Application of Legal Realism in The Criminalisation of Computer Crimes in Malaysia and Singapore

Ani Munirah Mohamad[1*], Nurhazman Abdul Aziz[2], Zaiton Hamin[3], Mohd Zakhiri Md Nor[4]

[1]School of Law and Center for Testing, Measurement and Appraisal (CeTMA), Universiti Utara Malaysia, 06010 Sintok, Kedah, MALAYSIA
[2]School of Communication & Management, Republic Polytechnic, 738964, SINGAPORE
[3]Faculty of Law, Universiti Teknologi MARA, 50450 Shah Alam, Selangor, MALAYSIA
[4]School of Law and Institute for Management & Business Research (IMBRe), Universiti Utara Malaysia, 06010 Sintok, Kedah, MALAYSIA

**Corresponding author: animunirah@uum.edu.my*

Abstract

Legal realism is a reactionary movement against formalism in which the latter emphasises the application of legal provisions over the real problems in issue and disregards added values in the community. In contrast, realism emphasises the added-legal aspects, such as emotions, psychological values as well as the behaviour of the accused persons in arriving at a conclusion. Scarcity of past researches on the application of legal realism in the context of criminalisation of computer crimes in Malaysia and Singapore have motivated this study. While engaging in librarybased legal research, this study aims to demonstrate the application of legal realism in the criminalisation of computer crimes within the ambit of Malaysia's Computer Crimes Act 1997 and Singapore's Computer Misuse Act 1993. Past court decisions are analysed to illustrate the criminalisation of computer crimes given legal realism. The study found that computer crimes are criminalised 'as they are' as opposed to the actual legal provisions 'as to how they are imagined' or 'prescribed'. Hopefully, this study would shed light into the understanding of computer crimes, and how the cases are adjudged in the courts of law.

Keywords: Legal realism, realism theory, computer crimes, computer misuse, cybercrime, cybersecurity, cyberlaw

Introduction

There are various approaches in understanding the law and how the law works, such as naturalist, positivist and realist approaches. One of the commonly adopted at present is - the realist approach, also known as legal realism. It centralises upon the extra-legal factors in determining the law in action in the real world, rather than black letter law approach as to how the law is recorded in the legal textbooks and written rules. For instance, legal realism looks at the reality of a certain dispute between the disputing parties, as well as the court judgment with regards to the dispute, particularly how the matter is adjudged in the actual court of law, rather than by looking into the actual legal provision of the written rules. In essence, legal realists believe that how the law is being implemented in the real world is how the real law is. This is where the term "realism" actually originates, that is the reality of things, instead of what is expected to be applied (Priel, 2019; Olsen & Toddington, 2017).

Within the context of computer crimes in Malaysia, an action is ruled as "a crime" or "an offence" if it falls into any of the offences provided in the "Computer Crimes Act 1997" (hereinafter CCA 1997), one of the cyber law legislation introduced by the Parliament of Malaysia to regulate the digital and multimedia framework in Malaysia. Likewise, within the context of Singapore, the Computer Misuse Act 1993 (hereinafter CMA 1993) regulates the criminalisation of computer-related offences as both have some similarity that allows the studies to be observed and will be discussed in this paper.

Nevertheless, the limited number of court cases to adjudge computer crimes gives rise to the implementation issues of legal realism among the court cases. Following the shortage of funds on legal realism in Malaysia and Singapore, coupled with the limited number of court cases involving the CCA 1997 and CMA 1993, it is farfetched to conclude whether legal realism is implemented in the criminalisation of computer crimes in both Malaysia and Singapore. This paper attempts to examine the key research question of: ***How does legal realism***

apply in the criminalisation of computer crimes in Malaysia and Singapore? Accordingly, this paper intends to **prove the application of legal realism in the criminalisation of computer crimes in Malaysia and Singapore**. There are four primary parts in this paper. First, the review of the literature on the main ideas of the work are presented, covering the theoretical aspect of legal realism and computer crimes. The following section (or the second section) presents the legal position of computer-related crimes in Malaysia and Singapore, followed by the findings by demonstrating the application of legal realism in six case studies involving the criminalisation of computer crimes in the respective jurisdictions contributed to the third section. The final section (the forth section) concludes the discussion and proposes a direction for future research.

