International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =7.938, January-June 2024, Submitted in January 2024, ISSN -2393-8048

Cyber Law and Digital Rights Management: An Extensive Examination of Legal Cases, Privacy Concerns, And Global Consequences

Farhat Jahan, Research Scholar, Dept. of Law, The Glocal University Saharanpur, Uttar Pradesh
Dr. Kuldip Singh, Professor, Research Supervisor, Glocal Law School & Jurisprudence, The Glocal University, Saharanpur, Uttar Pradesh

ABSTRACT

The digital age demands the protection of intellectual property rights and the enforcement of cyber laws to ensure the integrity and security of online content. Digital Rights Management (DRM) and cyber law play crucial roles in preventing unauthorized use, duplication, transmission, and alteration of copyrighted materials. DRM uses techniques like restrictive agreements, encryption, and content scrambling to safeguard digital content, ensuring only authorized users can access and utilize it. Despite challenges posed by standardized technologies and vulnerabilities exploited by attackers, effective DRM systems integrate secure software and hardware solutions to protect digital intellectual property. The interrelation between cyber law, cyberspace, and cybercrimes is also examined, emphasizing the need for robust legal frameworks to govern online activities and prosecute cyber offenses. Understanding this interrelation is crucial for developing effective legal mechanisms to combat digital offenses and protect privacy and intellectual property rights. The ongoing development and enforcement of DRM systems and cyber laws are essential for safeguarding digital rights and fostering a secure and equitable digital environment.

Keywords: Digital Rights Management (DRM), Cyber Law, Intellectual Property Rights, Cybercrimes.

1. INTRODUCTION

Within the context of the modern digital world, the convergence of cyber law and digital rights management (DRM) is a crucial nexus that has an impact on the economic, social, and political spheres on a global scale. The legal frameworks that regulate cyber activities have gotten more complicated and vital as technology continues to advance. This is because the protection of digital material has also become increasingly difficult. This investigation dives into the complex realm of digital rights management (DRM) and cyber law, including the investigation of key legal cases, concerns over privacy, and the far-reaching global consequences of these issues.

The term "cyber law" refers to the collection of rules and regulations that regulate the use of the internet, digital communication, and electronic commerce. The security of data, the prevention of cybercrime, the preservation of intellectual property rights, and the freedom of expression online are all included in this. Cyber law has become more important in maintaining the integrity, security, and fairness of digital interactions as a result of the expansion of digital technology.

A term that is used to describe the technical solutions and legal frameworks that are used in order to govern the usage, distribution, and access to digital information is called "digital rights management." For the purpose of safeguarding intellectual property rights in the digital age, digital rights management (DRM) is an essential tool. This includes software, music, video, and other types of digital material. The goal of effective digital rights management (DRM) methods is to prohibit unlawful access, copying, and distribution of material, therefore protecting the interests of producers and distributors of content.

Legal Cases

Prominent court decisions in DRM and cyber law demonstrate the dynamic and continuing challenges in these domains. Historic cases often provide guidelines that influence how the law will be interpreted and applied in the future. An increased focus on DRM systems resulted, for instance, from the Napster case in the early 2000s, which was crucial in tackling the unlawful online sharing of music files. In the same way, legal cases such as Google Spain

SL v. Agencia Española de Protección de Datos (2014) have influenced digital era privacy rights and the right to be forgotten.

- **Privacy Concerns**

A key topic of debate when it comes to DRM and cyber legislation is privacy. Individual privacy is seriously jeopardized by the way governments and companies gather, store, and use personal data. Regulations like the General Data Protection Regulation (GDPR) in the European Union, which lays out stringent requirements for data management methods, are examples of cyber laws that attempt to address these problems. But it's still difficult to strike a balance between the preservation of people's right to privacy and the need of security and monitoring.

- **Global Consequences**

Cyber law and DRM have significant worldwide ramifications that impact economic policy, foreign relations, and social conventions. A complicated network of international laws and treaties is the result of different nations taking different stances on digital rights and cyber control. Because of its worldwide reach, cybercrimes must be properly combated and fair use of digital information must be ensured via cross-border cooperation and harmonization of legal norms.

Examining digital rights management and cyber law shows a dynamic and developing topic that is essential to the operation of contemporary society. By examining court cases, privacy issues, and worldwide ramifications, this research offers a thorough grasp of the difficulties and possibilities brought about by the digital era.

