المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الخامس عشر شهر (8) 2019
www.eimj.org

# COPYRIGHT AND INTERNET LAWS IN SAUDI ARABIA " THE NEED OF IMPROVEMENT "

By: Dr. Hussain Agil
Assesstant professor
Jazan University
School of Sharia and Law
Jazan 2019
Email: h_n_aqil@hotmail.com

**Abstract**

The existence and implementation of copyright and cybercrime law in Saudi Arabia is a fairly recent matter. The research study purposed to identify the current state of legislation concerning copyright and cybercrime-related activities to gain a perspective of the current level of protection that is offered, as well as existing vulnerabilities and how to mitigate them. The research study was conducted through a thorough review of existing legislation of copyright and cybercrime as well as a review of existing literature. The findings of the review indicated that although the legislation in the Kingdom of Saudi Arabia, concerning cybercrime and copyright, agreed to some international standards, the local laws did not provide full protection of victims of related crimes. Some of the vulnerabilities that were identified include the lack of legislation that fully protects one from identity theft and application of internationally agreed-upon laws was often lacking insignificance. The recommendations made therein were for the update of existing laws to include more stringent legal action to be taken against perpetrators of copyright infringement and cybercrime activities.

## Introduction

The Kingdom of Saudi Arabia, known as the KSA, is the largest country by geographical size in the Arabian Peninsula. Saudi Arabia is located in the southwest corner of Asia and at the crossroads of Europe, Africa, and Asia. The history of internet and copyright law in Saudi Arabia is fairly recent. However, in the last decade, KSA has been able to agree to some international law standards concerning copyright and cybercrime laws, on their application in a local matter. Nevertheless, the current legislation on cybercrime and copyright in KSA offers little protection to internet users and intellectual property owners from both local and foreign jurisdictions. The following paragraphs will prove to show the current status of KSA copyright and cybercrime laws, the level of protection they offer, as well as areas of existing vulnerabilities and how to deal with such weaknesses in current legislation.

## Research Questions

- What is the current state of legal protection, according to cybercrime and copyright laws in Saudi Arabia?
- Does the current state of legal protection according to cybercrime and copyright laws in Saudi Arabia adequate in dealing with related crimes, or does it need to be improved?

## History of Internet Use in Saudi Arabia

The internet has been a source of vulnerability for any developed or developing country when it comes to cybercrime opportunities it presents with. In Saudi Arabia, the internet has a fairly young history that officially commenced in the year 19997 when internet service became available to the citizens of KSA. Since then, a period spanning over two decades, the internet has been integral in the growth of the Saudi economy and society in different aspects. According to an annual report that was prepared by the Communication and Information Technology Commotion (CITC) of KSA in the year 2016, there was a significant increase in internet access in the country from 47% to 74.9% from 2011 to the end of 2016 respectively[1].

[1] Zayid, Elrasheed Ismail Mohommoud, and Nadir Abdelrahman Ahmed Farah. "A study on cybercrime awareness test in Saudi Arabia-Alnamas region." In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 199-202. IEEE, 2017.

The country's population is estimated at 3 million, and the estimated number of internet users estimated at 24 million people, shows that at least 75% of the total population has internet access. The CITC report of 2016 also indicates that due to the growth of the use of internet platforms and applications such as social media and internet-based games, the demand for broadband and internet services has acutely increased[2]. The report further indicates that the use of the internet and ICT relates services in the country is expected to grow at a greater momentum than witnessed in recent years. As such, the report states that information security will become an essential need for to75% of the total population of KSA that access internet services on a regular basis.

The digital transformation strategy for the Kingdom of Saudi Arabia lists information security and cybersecurity as some of the components that will be integral to the development of the use of internet-based services in the country. The strategy comes at a time when KSA is witnessing the rise in the number of companies that are interested in the implementation of proactive and advanced information security solution[3]. This, in addition to the increasing capacity for international internet connectivity, creates a significant issue that is brought about by the steady increase in the demand for internet use within KSA.

