its effectiveness depends on how well the technology is integrated with law enforcement and user awareness about the importance of respecting copyright. Ultimately, DRM is effective in restraining piracy to a certain extent, but it is unable to completely eliminate this threat without the support of stronger regulations and evolving technology.

Although Digital Rights Management (DRM) in Indonesia has been implemented to protect digital content, both in terms of technology and regulation, its effectiveness in providing preventive and repressive protection is still less than optimal. From the preventive side, although DRM technologies such as encryption, access control, and watermarking have been implemented, weaknesses still arise when the content decrypted on the user side, which opens a gap for piracy. Dynamic DRM technology is able to restrict access, but the development of increasingly sophisticated piracy technology continues to challenge the limits of DRM capabilities. addition, there is no regulation that strictly regulates the standard of DRM technology that should be applied by digital platforms in Indonesia, which causes inconsistency in its application across platforms.

From the repressive side, law enforcement is still hampered by the complaint offense system, which means that legal action against digital copyright infringement can only be taken if there is a report from the right holder. This leads to many violations that are not followed up because rights holders do not always report or realize the violations that occur. addition, the sanctions set out in the Copyright Act are often considered not to provide a sufficient deterrent effect. The lack of proactive law enforcement and reliance on rightsholder reports means that repressive protection against DRM infringement is far from effective. Prevention and enforcement efforts require better coordination between evolving technologies with stronger regulations and strict implementation.

In addition to Indonesia, several other countries also implement a DRM system or sometimes called ERM which is regulated in copyright regulations. These countries are countries such as the United States, Germany, Australia, Japan, and several other countries that have ratified the WIPO Internet Treaties. This shows that a mutual agreement has been reached to adopt rules regarding DRM protection technology. This agreement aims to provide more effective protection of copyright. As a comparison related to its effectiveness, here is a comparison table between the effectiveness of DRM Implementation on Digital Streaming Services in Indonesia, the United States, and Germany:

Table 1. Comparison of the Effectiveness of DRM Implementation on Digital Streaming Services between Indonesia, the United States, and Germany

Aspects	Indonesia	United States of America (Bechtold, 2004)	Germany (Bechtold, 2004)
Key Regulations	Law Number 28 of 2014 concerning Copyright	Digital Millenium Copyright Act (DMCA)	Copyright Act and implementation of the EU Copyright Directive
Law Enforcement	Depends on complaint offense, so enforcement is still relatively weak without a report from the right holder.	Strong, with clear anti-circumvention rules and strict legal sanctions	Very strict, with a ban on bypassing safety technology and the application of serious sanctions
Technology Used	Encryption, access control, watermarking	Advanced encryption, public/private keys, access control, and watermarking	Uses advanced DRM technology, multilayered encryption, and access control
Effectiveness of DRM Usage	Moderate, depending on rights holders' awareness and law enforcement involvement	Effective, supported by strict regulations and advanced technology	Highly effective, backed by harmonized EU law and leading-edge technology

Efforts and Recommendations in Strengthening the Implementation of Digital Rights Management (DRM) Regulations in Indonesia

Regarding efforts to strengthen the implementation of Digital Rights Management (DRM) regulations in Indonesia, an important step that can be taken is to strengthen the existing legal framework. Although the Copyright Law has recognized the existence of DRM, the regulation still has weaknesses and is not very specific.

When the Copyright Law was enacted in 2014, the development of digital technology, including streaming technology and online distribution of content, was not as rapid as it is now. Although the Copyright Law has recognized the existence of DRM, at that time DRM technology and issues related to the protection of digital content were not very relevant or a major concern. Along with the rapid growth of streaming services and the increasing threat of digital piracy, copyright protection through DRM mechanisms has become increasingly important. The regulation is still general and has not specifically regulated the application of DRM, so there is a need for improvement and updating of the legal framework. Copyright Law needs to keep up with the times in order to provide more effective legal protection for digital content.

In addition to improving the Copyright Law, regulations on Cyber Security and Resilience are also needed. The application of the upstream regulation model can be a transformative legal approach in dealing with cybersecurity challenges that continue to grow along with rapid digital transformation. This regulatory model emphasizes the importance of strict security standards in the early stages, before cyber threats hit consumers or end users. With strict regulation at the upstream level, digital companies and industries will be encouraged to develop better security solutions to meet the requirements (Ramli, 2024b). , although DRM technology exists, its implementation is still vulnerable to cyberattacks, such as hacking, content piracy, and data theft involving copyright. With upstream regulation, regulators can set minimum security standards that the industry must adhere to in order to protect copyright and the digital infrastructure as a whole. Regulators play a role in conducting audits and inspections and enforcing compliance with regulations to ensure economic and social stability through effective cybersecurity (Ramli, 2024b).