Literature Review

This part (first section) gives a description of the literature review of the two main ideas used in the research, being (1) legal realism and (2) computer crimes.

Legal Realism

Legal realism is a reactionary movement against formalism, which the latter emphasises on the application of law over problems, without regard to other values of the society (Dagan and Kreitner, 2018). For instance, when confronted with a certain legal problem, such as theft, formalists stress upon the legal provision for the criminalisation of the offence and the punishment thereof, being the Penal Code. However, legal realists stress upon how the crime is decided by a judge in a court of law. For realists, they look at the law as to how it is carried out in reality and considers the extra-legal factors, rather than how it is legally provided under the law (Spaak, 2018). Realism advocates want to understand how the law is actually in process.

Additionally, Friedman (1975) believed that the realists like to assess any aspect of the law "in terms of its effects". That essentially means how the law is practised in the real world, rather than in the black letter law as provided by the rules. Further, several works of literature also suggested that realists believe that there can be no certainty about law as in the written rules, and Its predictability is based on the collection of facts presented for review by the court (Fittipaldi, 2016; Shaffer, 2015). In this regard, realist advocates do not support a formal, rational, and conceptual approach to law since courts often make judgements based on feelings rather than logic when they are determining cases. Hence, judges as much influenced by psychology. They lay more significant stress on the psychological perspective to the right understanding of law as it relates to human behavior and the judgments of the attorneys and judges (Nardin, 2017).

Along the same line of discussion, they believe that the actual law is in the judicial precedents, and not in statutes. For example, if a crime provides for ten years imprisonment, but no court has ever awarded more than five years, then the actual law should be five years and not ten years. Essentially, in order to know the actual law, realists suggest that one should go to the court to see the real situation. This seems to be rightly so because, in the view of realists, the law is what the court has decided in respect of any particular set of facts prior to such a decision, the "*opinion of lawyers is only a guess as to what the court will decide, and this cannot be treated as law unless the Court so decides by its judicial pronouncement.*" (Frank, 2017)

Within the broader context, legal realism greatly contributes towards the development of the law, in the sense that the law is approached in a positive spirit and demonstrated the application of practical concepts of justice and natural law in the real world (Lang, 2015; Tamanaha, 2018). In addition, realists rationalise and modernise the law, upon which both the administration of the law and the material for legislative change would be achieved, by utilising the scientific method and considering the factual realities of social life.

Computer Crimes

Computer-related crimes, including physical damage to computer systems and stored data (Chawki et al., 2015), unauthorised use of computer systems and the manipulation of electronic data (Tivey and Pearson, 2015), internal and external hacking (Hu, Hart and Cooke, 2007), virus dissemination (Rieback, Crispo and Tanenbaum, 2005) and few other offences have been recognised as criminal offences in various parts of the world (Jaishankar, 2018). In all these situations, the offender would primarily engage in the use of computer systems or network in order to commit the crimes of physically damaging the computer or systems, or in some extreme cases, further led to damage to physical persons and properties, too (Jaishankar, 2007; Abdullah, Mohamad & Yunos, 2018; Crimewatch, 2019). Other offences which could potentially be committed in furtherance of the computer crimes usage of computer systems or networks for the purpose of stalking, bullying, pornography, theft of information or monies, or even more serious crimes such as money laundering, kidnapping, murder or rape (Martinu & McEwen, 2019; Kruisbergen, 2019).

The discussion found in the literature centrally focuses on issues and threats coming from two types of persons, external or internal. The first type of person is the outside community of the organisations, or more commonly known as external hacking (Woo-Sik, Han and Lee, 2014). External hacking occurs where the intruder has no privileges on the objective network, and either gain connection from external of the network perimeter or evades or undermines the target's physical and (or) network security measures to attain some degree of access to the target's internal network. Examples of situations involving external hackers access through weak, stolen or lost credentials; access through the compromise of remote access system; access through modem dial-up or wireless system; and, unauthorised access with the co-operation of the organisation's member of staff (Holtfreter and Harrington, 2015).