## History of Intellectual Property Rights in Saudi Arabia

Unlike the history of internet users in the country, copyright law in Saudi Arabia has a fairly young history. The participation of KSA in intellectual property law at the international level is also quite recent. In the past, prior to the beginning of the 1st century, countries did not appreciate the importance of copyright law and its substantial impact on the national economies[4].

[2] Zayid, Elrasheed Ismail Mohommoud, and Nadir Abdelrahman Ahmed Farah. "A study on cybercrime awareness test in Saudi Arabia-Alnamas region." In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 199-202. IEEE, 2017.
[3] Ibis.
[4] Syed, Abdul Malik, and M. M. Sulphey. "Patterns of Intellectual Capital in Saudi Arabian Banking Industry." *Available at SSRN 3067157* (2017).

The majority of developed and developing countries did not have a solid legal framework that could appropriately respond to the changing trends and patterns in copyright law[5]. As such, a negative impact has been witnessed in developmental impacts that could have benefited the economies provided that they had not been exploited by the reigning governments. Research shows that the general influence on the development of intellectual property laws in the Gulf Cooperation Council was from external parties and societies and increasing pressures from other developed countries to enable protection of copyrightable products that had found a lucrative market overseas[6].

The external international influence for the development of comprehensive legal frameworks on copyright was necessitated from the increasing need to protect intellectual property rights in the global community in regard to the advancing use of technological operations that were shaping globalization through increased communication and reorganization the global economy. The history of intellectual property law in the KSA is therefore fairly recent given that KSA joined the Berne Copyright and Paris Industrial property Conventions on March 2004, and the WTO on December 2005[7]. The history of KSA cooperation on internationally enforceable copyright law has a history of fewer than two decades for a country that is significantly developed in the Middle-East region.

The KSA boasts of four main intellectual property laws that were enacted within the last two decades.

---

[5] Jones, Andrew, Fahad Alanazi, and Catherine Menon. "Sharia Law and Digital Forensics in Saudi Arabia." *Journal of Digital Forensics, Security and Law* 13, no. 3 (2018): 5.

[6] Alabdulkarim, Abdulrahman. "Intellectual Property Rights in the Kingdom of Saudi Arabia In Light of Sharia and the TRIPS Agreement." (2017).

[7] World Trade Organization. "Copyright Law-Saudi Arabia." In *Copyright Law, World Trade Organization TRIPS Agreement.* 2003. Retrieved from: https://www.wto.org/english/thewto_e/acc_e/sau_e/WTACCSAU56_LEG_4.pdf

These laws include the Law of Patents: Layout designs of integrated circuits, industrial designs and plant varieties, Law of Tradenames 2010, the Law of trademarks 2002 and the copyright law 2003[8]. Furthermore, the constitutional framework of the KSA contains 17 intellectual property related laws and implementing regulations and rules totaling 21 in number. In this perspective, intellectual property law in the KSA is recent and has undergone insignificant development in structure within the last decade. The local copyright laws are, however, structured in accordance with the legal framework provided by the WTO's international agreement on Trade-Related Aspects of Intellectual Property rights (TRIPS)[9]. The conformation of KSA local copyright law to the WTO international agreement on the same depicted the country's ascension to the WTO. The focus on the history of KSA copyright and by extension intellectual property law is young and cannot be depicted as a well-developed and structured legal framework that is based upon years of dealing with intellectual property cases of legal nature.

**Current State of Cyber Security in Saudi Arabia**

The current state of cybersecurity in KSA is alarming. KSA's National Cyber Security Center (NCSC) reported a threat overview of Saudi Arabia from the period starting 1st of July 2017 to the 30th of September 2017, which is the third quarter of the year 2017. The threat overview depicted that the NCSC responded to a total of 34 significant incidents of cybercrime. Within the same threat overview period, the NCSC realized 113 relevant threat alerts that instigated their action with the support of the Indicator of Compromise (IoC's) and created proper mitigation plans for the rest of the year (NCSC, 2017).