The Cyber Security and Resilience Act will be an important foundation in protecting copyright in the digital world. Cybersecurity, which involves protecting digital infrastructure

from external threats, is closely related to copyright protection (Ramli, 2024c). Attacks on digital infrastructure, such as streaming sites, storage servers, and content distribution applications, can result in massive leakage and piracy of copyrighted content. In this case, DRM requires the full support of a robust cybersecurity system, which starts with the implementation of clear and strict upstream regulations.

, copyright infringement through digital content piracy often involves organized international networks operating outside of Indonesian jurisdiction. Therefore, this regulation should include provisions that enable cross-border cooperation in handling cybercrime involving copyright infringement. Strengthening cooperation with other countries that have strong cybersecurity laws, such as the United States and countries in Europe, is essential to ensure that Indonesia can follow international standards in copyright enforcement in the digital realm (Ramli, 2024a).

This cross-border cooperation can be carried out through the mechanism of bilateral and multilateral agreements that allow the exchange of information, joint investigations, and extradition of perpetrators of copyright infringing cybercrime. For example, Indonesia can strengthen partnerships with countries that are members of the Budapest Convention on Cybercrime, which specifically regulates the handling of cybercrime including digital copyright infringement. The Convention provides a framework for countries to cooperate in tracking and cracking down on crimes that occur in cyberspace, especially in cases where the perpetrators operate outside of national jurisdiction.

By strengthening the legal framework for international cooperation, Indonesia can more effectively crack down on digital content piracy, which is often perpetrated by international networks that are difficult to reach under national law. addition, digital service providers operating in Indonesia, both local and international, will have a clearer obligation to collaborate with the government in identifying and cracking down on copyright infringement that occurs on their platforms.

The Regulation on Cyber Security and Resilience can provide a legal foundation for the government to adopt more advanced international cybersecurity technologies and standards in protecting copyright. Technologies such as end-to-end encryption, security certification for software, and real-time infringement detection systems can be integrated into Indonesia's digital infrastructure, thereby strengthening DRM and copyright protection as a whole.

As a reference, regulations on Cyber Security and Resilience in Indonesia need to reflect on other countries that already have legal arrangements. Some developed countries already have strong regulations related to cyber security and resilience. The European Union, for example, through the EU Cyber Resilience Act and the NIS Directive, focuses on the protection of critical infrastructure and cross-border coordination in the face of cyber threats. The United States has also issued an Executive Order on Improving the Nation's Cybersecurity, which strengthens software supply chain security and encourages cybersecurity modernization in the government and private sectors. , NIST has become a global reference in cybersecurity standards (Ramli, 2024d).

In Asia, Japan implemented The Basic Act on Cyber Security, which focuses on cyber risk management and critical infrastructure protection, and is supported by NISC as a watchdog agency. Singapore, with its Cybersecurity Act and Personal Data Protection Act (PDPA), has built a strong legal framework to protect critical infrastructure and personal data, making it a leader in cybersecurity in the Southeast Asian region (Putra, 2019).

In addition to regulations on Cyber Security and Resilience, Indonesia also needs to develop comprehensive regulations related to Artificial Intelligence (AI), especially as AI is now increasingly playing a role in various industrial fields, including the creative industries related to copyright and DRM (Ramli, 2022). In the music sector, for example, AI is used to generate songs, create new melodies, and even modify or imitate artists' voices through technologies such as deepfake and soundlike (Riyanto & Pertiwi, 2022). This poses a major

challenge to copyright protection as AI is able to create new works using existing data or works without the consent of the copyright owner.

In an effort to strengthen DRM regulation, AI has great potential to optimize the digital content protection system, especially with its ability to analyze illegal content distribution patterns and detect piracy in real-time. AI can be used to identify suspicious activities involving copyrighted content, such as illegal uploading and distribution of movies or music on various platforms. With machine learning technology, AI is able to learn from previous patterns of illegal content distribution and update its methods to prevent copyright infringement more efficiently and precisely

Several other countries have implemented AI-related regulations to ensure the safe and ethical use of this technology. The European Union, for example, passed the EU Artificial Intelligence Act, which regulates AI based on risk levels, ensures copyright protection, and prohibits the use of AI to produce unauthorized works (Hickman, Lorenz, & Teetzmann, 2024). , the United States, through its Executive Order on AI, emphasizes safe and ethical AI development and protects intellectual property rights. The National Institute of Standards and Technology (NIST) has also developed a framework for managing AI risks.

In Southeast Asia, Singapore through its Model AI Governance Framework and Personal Data Protection Act (PDPA), emphasizes ethical responsibility in AI development as well as protecting personal data and copyright. These countries are trying to create balanced regulations between technological innovation and protection of intellectual property rights, and this is what Indonesia needs to do.