2. LITERATURE REVIEW

C. Adamuthe et al. (2015)written about a topic that is a subject of much discussion: cloud computing. They specifically recommended research methodologies in addition to a market viewpoint. They went over the foundations of cloud computing, including its architecture, its widespread use, and the security issues that come with it. The services that must be provided must be based on the needs of the customers, regardless of the type of business—banks, organizations, sectors, health care, or education. It is imperative to use cloud computing to satisfy their expectations. Businesses and the service industry rely on cloud computing in the modern world to increase worker productivity. Numerous layers of various cloud models are considered, and the security issues associated with them are investigated. Nonetheless, there are other risks, including data filtration, theft, and internal cloud attack threats. It offers a more thorough comprehension of the issues, enabling safer and better services.

Arora, Amarpreet et al. (2012)explained a computer invention in forensics. This technology can fight cybercrime. This research aimed to examine the application of fundamental methods and approaches used by any country's security agency to combat cybercrime. Cybercrimes can also involve tactics or techniques that are used to cope with other criminals and investigations. This is due to the fact that criminals' mental psyche remains the same whether they operate in the actual or virtual environment.to guarantee the efficacy of our solutions. Thanks to the internet, cybercriminals are not limited to a single nation or country; they can utilise their malevolent intent to enter other nations' secret societies as well.

Balte et al. (2015)issues with IoT security that have come to light. They provided a questionnaire regarding the internet of things. They described the encryption methods that are used to safeguard data that is transferred over the internet. To guarantee the security of data transmission via the internet, a plethora of methods are available. Certain cryptographic algorithms, like symmetric and asymmetric cryptographic techniques, are subjected to comparative study. Additionally, a study of their algorithms is carried out. The authors concluded by pointing out the effectiveness of the two previously described tactics. How much can a user depend on these precautions to keep them secure is the question.

C. Donald et al. (2013)examined the subject of security for mobile clouds. There was also discussion of the problems and challenges. The authors described how the availability of networks has led to an increase in global intelligence. The internet has produced autos,

mobile devices, and smart cities. individuals now have more facilities as a result, but because of the overexposure of individuals and resources, as well as how simple it is to access them online, this has resulted in issues relating to cyberspace that are known as cyber-attacks. Research on legal frameworks is another way that these issues are being addressed. They provided instructions on how to use mobile devices for safe online transactions. The author claims that mobile technology is being widely adopted worldwide, indicating that everyone is using their handheld devices to fulfil all of their responsibilities, including completing transactions. However, there is also a problem with the transfer of secure data. One-time private key use is one of the security authentication techniques that the author discusses.

D. Smith et al. (2002)wrote an essay about the challenges associated with cyber security. They were well aware of the possible risks posed by hackers. We talked about the September 11 attacks and how they changed the path of history. The world's rapid growth, according to the author, is changing the facts of business. As technological advancements persist, the internet has impacted all facets of global life, including business. Nonetheless, the number of crimes connected to the internet has increased as a result of the web world's accelerating speed. The author claims that the explanation of intellectual property rights was provided. Furthermore, the security of the cyberspace and the safety of individuals who transact business or communicate via it are highly stressed.

Garg et al. (2003)A plan to measure the financial effect of information technology security breaches was put forth. Since the beginning, the issues around protection have grown along with the development of information sharing. Even though there are techniques to check on these problems, some of these techniques are starting to fail as technology advances. This study aims to investigate several distinct detection and prevention strategies. The way that safety is ensured by implementing identifying procedures at various network levels.

K. Maitra, (2015)explained the tools that cybercriminals use. They also described the technique, as well as the legal and strategic approach that hackers use. Through their text, the writers shed light on a variety of crimes that occur in the cyber world and the fundamental forces that contribute to the occurrence of such crimes. The study also discussed the effects that crimes related to information technology have on society and explained the age that follows that of related cybercrimes.

3. MANAGEMENT OF DIGITAL RIGHTS

Digital Rights Management (DRM) is a systematic approach to safeguarding digital intellectual property rights via "digital media". The goal of "Digital Rights Management (DRM)" is to stop copyrights from being used, altered, deleted, transmitted, or distributed without authorization. Publishers and authors may now more effectively protect their rights in the "digital world," just as they would in the real print world, thanks to the DRM system. Original material may be created and shared for free thanks to advanced software and digital technologies. Only specialists are able to differentiate between original and extracted copies. This is the reason for the world of DVDs, CDs, and pirated movies. The DRM is a vital part when it comes to providing individuals with access to critical information, like a pricing catalog, a contract's details, a book, reports, or other papers. If DRM is absent, we don't take any more steps to prevent others from gaining intellectual property.

A collection of tools and procedures known as digital rights management (DRM) are intended to protect intellectual property rights in the digital sphere. Its goal is to stop illegal copies, distribution, editing, or removal of digital material, including software, photos, videos, and text. For content producers, publishers, device makers, and copyright holders to keep control over who may access and utilize their digital assets, DRM is an essential tool.