The current composition of cybersecurity threats in the KSA was as follows.

[8] Price, David, and Alhanoof AlDebasi. "'The golden thread that binds'–the Shariah and intellectual property protection." In *Protecting Intellectual Property in the Arabian Peninsula*, pp. 35-55. Routledge, 2017.

[9] Price, David, and Alhanoof AlDebasi. "TRIPS and intellectual property enforcement." In *Protecting Intellectual Property in the Arabian Peninsula*, pp. 198-224. Routledge, 2017.

The majority of the threat alerts were represented by intrusion and intrusion attempts, which accounted for 59% of the threats that were received for the threat overview period that was analyzed by the NCSC. The second most significant cybersecurity threat was malicious code, which accounted for at least 19% of the total threats encountered by the NCSC. Intrusion and instruction attempts in cybercrime are mostly known for the attempt to exploit the vulnerabilities of a computer information system or network that is either public or private. The majority of intrusions are conducted through brute force, privileged account compromise, network attack signature, unprivileged account compromise, remote command executions, application attacks, and remote access tools.

Malicious code is mostly used in cybercrime in the form of a software that is developed for the sole purpose of running malicious commands in the system to undertake different actions that benefit the attacker. Various forms of malicious code include a virus, worms, and Trojan horse software. The NCSC report indicated that the majority of threat alert that had been encountered during the threat overview period had been directed to the government and its organizations and agencies[10]. The threat to affiliated government entities accounted for 65% of the total threat alerts.

The next important sectors of the KSA economy were the energy and the telecommunications sectors, which accounted for 8%, and 7% of the threat alerts responded to respectively[11]. The high amount of threats that were directed to the KSA government are alluded to be caused by the geopolitical position of the nation. Furthermore, the two sectors of the economy are the most lucrative and important in the national economy,

[10] Alshammari, Tareq Saeed, and Harman Preet Singh. "Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index." *Archives of Business Research* 6, no. 12, (2018).

[11] Alotaibi, Faisal, Steven Furnell, Ingo Stengel, and Maria Papadaki. "A survey of cyber-security awareness in Saudi Arabia." In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 154-158. IEEE, 2016.

thereby suggesting that attackers would have gained significant leverage if attacks to the sectors were deemed successful.

According to an NCSC report for he threat overview period for the last quarter of 2017 (from 1st October to 31st December), the threat alerts increased significantly by 7%, in comparison to the previous quarter. The report indicated that Modification, Usage and Unauthorized access of computer information systems and computer networks, as well as malicious code comprised of the significant majority of threat, alters that were responded to the by the NCSC incident response team. However, there was witnessed a significant decrease in intrusion and intrusion attempts in the last quarter of 2017. Nonetheless, malicious code and Unauthorized Access, Modification, and Use were depicted to have witnessed a significant increase in the threat landscape of KSA. The increase that was witnessed in the two categories of threat alerts mentioned above shows that there were a number of attackers that were successful in gaining access to vulnerable and affected systems during the fourth quarter of the year 2017.

The threat composition in KSA's national economy was stagnant as the priority of the cybersecurity threats was identified as the government, Energy sector, and telecommunications sector in that order. The above depicts a significant influence in the actors of cybercrimes in controlling or impacting the national economy. Nonetheless, the threat overview report for the last quarter of the year indicated that there was witnessed a significant drop in the threat alerts that were focused on the government and its affiliated agencies, while a significant increase was witnessed in the energy and telecommunications sectors. The above change in the composition of the targets and focus of cybersecurity attacks depicts that actors of such crimes have been focused on impacting the KSA economy on a significant level.

The reality of the situation is far from becoming better as recent reports of threat overviews after 2017 indicate a significant increase in the threat alerts directed to the energy and telecommunication sectors.