In addition to strong and specific regulations, the role of society is also an important element in strengthening copyright protection, especially in the context of DRM and intellectual property. Without high awareness from the public, legal and technological efforts in protecting copyright will not achieve optimal results. Public awareness to respect copyrighted works by not downloading, reproducing, or distributing digital works illegally is one of the most effective preventive measures. In today's digital era, where content can be accessed easily, the role of society is vital to create a healthier digital ecosystem that respects the rights of creators.

The public needs to be encouraged to use legal services to enjoy digital content, such as official applications for streaming music, movies, and purchasing electronic books. Awareness that illegal use of content not only harms creators, but also hinders the development of the creative industry, must be socialized more intensively. The government and digital platforms also have the responsibility to educate the public about the adverse effects of piracy.

CONCLUSION

The effectiveness of Digital Rights Management (DRM) in Indonesia in protecting copyright on digital platforms still faces a number of challenges, both in terms of technology and law enforcement. Although the Copyright Law and other regulations such as the ITE Law have provided a legal basis for DRM, there are still limitations in its implementation. DRM in Indonesia uses methods such as encryption, access control, and watermarking to restrict illegal access, but these technologies are still vulnerable to piracy when content is decrypted at the user side. addition, complaint-based law enforcement makes the legal process dependent on complaints from rights holders, potentially reducing the deterrent effect for violators. By comparing Indonesia with other countries such as the United States and Germany that have stronger DRM regulations and technology, it appears that the effectiveness of DRM protection in Indonesia is still moderate and requires strengthening, both in more specific regulations and proactive law enforcement.

To strengthen the implementation of DRM in Indonesia, various strategic steps are needed, including the improvement of copyright regulations and stricter cybersecurity enforcement. Although Law No. 28/2014 has recognized DRM, it is not specific enough and needs to be updated to keep up with the development of digital technology and the increasingly

complex threat of content piracy. Approaches such as upstream regulation and strengthening cross-border cooperation will help tackle cyber-attacks on digital copyrights. In , the application of Artificial Intelligence (AI) technology in DRM can increase the effectiveness of the digital content protection system through real-time monitoring of illegal distribution. Comprehensive AI regulations, such as those implemented in the European Union and Singapore, are important references for Indonesia. In addition to regulation and technology, the role of society is crucial in creating awareness and reducing piracy through the use of legal content services. All of these steps will strengthen the copyright protection ecosystem in Indonesia and support the healthy development of the creative industry.

REFERENCE

Adrian, A. (2009). Digital Rights Management Terapan serta Ancamannya. Bandung.

Amirulloh, M., & Muchtar, H. N. (2016). Buku Ajar Hukum Kekayaan Intelektual (Vol. 1). Sumedang: Universitas Padjadjaran, Unpad Press.

Andrea, D. L., Permata, R. R., & Safiranita, T. (2020). Freedom of Panorama Terkait Pelindungan Karya Cipta di Ruang Publik Berdasarkan Hukum Hak Cipta dan Hukum Teknologi Informasi dan Komunikasi. JIHK, 2(1), 59–75. https://doi.org/10.46924/jihk.v2i1.133

Bechtold, S. (2004). Digital Rights Management in the United States and Europe. The American Journal of Comparative Law, 52(2), 323–382.

Daud. (2024). Perspektif Undang-Undang Hak Cipta dan Undang-Undang ITE Terhadap Penyebarluasan Buku Elektronik. Socius: Jurnal Penelitian Ilmu-Ilmu Sosial, 1(6), 359–362.

Dirjen KI. (2025). Sejarah DJKI. Retrieved February 24, 2025, from https://www.dgip.go.id/tentang-djki/sejarah-djki

Faisal, A. (2024, February 1). Film Nasional Berpotensi Berkembang di Era Layanan Streaming.

Hickman, T., Lorenz, S., & Teetzmann, C. (2024). Long Awaited EU AI Act Becomes Law after Publication in the EU's Official Journal.

Irawati. (2019). Digital Right Managements (Teknologi Pengaman) dalam Perlindungan Terhadap Hak Cipta di Era Digital. Diponegoro Private Law Review, 4(1).

Jamba, P. (2015). Analisis Penerapan Delik Aduan dalam UU Hak Cipta untuk Menanggulangi Tindak Pidana Hak Cipta di Indonesia. Jurnal Cahaya Keadilan, 3(1).

Julianti, L., & Subekti, R. P. (2018). Standar Perlindungan Hukum Kegiatan Investasi Pada Bisnis Jasa Pariwisata di Indonesia. Kertha Wicaksana, 12(2), 156–166.