Dissemination of virus into the computer network or system is another type of computer crime. A computer virus is a software that can attack other programs by altering them so that a copy of itself is included. Any application that seeks to conceal its destructive function and spread to as many computers as possible is included in this category (Tesauro, Kephart and Sorkin, 1996). In certain circumstances, the damage could cause a denial of service to the victims, defacement of governmental or private-owned websites, obscenity in the websites or computer programs, and other similar grave impacts (Rouse, 2017, Hamin, Othman & Mohamad, 2012).
Within the contexts of Malaysia and Singapore, specific computer-related crimes are criminalised pursuant to the CCA 1997 and CMA 1993, such as unauthorised access, unauthorised access with an ulterior motive, and unauthorised modification - detailed account of each type of crimes is discussed in the following section on the legal position of computer crimes in Malaysia and Singapore (Jayabalan, Ibrahim & Manaf, 2014; Urbas, 2008).

Criminalisation Of Computer Crimes In Malaysia And Singapore

The primary piece of legislation regulating computer crimes in Malaysia is the CCA 1997, while in Singapore is the CMA 1993 (as the second section). There are several offences provided under both statutes. However, this paper focuses on three types of offences only, being unauthorised access, unauthorised access with intent to facilitate the further offence, and unauthorised modification. Each of the offences is elaborated below in light of CCA 1997 in Malaysia and CMA 1993 in Singapore respectively.

Unauthorised Access To Computer Materials

The first offence criminalised under CCA 1997 is unapproved entry to computer materials, or usually referred to as "hacking" under Section 3. A person commits such a crime when they direct a computer to carry out any task with the goal of gaining unauthorized access to any data or program stored on a computer. He is aware of this as soon as he instructs the computer to carry out the desired function. On conviction, hacking is punishable under the Act with a fine not exceeding fifty thousand ringgit or imprisonment for a term not exceeding five years or both. Under this offence, the perpetrator could be accesing the computer without a person's authority such as gaining access to another person's computer to get information contained in the computer (Nazlina, 2018).
Similarly, within the context of Singapore, such an offence is provided under Section 3 of the CMA 1993. On conviction, unauthorised access is punishable under the Act with a fine not surpassing five thousand dollars or a maximum term of two years imprisonment or both, for the first conviction. Second and subsequent convictions for this offence would warrant a fine not exceeding ten thousand dollars or imprisonment for a term not exceeding three years or both. Additionally, section 3(2) of the CMA 1993 provides that if there is any damage caused entailing the commission of the offence, the accused shall be liable to a fine not exceeding fifty thousand dollars or imprisonment for a term not exceeding seven years or both. One situation which could illustrate this offence is the unauthorised access to the computer system committed by a police officer, for non-related works (Chong, 2017). In this situation, a police officer used his own credentials to access the computer network for the police to vet information relating to this girlfriend, which is a clear commission of the crime of unauthorised access of computer system within the definition of CMA 1993.
For the offence of unauthorised access to computer materials, the person committing the offence could be someone who initially had no authority to access the system, but still gains access to the system, knowing that he does not have the authority. Another situation is when a person initially has access to the system, or has the authority to access or operate using the computer system, but have exceeded the authority given to him (Saha, et al., 2019; Mohammed, Nawang & Mustaffa, 2019).

Unauthorised Access With Intent To Facilitate The Further Offence

Another offence criminalised under the CCA 1997 is unauthorised access with intent to commit or facilitate the commission of the further offence. Another terminology commonly used for this offence is the 'unauthorised access with ulterior motive'. On conviction, Section 4 of CCA 1997 provides that this offence is punishable with

a fine not exceeding one hundred and fifty thousand ringgit or imprisonment for a term not exceeding ten years or both. Under this offence, the perpetrator would commit unauthorised access, and subsequently he is intending to commit another crime. An example situation is when workers of a car service center for Perodua accessed the computer system of the employer without proper authority to create fake service appointments, which is also an offence (Lai, 2018).

Within the context of Singapore, this offence is provided under Section 4 of the CMA 1993. On conviction, the legal provision provides for a fine not exceeding fifty thousand dollars or imprisonment for a term not exceeding ten years or both. A situation came up when a graduate student of Singapore Management University used keylogger sticks to commit unauthorised access to the university's computer system. His aim was to commit academic dishonesty, when he proceeded to delete the examination scripts of his coursemates (Chong, 2016).