The geopolitical position of the KSA with its neighbors in the larger Middle East region makes it a significant target of terrorist attacks through cybercrime that works to cripple the national economy[12]. In addition to the increased use of computer networks and use of computers by the KS population for economic and social purposes, the steady increase of cybersecurity crimes is expected to go into the future regardless of the significant efforts that are undertaken by the government and private security experts in the country.

Of significance in KSA economy and the global economy is the increasing dependence on technologies that require internet use and the increased reliance by business entities on internet applications such as the cloud and the Internet of Things (IoT) for business purposes. The threat landscape for KSA is steadily increasing, making it a necessity for the country to respond in a proactive manner to keep up with the changing patterns and trends of technology and internet use. The application of appropriate, advanced and up-to-date defense measures and the provision of guidance and technology to protect information sources and assets crucial to the government and the national economy is an ever-rising strategic need for boosting cybersecurity in the country[13].

The government is working extensively and relentlessly in the fight against cybercrime to enable the protection and safeguarding of the integrity, confidentiality, and the availability of critical national assets and infrastructure connected to the internet. One of the ways in which the government seeks to do this is by legislation. However, a look at the current legislation concerning cybercrime in the KSA depicts significant weaknesses that need to be dealt with in the near future to enable the country to achieve its vision 2030 of enabling better information sharing and protection of data and privacy through the provisions provided for in clear legal frameworks regarding privacy and data security in the country.

[12] Al Amro, Sulaiman. "Cybercrime in Saudi Arabia: fact or fiction?." *International Journal of Computer Science Issues (IJCSI)* 14, no. 2 (2017): 36.
[13] Ibis.

**Current State of Intellectual Property Rights in Saudi Arabia 500**

The cost of online piracy is significantly increasing year after year. The majority of companies whose business relies on the protection of intellectual property suffer significant losses as has been the case with local and international companies based and operating in KSA. As of the year 2018, the cost of piracy has steadily risen to a staggering number of billions, which represented a daunting figure. Nonetheless, the loss of revenue is not appreciated as a negative impact of business in intellectual property but rather a matter of improved and unsolicited market. Owners of products that are copyrighted agree that having their work pirated has a positive impact on their future business as it works to create customers in the future as long as the work is being of use to an individual.

Companies such as Microsoft, whose owner and founder Bill Gates has acknowledged the benefit of having one's work pirated make significant losses amounting to billions of dollars. In the view of such companies, the loss of present revenue sources will be compensated in future revenue earned to a steady increase in loyal customers[14]. However, the reality is not so tender on companies in the KSA that are still in the infancy stage as piracy significantly hurts the business prospects of growth and development in the future due to lack of substantial revenue to run the business in the present. Taking a deeper look at the intellectual property economy in KSA, the United States Department of State has indicated that between the years 1999 to 2011, companies operating in Saudi have lost close to 10 billion US dollars in revenue due to piracy of their products.

The staggering amounts of losses that have been made in Saudi Arabian companies due to piracy show an increasing lack of capability of the government to effectively undertake the protection of intellectual property rights. The findings by the US Department of State and other internationally recognized bodies necessitated that KSA is placed on the USTR priority list following the recommendation of the International Intellectual Property Rights Alliance.

[14] Aljabre, Abdulaziz. "Understanding Software Piracy in Saudi Arabia and the Need for Change." *Journal of Emerging Trends in Computing and Information Sciences* 3, no. 11 (2012): 1516-1520.

The resulting situation after the KSA has not been better as the cost and demand for pirated products keeps on increasing depicting a lucrative business economy based on piracy. The listing of KSA on USTR's priority list depicts an increasing need for the country to critically reflect upon the existing legal framework of intellectual property rights as well as the cultural opinion on the same and work towards changing the environment in which creators provide their products and gain access to the market, with a measure of guarantee in the protection of their intellectual property