Kharisma, M. D. L., Hakim, N., & Mustafa, M. E. (2024). Peran Digital Right Management sebagai Teknologi Pengaman atas Upaya Perlindungan Hak Cipta dari Pembajakan. Blantika: Multidisciplinary Journal, 2(11), 525–544. https://doi.org/10.57096/blantika.v2i11.233

Kim, J.-H., & Leung, T. C. (2021). Eliminating digital rights management from the E-book market. Information Economics and Policy, 57, 100935. https://doi.org/10.1016/j.infoecopol.2021.100935

Kusno, H. (2017). Perlindungan Hukum Hak Cipta Terhadap Pencipta Lagu yang Diunduh Melalui Internet. FIAT JUSTISIA: Jurnal Ilmu Hukum, 10(3). https://doi.org/10.25041/fiatjustisia.v10no3.789

Mikafa, A. B., Hariandja, T. R., & Nail, M. H. (2022). Perlindungan Hukum Pemilik Hak Cipta Terkait Pembajakan Karya Sinematografi Pada Platform Telegram. Welfare State Jurnal Hukum, 1(2), 187–216. https://doi.org/10.56013/welfarestate.v1i2.1669

Mulyani, S., Lestari, A. T. W., W, A. M. J., & Tedjosaputro, L. (2024). Perlindungan Hukum Hak Cipta pada Industri Konten Digital dalam Perspektif Society 5.0. SPEKTRUM HUKUM, 21(1), 1. https://doi.org/10.56444/sh.v21i1.5090

Nasution, S. M., M., R. R., & Virgono, A. (2016). Implementasi Digital Rights Management pada Media-Streaming sebagai Pelindung Data Digital. Jurnal SIFO Mikroskil, 17(1), 71–80.

Pemerintah RI. Undang-undang (UU) Nomor 28 Pasal 1 Tahun 2014 tentang Hak Cipta. , https://peraturan.bpk.go.id/details/38690 § (2014). Indonesia: LN.2014/No. 266, TLN No. 5599, LL SETNEG: 57 HLM.

Pemerintah RI. Undang-undang (UU) Nomor 28 Pasal 5 Tahun 2014 tentang Hak Cipta. , https://peraturan.bpk.go.id/details/38690 § (2014). Indonesia: LN.2014/No. 266, TLN No. 5599, LL SETNEG: 57 HLM.

Pemerintah RI. Undang-undang (UU) Nomor 28 Pasal 9 Tahun 2014 tentang Hak Cipta. , https://peraturan.bpk.go.id/details/38690 § (2014). Indonesia: LN.2014/No. 266, TLN No. 5599, LL SETNEG: 57 HLM.

Pemerintah RI. Undang-undang (UU) Nomor 28 Pasal 40 Tahun 2014 tentang Hak Cipta. , https://peraturan.bpk.go.id/details/38690 § (2014). Indonesia: LN.2014/No. 266, TLN No. 5599, LL SETNEG: 57 HLM.

Putra, K. I. (2019). Belajar dari Tata Kelola Keamanan Siber Singapura. Universitas Gadjah Mada, 1–12.

Ramli. (2024a). Keamanan Siber dan Urgensi “Upstream Regulation” (Bagian I).

Ramli. (2024b). Keamanan Siber dan Urgensi “Upstream Regulation” (Bagian II Habis).

Ramli. (2024c). Pentingnya UU Keamanan dan Resiliensi Siber.

Ramli. (2024d). “UN Convention Against Cybercrime”: Konvensi Pertama PBB Tentang Kejahatan Siber (Bagian I).

Ramli, T. S. (2020). Aspek Hukum atas Konten Hak Cipta Dikaitkan dengan Undang Undang Informasi dan Transaksi Elektronik No. 19 Tahun 2016. Jurnal Legislasi Indonesia, 17(1), 62. https://doi.org/10.54629/jli.v17i1.589

Ramli, T. S. (2022). Hak Cipta Dalam Media Over The Top (Vol. 1). Bandung: PT Refika Aditama.

Riswandi, B. A. (2016). Doktrin Perlindungan Hak Cipta di Era Digital (Vol. 1). Yogyakarta: F.H.UII Press.

Riyanto, G. P., & Pertiwi, W. K. (2022). Menilik Teknologi “Deepfake” di Balik Video Diduga Mirip Nagita Slavina.

Sandra, E. N., Ra’fah, A. F., & Permana, A. (2023). Optimalisasi Perlindungan Keamanan Karya Digital Di Indonesia : Teknologi Digital Right Management Sebagai Solusi Privacy Engineering. Prosiding Lomba Karya Tulis Ilmiah Dr. Mochtar Riady Legal Week 2023, 1–16. Banten: Anthology: Inside Intellectual Property Rights.

Venkataramu, R. (2007). Analysis and Enhancement of Apple’s Fairplay Digital Rights Management. San Jose.

Wang, Y., & Shen, Y. (2009). Compatible Digital Rights Management System on MS Windows Platform. 2009 International Conference on Information Engineering and Computer Science, 1–4. IEEE. https://doi.org/10.1109/ICIECS.2009.5367148.