Definition and Scope of Digital Rights Management

The use of access control technologies to prevent users from accessing or using digital material in ways that have not been approved by the content provider or copyright holder is known as DRM. DRM concentrates on incorporating access restrictions straight into the digital material itself, as opposed to using more conventional copy protection techniques like

key files or serial numbers. This guarantees that material may only be viewed or used in compliance with the terms and conditions that the content owner has established.

Common Techniques of Digital Rights Management

Several techniques are employed within DRM frameworks:

1. **Management of Restrictive Agreements:**In order to protect copyright and public domain rights, this method uses license agreements that specify how digital information may be accessed, utilized, and disseminated.
2. **Encryption and Scrambling:**Digital rights management (DRM) uses encryption techniques to jumble digital material and adds tags to restrict access and duplication. This guarantees that the material can only be accessed by authorized individuals who possess decryption keys.

Requirements and Challenges in DRM Implementation

The necessity to stop illegal sharing and unauthorized access to digital information on the internet is what motivates the use of DRM. Limiting device compatibility, imposing use restrictions during designated subscription times, limiting the number of devices that may access the material concurrently, and establishing maximum download limits are some of the essential needs. Managing various digital environments and resolving vulnerabilities used by attackers to get around DRM safeguards are challenges associated with DRM implementation.

Formats and Failures of Digital Rights Management

DRM systems, like the Content Scrambling System (CSS), which is extensively used in commercial DVDs, are often organized around certain formats. Unfortunately, the absence of best practices and flaws that make DRM schemes unreliable against dedicated attackers have led to their failure. To reduce these dangers, several companies create in-house DRM systems that are suited to their unique demands and security specifications.

Components of a Robust DRM Scheme

A robust DRM scheme should encompass the following components:

- **Secure Hardware and Software:**Using encryption engines and secure hardware keys to prevent illegal access to DRM keys, passwords, and licensing data.
- **Legal Framework:**Integration with a strong legal framework that encourages the use of the law to enforce and defend digital rights.
- **Asset Protection Mechanisms:**Implementing temporary keys for access to restricted material, storing DRM keys and licensing files securely, and sending decrypted content to authorized users securely.

DRM is essential for safeguarding digital intellectual property rights because it uses technology and legal frameworks to stop illegal access to and distribution of digital information. Effective DRM techniques will remain crucial in the fight against piracy and maintaining the integrity of intellectual assets as digital environments change.

4. INTERRELATION BETWEEN CYBER LAW, CYBER SPACE AND CYBER CRIMES IN INDIA

There is an unbreakable and profound relationship between cyberspace, cybercrimes, and virtual offenses. Cyber law is the body of legislation that governs all online and virtual activities carried out by individuals and organizations alike. It also establishes mechanisms for cyber authority and provides criminal justice systems and a list of cyber offenses that are punishable under cyber law. The "virtual world" or "cyber space" is also the crime scene. All you need to commit a cybercrime or violate a cyberlaw is a computer, a keyboard, and an internet connection. A network connection is typically the lifeline for someone looking to commit a cybercrime. To put it briefly, cybercrime + cyberspace = cyberlaw, or cybercrime = cyberlaw + cybercrime violation + cyberspace (virtual crime scene)

These terms have the following meanings in this context:

• **Cyber Law:** is prescribed rules of cyber conduct;

• **Cyber Space:** is crime scene;

• **Cyber-crime:** is denial to follow prescribed cyber conduct or infringement of cyber law;

By understanding of basic attributes of cyber law, cyber space and cyber-crimes in depth we could easily understood interrelation among these.

Cyber Law in India

The internet and information technologies are dominating the global cyber community and expanding quickly. The globe faced new challenges as well as new opportunities brought about by information technology. Information technology is now present in practically every aspect of peoples' personal, professional, and social lives, including commerce, entertainment, science, sports, innovation, intellectual property rights, and education. It's expressed quite nicely that- **'every coin has two side, but one is always remaining in dark. Both these side are diverse as well as complimentary with each other but still both remain in the same frame work.'**

In the same way the- **"cyber law and cyber offence both are part of cyber legislation both are opposite with other, but both are framed in the same framework."**

The world wide web. has its own advantages as well disadvantages? It is well said that- **"A technology is a double-edged weapon, which could be used for saving life and also for endangering others life".**

The internet may use the same idea. With the mere assistance of a computer and keyboard network connection, it is the most potent weapon available, capable of causing more harm than any other. For instance, we may transmit or distribute any information at lightning speed, and we can also use a single click to propagate viruses. Unexpectedly, the Internet has drawbacks of its own. The computer could be used for a number of illegal acts, such as hacking, ID theft, data theft, software piracy, ATM debit or credit card fraud, spamming, email espionage, cyber fraud, and breach of privacy.