**Current Legislation on Cybercrime and Intellectual Property**

According to the report on the threat overview conducted by the CITC (2016), the Kingdom of Saudi Arabia is facing an increasing amount of cybercrime incidents. The necessity of cybersecurity has never been crucial to the survival of the country's economy. Saudi Arabia's current law on cybercrime is depictive on the significant aspects that internet use and how to protect people from being vulnerable to criminal activities. The nature of cybercrimes has ever been increasing, making it extremely difficult to draft legislation that will respond to each of them. In this perspective, it becomes paramount that the laws that are drafted and implemented take act as an umbrella cover against the broad scope of cybercrime in Saudi Arabia. As such, cybercrime laws ought to cover the following broad areas:

- Data interception-legislation ought to prohibit the intentional interception of computer data that is being transported for non-public use without any prior authorization being provided. By intercepting transmissions of computer data, the communication channels lose confidentiality as well as the individuals lose trust in the communications channel.
- Data interference-legislation should prohibit anyone from intentionally deleting, damaging, degrading, and altering or suppress another individual's computer data without authorization. The act of data interference includes using malicious code to delete or change the nature of computer data in another person's computer so that it either becomes useless or unusable to the individual.

- System interference-legislation on cybercrime should be able to prohibit an individual from doing the following, input, delete, damage, deteriorate, suppress or alter data in another individual's computer without prior authorization or right. This involves anyone who causes serious hindrance of use of the computer system without right.
- Illegal access-the legislation on cybercrime ought to prohibit one from intentionally accessing another's computer system without having been given the rights or authorization to do so. In the perspective of cyberspace, it is the equivalent of trespassing on another person's property.

The list above forms the basis upon which all legislation of cybercrime to be drafted. The four points above cover the entire scope on which cybercrime activities are based. Saudi's current legislation status on cybercrime has been in existence since 2007 and has not changed much from that time. As such, the perspective of scholars is that the majority of the crimes in scope and perspective have not been covered or included therein creating a legal loophole that allows cybercriminals to get away with their activities from time to time as the judicial process fails to hold them accountable. The following depicts the current state of the cybercrime-related laws in the kingdom of Saudi Arabia:

- Prevention of data interception – According to Article 3 (1) of the Saudi Arabia Cyber Crime Law, the act of spying, reception or interception of data transmitted through a computer system or information network without prior legitimate authorization substantiates a cybercrime[15]. According to Article 3(1), the punishment for being found guilty of this offense is imprisonment for a period of not less than a year and a fine that does not exceed five hundred thousand Saudi Riyals or either punishment.

[15] CITC. "Cyber-Crime Law." In *the Cyber Crimes Act.* 2007. Retrieved from: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx

- Prevention of data interference – article 3(3) of the Saudi Cyber Crime law states that the intentional hacking of a website for the purpose of changing its layout, design, or URL substantiates a cybercrime. According to Article 3(1), the punishment for being found guilty of this offense is imprisonment for a period of not less than a year and a fine that does not exceed five hundred thousand Saudi Riyals or either punishment. In the same perspective, article 5(2) of the cybercrime law illegalizes the act of halting an information network, altering or leaking, deleting or damaging information contained therein as well as making any changes to stored programs[16]. The punishment for being found guilty of committing this offense is imprisonment for a period no more than four years as well as a fine that does not exceed three million Saudi riyals or either punishment.
- Prevention of system interference – Saudi cybercrime law as stated in Article 7(2) prohibits the unlawful or unauthorized access to an information system that involves the intention of obtaining computer data for the sole purposes of jeopardizing external or internal security of the national economy or the state[17]. As per the provisions laid out in Article 7(2) of the Saudi cybercrime law, the punishment for being found guilty of this act or crime is imprisonment for a period that does not exceed ten years and a fine that does not go beyond five million Saudi riyals or punishment.
- Prevention of illegal access – this is one of the laws that is covered by a significant number of Articles pertaining to Saudi Arabia's cybercrime law. Article 3(2) prohibits anyone from unlawfully accessing computers with the intention of blackmailing or threatening any person and compelling them to refrain or take any action. The Article stipulates the punishment for someone that has been found guilty of this offense to be imprisoned for a period that does not exceed one year as well as a fine that does not exceed five hundred thousand Saudi riyals and punishment.