The offence of unauthorised access with intent to facilitate the further offence primarily centralises upon the gaining of access to the computer or computer system without authority or exceeding the initial authority possessed by the perpetrator, with the aim to commit another crime which is recognised under the law, such as theft, kidnapping or murder (Hutchings, 2014; Bell, 2002). This type of computer crime would involve another crime to be committed in furtherance of the unauthorised access to the computer systems or network. This essentially means that the perpetrator uses the computer system or network without proper authority or exceeds his authority in doing so, intending to commit another offences (Sagar, 2019; Mohamed, 2013)

Unauthorised Modification Of Computer Material

Unauthorized editing of any computer's data is addressed in Section 5 of the CCA 1997. A person is considered to have violated this section if they take any action that they know will result in an unauthorized modification of any computer's contents. Upon conviction for a violation of this section, a person is subject to a fine not to exceed 100,000 ringgit, a term of imprisonment not to exceed seven years, or both; or if the act is done with the intent to cause injury as defined by the Malaysian Penal Code, be subject to a fine not to exceed one hundred and fifty thousand ringgit or to imprisonment for a term not to exceed ten years, or to both. Modifications such as effecting changes to the online voting system during national elections is a straight forward situation of unauthorised modification within the meaning of this section. (Fazlul Haque, 2018). In this situation, an information technology expert had accessed into the online voting system and modified the contents of the voting, which is a crime under section 5 of the CCA 1997.

As for Singapore, the offence of unauthorised modification of computer material is provided under section 5 of the CMA 1993. On conviction, this offence is punishable under the Act with a fine not exceeding ten thousand dollars or imprisonment for a term not exceeding three years or both, for the first conviction. Second and subsequent convictions for this offence would warrant a fine not exceeding twenty thousand dollars or imprisonment for a term not exceeding five years or both. Additionally, section 5 (2) of the CMA 1993 provides that if there is any damage caused entailing the commission of the offence, the accused shall be liable to a fine not exceeding fifty thousand dollars or imprisonment for a term not exceeding seven years or both. Example situation of a case involving unauthorised modification is the use of modified ride-hailing application of Gojek in Singapore, which enabled the drivers to bypass verification, fake their location, cancel jobs without being penalised and, in some cases,view private customer information (Sun, 2020). This case is a clear example of unauthorised modification of the computer application, an action which is criminalised under the CMA 1993. This offence of unauthorised modification is an enhancement of the earlier two types of offences. If the earlier ones involve gaining access to computer or computer system without authority, or gaining such access with the intent to commit a further offence, Section 5 of both CCA 1997 and CMA 1993 primarily provide for effecting modification to the computer or computer system, while knowing that his act would cause such modification. Example situations are like acting without proper authority to change certain data in the spreadsheet or modify the algorithm in the computer system or applications (Worthy & Fanning, 2007; Bainbridge, 2007).
The following section demonstrates an analysis of the application of legal realism in the criminalisation of computer crimes in both Malaysia and Singapore.

Application Of Legal Realism In The Criminalisation Of Computer Crimes

This part demonstrates how legal realism applies in computer crimes cases which have been decided by the courts of law in Malaysia and Singapore. For illustration purposes, the following six cases are analysed, describing the brief facts of the case and court judgment. The first three cases were decided in the Malaysian courts, while the remaining three were decided in the Singaporean courts.

Basheer Ahmad Maula Sahul Hameed And Anor V Public Prosecutor [2016] 6 CLJ 422 (Kuala Lumpur High Court Of Malaysia)

In February 2014, a Malaysian Airlines (MAS) aeroplane went missing from the radar en route from Kuala Lumpur to China. The plane was reported missing, and the passengers and crew members were presumed dead. In May and June the same year, multiple withdrawals were made from the bank account of one of the passengers. Investigations by the authorities led to the discovery of the bank's member of staff and her husband. Both the wife and husband were charged under Section 4 of CCA 1997, which provides for unauthorised access with the intention to commit a further offence. It came to light that the couple has gained access to the bank account of the deceased with the intention to commit the act of theft of the monies therein.

Despite the prescribed maximum punishment for the offence under the CCA to be ten years imprisonment, or RM150,000 fine or both, the court sentenced the bank's staff to seven years imprisonment and RM70,000 fine. As for the husband, he was sentenced to six years of imprisonment and RM8,000 fine. The clear disparity between the prescribed punishment under the CCA 1997 and the actual sentence by the court only suggest that legal realism was actually implemented in this case.