Cyber Space, The Virtual World

Technology is unified in the "Cyberspace." It originated in science fiction and the arts and made its way into popular culture. Today, security experts, government, military, business, and industry leaders use it to characterize various aspects of the global technology environment, including technology strategy.Another thing to keep in mind about cyberspace is that it's merely a hypothetical setting where communication via the internet is possible. Since 1990, the globe has witnessed an increase in the usage of the internet and digital communications in practically every aspect of human social and professional life. This has led to the rise in prominence of the cyberspace. It is the most uncontrolled and unregulated sphere in human history, created by the peoples of the physical world.

Cyber nuts, as they are commonly known, use cyberspace for practical purposes such as human interaction, opinion, and idea sharing, formal correspondence, instant messaging, gaming, artistic endeavours, political conversations, and more. Cyberspace is typically defined as a platform connected to the internet and other online cultures.

5. CONCLUSION

Digital Rights Management (DRM) is a crucial tool in the digital era to protect digital intellectual property rights and prevent unauthorized use, duplication, transmission, and alteration of copyrighted content. DRM systems use techniques like restrictive agreements, encryption, and content scrambling to ensure that only authorized users can access and use digital content. However, traditional DRM technologies often fail due to standardized technologies and vulnerabilities exploited by attackers. A good DRM scheme should include secure software and hardware solutions to protect content creation, allocation, and utilization against various attacks. Cyber law governs online activities, providing a legal framework for regulating and prosecuting cyber offenses. In India, cyber laws aim to address challenges such as hacking, identity theft, software piracy, and data breaches. Understanding the interrelation between cyber law, cyberspace, and cybercrimes is essential for developing effective legal mechanisms to combat digital offenses and protect privacy and intellectual property rights. DRM provides necessary tools to protect digital intellectual property, while

robust cyber laws are essential for regulating cyberspace, preventing cybercrimes, and upholding legal and ethical standards in the virtual world.

REFERENCES

1. Adamuthe, A. C., Salunkhe, V. D., Patil, S. H., & Thampi, G. T. (2015). Cloud computing–A market perspective and research directions. International Journal of Information Technology and Computer Science (IJITCS), 7(10), 42-53.
2. Arora, A. S., Bhatt, S. C., & Pant, A. (2012). Forensics Computing-Technology to Combat Cybercrime‖. International journal of advanced research in Computer Science and software Engineering, 2(7).
3. Balte, A., Kashid, A., & Patil, B. (2015). Security issues in Internet of things (IoT): A survey. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4).
4. Delerue, F. (2020). Cyber operations and international law (Vol. 146). Cambridge University Press.
5. Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. Risk Management and Insurance Review, 24(1), 93-125.
6. Fuster, G. G., &Jasmontaite, L. (2020). Cybersecurity regulation in the European union: the digital, the critical and fundamental rights. The ethics of cybersecurity, 97-115.
7. Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. Information Management & Computer Security, 11(2), 74-83.
8. Maitra, D., Scarpaci, J. F., Grinberg, V., Reynolds, M. T., Markoff, S., Maccarone, T. J., & Hynes, R. I. (2017). Simultaneous multiwavelength observations of V404 Cygni during its 2015 June outburst decay strengthen the case for an extremely energetic jet-base. The Astrophysical Journal, 851(2), 148.
9. Rusakova, E. P., Frolova, E. E., & Gorbacheva, A. I. (2020). Digital rights as a new object of civil rights: issues of substantive and procedural law. In Artificial intelligence: Anthropogenic nature vs. social origin (pp. 665-673). Springer International Publishing.
10. Schnettler, E., Donald, C. L., Human, S., Watson, M., Siu, R. W., McFarlane, M., ... &Fragkoudis, R. (2013). Knockdown of piRNA pathway proteins results in enhanced Semliki Forest virus production in mosquito cells. Journal of General Virology, 94(7), 1680-1689.
11. Sidorenko, E. L., & von Arx, P. (2020). Transformation of law in the context of digitalization: Defining the correct priorities. Digital LJ, 1, 24.
12. Smith, D. M., Heindl, W. A., & Swank, J. H. (2002). Two different long-term behaviors in black hole candidates: Evidence for two accretion flows?. The Astrophysical Journal, 569(1), 362.
13. Strupczewski, G. (2021). Defining cyber risk. Safety science, 135, 105143.
14. Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67, 101734.
15. Wang, A. (2020). Cyber sovereignty at its boldest: A Chinese perspective. Ohio St. Tech. LJ, 16, 395.