[16] Ibis.
[17] CITC. "Cyber-Crime Law." In *the Cyber Crimes Act.* 2007. Retrieved from: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx

Article 4(2) of the Saudi Arabia Cybercrime law states that the illegal access of credit or bank information or data pertaining to the ownership of securities to obtain information, data, services or funds is a perceived as a cybercrime[18]. The Article points out that any person that is found guilty of committing the crime is subject to imprisonment for a period not exceeding three years and a fine that does not exceed two million Saudi riyals or either punishment. Lastly, Article 5(1) of Saudi Arabia's cybercrime law illegalizes the act of gaining unlawful access to another person's computer, destroying, leaking, altering distributing, or damaging private data[19]. According to Article 5(1), the state punishment for an individual found guilty of the offense is punishment for a period that does not exceed four years as well as a fine that does not go beyond three million Saudi Riyals.

- Prevention of invasion of privacy – KSA's cybercrime and related laws depict the invasion of privacy through the misuse of camera-equipped mobile phones and other technological equipment as a cybercrime. According to Article 3(4), the state punishment for an individual found guilty of the above crime is imprisonment for a period of not less than a year and a fine that does not exceed five hundred thousand Saudi Riyals or either punishment.
- Prevention of cyber terrorism – Saudi Arabia's cybercrime and related laws prohibit the construction of a website for the purpose of facilitating communication amongst members of a terrorist organization, promoting their ideologies or financing of terrorist activities. Article 7(1) states the punishment for an individual found guilty of the above is imprisonment for a period that does not exceed ten years and a fine that does not go beyond five million Saudi riyals or punishment[20].

[18] Ibis.
[19] CITC. "Cyber-Crime Law." In the *Cyber Crimes Act.* 2007. Retrieved from: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx
[20] Ibis.

- Prevention of attempt to commit cyber-crime – Any individual within the jurisdictional boundaries of the KSA government, who attempts to commit any type of cybercrime shall be subject to punishment that does not exceed half of the maximum punishment that is designated for the crime that was to be committed. In this perspective, the law prevents the attempt to commit crimes even if they are deemed to be unsuccessful.
- Investigation and prosecution bodies – Article 15 directs that the investigation and prosecution of cybercrimes be conducted by the Bureau of Investigation and Public Prosecution while article 14 of Saudi ACCL states that the CITC will provide undue assistance and support to the competent security agencies for the purposes of investigating and prosecuting cybercrimes[21].

The above depicts the state of legislation that is bound to prevent the occurrence of any type of cybercrime in Saudi Arabia. Consequently, the copyright law that governs intellectual property matters in Saudi Arabia is focused in the following manner. Protected works are covered in Article 2, author' moral rights in article 8, author's financial rights in article 9, mandatory licenses for copyrighted works in article 16, exceptions pertaining to the lawful use of works that have been copyrighted in article 15, duration of protection in article 19, scope of protection in article 18, penalties in article 2 and the provisions of infringements in article 21[22]. The above provides the legal framework within which intellectual property cases and crimes are investigated and prosecuted in Saudi Arabia.

[21] CITC. "Cyber-Crime Law." In *the Cyber Crimes Act.* 2007. Retrieved from: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx
[22] KACST. "Law of Patents, Layout Designs of Integrated Circuits, Plant Varieties, and Industrial Designs." 2007. Retrieved from: https://www.kacst.edu.sa/eng/IndustInnov/SPO/Regulations/Patents,%20Layout%20Designs%20of%20Integrated%20Circuits,%20Plant%20Varieties%20,%20and%20Industrial%20Design.pdf

It is evident upon looking at the specific articles pertaining to copyright law in Saudi Arabia that KSA Copyright Law and the implementing regulations show a significant measure of willingness to comply to internationally set standards of intellectual property protection that have been enshrined in TRIPS Agreement[23]. Recently, Saudi Arabia established a new authority known as SAIP (Saudi Authority for Intellectual Property. SAIP was established for the purpose of consolidating the different departments of IP protection under one umbrella body[24]. The establishment of SAIP depicts an increased willingness of the national strategy in fighting theft of intellectual property and the subsequent provision of IP products and entities in a high-quality and timely manner to those in need. The country's focus in increase IP marketing and awareness for all stakeholders and coordination of enforcement efforts with other departments and ministries illustrates a renewed effort in the fight against theft of intellectual property.