Public Prosecutor V Roslan Mohamed Som [2016] 1 LNS 651 (Kuala Lumpur Sessions Court Of Malaysia)

In this case, the two accused persons were officers with the Tabung Haji Corporation, a government-linked organisation responsible for managing Malaysian pilgrims and pilgrimage activities in Mecca. They were charged with altering the database of pilgrims and accepting bribery in the course. This followed the strict registration and ordering of the pilgrimage of the Malaysian registrants for the performance of pilgrims then plaguing the entire community. Essentially, the accused modified the contents of the computer database of Tabung Haji by entering the names of 27 individuals into the list of pilgrims, at three occasions, primarily with the aim so that the individuals would be able to skip the waitlisting their turn for performing pilgrimage in Mecca. Upon completion of investigations, the two accused persons were slapped with three counts of charge under Section 5 of the CCA 1997 for the unauthorised modification of computer system.

Notwithstanding the maximum prescribed punishment under the CCA 1997 to be seven years imprisonment, or RM100,000 fine, or both, the actual sentence by the court was three years imprisonment and RM20,000 fine for each count. The imprisonment sentence would run concurrently for all three counts. As in the earlier case analysis, the reduced sentence by the court in this case, as opposed to the actual punishment prescribed by CCA 1997, centralises to the point that legal realism was in fact engaged in the criminalisation of this offence.

Kangaie Agilan Jammany V Public Prosecutor [2017] 1 LNS 1640 (Shah Alam High Court Of Malaysia)

The final case analysis, within the Malaysian context, involved the offence of unlawful modification of online flights reservation system the Air Asia, one of the famous low-cost carrier flight operators in Malaysia and South East Asia. A flight assistant with the Air Asia Commercial Department, the accused logged into the computer system and modified some data to such modification that allowed her family members and friends to get lower prices for their flight ticket reservations. In total, there were 148 charges against her. She was later charged with 148 counts under Section 5 of the CCA 1997 for the unauthorised modification of computer system.

Section 5 provides for the maximum punishment to be seven years imprisonment, or RM100,000 fine, or both. However, the accused was only sentenced to five years imprisonment for each count, and the imprisonment would run concurrently. This sentencing given by the court supports the application of the legal realism, particularly for the offence of unauthorised modification of computer system under Section 5 of the CCA 1997.

Public Prosecutor Vs Balasubramaniam [2013] SGDC 119 (District Court Of Singapore) In this first case analysis within the Singaporean context, the accused was a husband who ran into marriage issues with his wife. It happened that he held a few joint accounts with the wife, while at the same time, he knew that his wife also held a few joint accounts with her other family members. At a few occasions, the accused got hold of the wife's debit card and accessed her the card without her authority. In total, he made 67 withdrawals using the card. The total amount involved in the charge was SGD128,962.

Later the accused was charged with 67 counts under Section 3 of the CMA 1993 for unauthorised accessed of the debit card. Albeit the prescribed punishment for first conviction under the Act was two years imprisonment, or SGD5,000 fine, or both, he was slapped with 12 months imprisonment on each of the 67 counts, with the

imprisonment sentence to run consecutively. As in the Malaysian context, this present case also demonstrates the application of the legal realism theory in the criminalisation of computer crimes in Singapore.

Public Prosecutor Vs Navaseelan Balasingam [2006] SGDC 156 (District Court of Singapore)

In this case, the accused were found to have possessed cloned bank cards belonging to a few international bank account holders. With these cards, he proceeded to make illegal withdrawals from automated teller machines (ATMs). The unauthorised access was committed with intent to commit theft of monies of the bank account holders. The total amount involved in the charge was SGD54,380.

Consequently, he was charged with five counts under Section 4 of the CMA 1993 for the offence of unauthorised access with intent to commit a further offence. This Section provides for the maximum punishment of ten years imprisonment, or SGD50,000 fine, or both. Clear demonstration of the application of legal realism, in this case, was when the court sentenced the accused to only 18 months imprisonment on each count, with the sentence to run consecutively.