**Recommendations for Improvement of Legal Protection**

In respect to the existing state laws that cover cybercrime and related criminal activities in Saudi Arabia, significant improvement needs to be conducted. A deep look into the existing legislation shows significant vulnerabilities that ought to be removed to enable the country to properly carry out prosecution of criminal activities without providing criminals with loopholes to evade the justice system. One of the significant vulnerabilities that exist is that existing legislation limits criminalization to the act of obtaining financial data, information, or services. This pertains to identity theft for financial purposes[25]. However, the law does not detail the criminalization of identity theft for non-financial motivations,

[23] Birnhack, Michael, and Amir H. Khoury. "The Emergence and Development of Intellectual Property Law in the Middle East." *The Oxford Handbook of Intellectual Property Law (2016 Forthcoming)* (2016).

[24] Alkhalaf, Abdulrahman Abdullah. "Reforming Saudi Arabian Intellectual Property Law." Ph.D. diss., 2018.

[25] Alabdulatif, Afnan. "Cybercrime and Analysis of Laws in the Kingdom of Saudi Arabia." Ph.D. diss., 2018.

which enables one to tarnish the image of another person through stealing their identity and using it inappropriately without being held legally liable[26].

Another significant oversight of Saudi law is the lack of defining neither the term personal data nor data controller, which makes the provisions that protect the privacy of data from being inadequate. Furthermore, Saudi laws do not entail any legislation that is related to the acts of aiding and abetting to commit cybercrimes as well as cyberbullying. Lastly, the existing legislation does not define the criminalization of possessing or transferring data and programs that might be used for the purpose of identity theft. The lack of these provisions in current legislation makes prosecutors unable to charge certain individuals with the pertinent cybercrimes. Significant changes need to be made to the above vulnerabilities by drafting legislation that includes the above types of cybercrime that are not yet recognized under current legislation.

Apart from cybercrimes, current copyright legislation is extremely lacking in that it does not prevent the sharing of copyrighted works for non-economic purposes. The above creates a significant loophole in which copyrighted works may be freely shared within a society without any legal action being taken against the perpetrators[27]. Furthermore, copyright law in Saudi dictates that foreign copyright standards from other countries do not directly apply to it unless they are entailed in accepted international standards of intellectual property protection. The legislation ought to be changed to take into consideration the foreign laws in as far as protection of foreign copyrighted works sold in the country is involved.

[26] CITC. "Electronic Transactions Law." In Electronic Transactions Law. 2007. Retrieved from: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx

[27] Israel, Jordan, and Syria Saudi Arabia. "A STUDY OF THE EFFECTIVENESS OF NATIONAL INTELLECTUAL CAPITAL USE IN THE MIDDLE EAST ECONOMIES." *Рекомендовано до друку на засіданні Вченої ради Харківського національного економічного університету ім. С. Кузнеця, протокол № 8 від 3 травня 2018 р.* (2018): 192.

Changes to the significant vulnerabilities mentioned above in both cybercrime law and copyright law will enable the responsible security agencies to prevent cybercrime and theft of intellectual property in an efficient manner.

## Conclusion

The current state of copyright and cybercrime laws in Saudi Arabia are lacking in judicial implementation as they leave a lot of room for undefined crimes that enable criminals to get away from the justice system. The analysis of current legal provisions for both copyright and cybercrime law in Saudi Arabia has depicted the existing vulnerabilities and improvements that need to be done for the laws to be effective. Furthermore, there is a need for Saudi Arabia to contend to international standards of cybercrime and copyright laws to ensure local jurisprudence does not restrict international law from being implemented in business that deals within the global economy, that are affected by related crimes.