Public Prosecutor V. Muhammad Nuzaihan Bin Kamal Luddin [2000] 1 SLR 34 (HighCourtOf Singapore)

The final case analysis for the Singaporean context involved a 17-years old student, who was described by the judge as "intelligent and resourceful young man with true talent and potential". Out of his brilliance and intelligence, he managed to access multiple computer systems and modified the contents by reconfiguring the Cloud4 server. By doing that, he downloaded files from the cable network of Brahms.

He was later charged with three counts under Section 5 of the CMA 1993 for the offence of unauthorised modification of computer material. Notwithstanding the maximum punishment which had been prescribed for the offence of three years imprisonment, or SGD10,000 fine, or both, the accused was sentenced to two months imprisonment on each of the three counts, with the imprisonment sentence for to counts to run consecutively. What can be concluded from the analysis of the six cases above is that, despite the written rules of the CCA 1997 having prescribed the maximum punishment for the specific offences under Sections 3, 4 and 5 respectively, in reality, the court sentenced a much lower punishment than the prescribed rules. The same situation applies to the Singapore courts of law as well, upon which much lower punishment was sentenced than the prescribed rules of the CMA 1993. The following **Table 1** summarises the application of the legal realism theory into the criminalisation of computer crimes vide CCA 1997 and CMA 1993.

Table 1. Analysis of prescribed sentencing versus actual sentencing under Malaysia's CCA 1997 and Singapore's CMA 1993

Malaysia	*Basheer Ahmad Maula Sahul Hameed and Anor v Public Prosecutor* (Section 4 of CCA 1997)	Ten (10) years imprisonment, or RM150,000 fine, or both	Staff: Seven (7) years imprisonment and RM70,000 fine Husband: Six years imprisonment and RM8,000 fine	Applied
Malaysia	*Public Prosecutor v Roslan Mohamed Som* (Section 5 of CCA 1997)	Seven (7) years imprisonment, or RM100,000 fine, or both	Three (3) years imprisonment and RM20,000 fine (each count)	Applied
Malaysia	*Kangaie Agilan Jamanny v Public Prosecutor (Section 5 of CCA 1997)*	Seven (7) years imprisonment, orRM100,000 fine, or both	Five (5) years imprisonment (each count)	Applied
Singapore	*Public Prosecutor v Balasubramaniam* (Section 3 of CMA 1993)	(First conviction) Two (2) years imprisonment, or SGD 5,000 fine, or both	Twelve (12) months imprisonment (each count)	Applied

Singapore	*Public Prosecutor v Navaseelan Balasingam* (Section 4 of CMA 1993)	Ten (10) years imprisonment, or SGD 50,000 fine, or both	Eighteen (18) months imprisonment (each count)	Applied
Singapore	*Public Prosecutor v. Muhammad Nuzaihan bin Kamal Luddin (*Section 5 of CMA 1993)	(First conviction) Three (3) years imprisonment, or SGD 10,000 fine, or both	Two (2) months imprisonment (each count)	Applied

All six case analyses which have been discussed in this study pointed to a central conclusion, that is legal realism was indeed applied in all these cases, as shown in the fifth column of **Table 1**. The comparison between the prescribed sentence provided by both CCA 1997 and CMA 1993 in the third column of the same table, as opposed to the actual sentence given by the Malaysian and Singaporean courts as shown in the fourth column of the same Table presents a clear and direct reduction in the actual sentences.

The analysis resulted in supporting the belief by the legal realism supporters, where the correct law to be taken has taken place, particularly for those that have been decided in the courts of law. The court decisions would, therefore, take precedence over the prescribed written rules in the statutes of law, because those laws are the ones imagined by the legislators, and not the ones happening in the real world as in the courts of law. True enough, this belief coincides with the famous quotation by Pound (1930) goes: "*Realism is the accurate recording of things as they are, as contrasted with things as they are imagined to be or wished to be or as one feels they ought to be*".

Conclusion

This study sought to address the question of: ***How does legal realism apply in the criminalisation of computer crimes in Malaysia and Singapore?*** Accordingly, this paper worked on a review of the relevant literature on the two main concepts engaged in the study: legal realism and computer crimes. The review concluded the scarcity of resources on the conceptualisation of legal realism in cases involving computer-related crimes, which triggered the present research.