**References**

Alabdulkarim, Abdulrahman. "Intellectual Property Rights in the Kingdom of Saudi Arabia In Light of Sharia and the TRIPS Agreement." (2017).

Alabdulatif, Afnan. "Cybercrime and Analysis of Laws in Kingdom of Saudi Arabia." Ph.D. diss., 2018.

Aljabre, Abdulaziz. "Understanding Software Piracy in Saudi Arabia and the Need for Change." *Journal of Emerging Trends in Computing and Information Sciences* 3, no. 11 (2012): 1516-1520.

Alkhalaf, Abdulrahman Abdullah. "Reforming Saudi Arabian Intellectual Property Law." Ph.D. diss., 2018.

Alotaibi, Faisal, Steven Furnell, Ingo Stengel, and Maria Papadaki. "A survey of cyber-security awareness in Saudi Arabia." In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 154-158. IEEE, 2016.

Alshammari, Tareq Saeed, and Harman Preet Singh. "Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index." *Archives of Business Research* 6, no. 12, (2018).

Al Amro, Sulaiman. "Cybercrime in Saudi Arabia: fact or fiction?." *International Journal of Computer Science Issues (IJCSI)* 14, no. 2 (2017): 36.

Birnhack, Michael, and Amir H. Khoury. "The Emergence and Development of Intellectual Property Law in the Middle East." *The Oxford Handbook of Intellectual Property Law (2016 Forthcoming)* (2016).

CITC. "Cyber-Crime Law." In *Cyber Crimes Act.* 2007. Retrieved from: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx

CITC. "Electronic Transactions Law." In Electronic Transactions Law. 2007. Retrieved from: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx

Israel, Jordan, and Syria Saudi Arabia. "A STUDY OF THE EFFECTIVENESS OF NATIONAL INTELLECTUAL CAPITAL USE IN THE MIDDLE EAST

ECONOMIES." *Рекомендовано до друку на засіданні Вченої ради Харківського національного економічного університету ім. С. Кузнеця, протокол № 8 від 3 травня 2018 р.* (2018): 192.

Jones, Andrew, Fahad Alanazi, and Catherine Menon. "Sharia Law and Digital Forensics in Saudi Arabia." *Journal of Digital Forensics, Security and Law* 13, no. 3 (2018): 5.

KACST. "Law of Patents, Layout Designs of Integrated Circuits, Plant Varieties, and Industrial Designs." 2007. Retrieved from: https://www.kacst.edu.sa/eng/IndustInnov/SPO/Regulations/Patents,%20Layout%20Designs%20of%20Integrated%20Circuits,%20Plant%20Varieties%20,%20and%20Industrial%20Design.pdf

Price, David, and Alhanoof AlDebasi. "TRIPS and intellectual property enforcement." In *Protecting Intellectual Property in the Arabian Peninsula*, pp. 198-224. Routledge, 2017.

Price, David, and Alhanoof AlDebasi. "'The golden thread that binds'–the Shariah and intellectual property protection." In *Protecting Intellectual Property in the Arabian Peninsula*, pp. 35-55. Routledge, 2017.

Syed, Abdul Malik, and M. M. Sulphey. "Patterns of Intellectual Capital in Saudi Arabian Banking Industry." *Available at SSRN 3067157* (2017).

World Trade Organization. "Copyright Law-Saudi Arabia." In *Copyright Law, World Trade Organization TRIPS Agreement.* 2003. Retrieved from: https://www.wto.org/english/thewto_e/acc_e/sau_e/WTACCSAU56_LEG_4.pdf

Zayid, Elrasheed Ismail Mohommoud, and Nadir Abdelrahman Ahmed Farah. "A study on cybercrime awareness test in Saudi Arabia-Alnamas region." In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, pp. 199-202. IEEE, 2017.