The paper went on further to outline the legal position of computer crimes within the ambit of CCA 1997 in Malaysia and CMA 1997 in Singapore. The primary aim of the investigation was to **demonstrate the application of legal realism in the criminalisation of computer crimes in Malaysia and Singapore**. For this purpose, an analysis of six decided court cases on computer crimes was carried out and demonstrated the application of legal realism in the criminalisation of computer crimes in both Malaysia and Singapore.

The finding of this study revealed that legal realism was indeed applicable in the criminalisation of computer crimes in Malaysia and Singapore, as has been decided in the six cases illustrated in the analysis. Essentially, all cases proved that the judicial approach by the courts in sentencing the computer crimes is the reduction of actual sentences as opposed to the prescribed sentences in both CCA 1997 and CMA 1993. Hopefully, this study can shed light into the better understanding of computer crimes, and how the cases are adjudged in the courts of law. Having demonstrated the application of legal realism in the criminalisation of computer crimes in Malaysia and Singapore, it just seems fair for future research to be carried out in broader contexts other than these two jurisdictions. Only then would we be able to provide a more conclusive finding of this under-researched area of jurisprudential theory in the real-world applications.

Acknowledgment

This research was supported by Ministry of Higher Education (MOHE) of Malaysia through **Fundamental Research Grant Scheme for Research Acculturation of Early Career Researchers (FRGS-RACER)** (RACER/1/2019/SSI10/UUM//1).

References

1. Abdullah, F., Mohamad, N. S., & Yunos, Z. (2018). Safeguarding Malaysia's Cyberspace against Cyber Threats: Contributions by CyberSecurity Malaysia. OIC-CERT Journal of Cyber Security, 1(1), 22-31.
2. Bainbridge, D. (2007). Criminal law tackles computer fraud and misuse. Computer Law & Security Review, 23(3), 276-281.
3. Bell, R. E. (2002). The prosecution of computer crime. Journal of Financial Crime, 9(4), 308-325.
4. Crimewatch, CSA. (2019). Crimewatch: Cybercrime Cases. Retrieved April 26, 2020, from Cyber Security Agency website: https://www.csa.gov.sg/gosafeonline/resources/crimewatch
5. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). Unauthorized Access Offences in Cyberworld Cybercrime, Digital Forensics and Jurisdiction (pp. 27-37): Springer.
6. Chong, E. (February 17, 2016). SMU student accessed accounts to delete scripts. The Straits Times. Retrieved 18 March 2020, website https://www.straitstimes.com/singapore/courts-crime/smu-studentaccessed-accounts-to-delete-scripts.
7. Chong, E. (July 20, 2017). Cop used police computer to vet girlfriend. The Straits Times. Retrieved 18 March 2020, website https://www.straitstimes.com/singapore/cop-used-police-computer-to-vetgirlfriend.
8. Dagan, H., & Kreitner, R. (2018). The New Legal Realism and the realist view of law. Law & Social Inquiry, 43(2), 528-553.
9. Fazlul Haque, E.H. (November 12, 2018). IT expert suspected of hacking PKR's e-voting system released on police bail. New Straits Times, retrieved May 1, 2020, website: https://www.nst.com.my/news/crime-courts/2018/11/430403/it-expert-suspected-hacking-pkrs-evoting-system-released-police.
10. Fittipaldi, E. (2016). Introduction: Continental legal realism. In A Treatise of Legal Philosophy and General Jurisprudence (pp. 1361-1382). Springer, Dordrecht.
11. Frank, J., & Bix, B. H. (2017). Law and the modern mind. Routledge.
12. Friedman, L. M. (1975). The legal system: A social science perspective. Russell Sage Foundation.
13. Hamin, Z., Othman, M. B., & Mohamad, A. M. (2012, May). ICT adoption by the Malaysian high courts: Exploring the security risks involved. In 2012 International Conference on Innovation Management and Technology Research (pp. 285-289). IEEE.
14. Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. Journal of Financial Crime, 22(2), 242-260.
15. Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security–a neo-institutional perspective. The Journal of Strategic Information Systems, 16(2), 153-172.
16. Hutchings, A. (2014). Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, Law and Social Change, 62(1), 1-20.
17. Jaishankar, K. (2018). Cyber criminology as an academic discipline: History, contribution and impact. International Journal of Cyber Criminology, 12(1), 1-8.
18. Jaishankar, K. (2007). Establishing a theory of cyber crimes. International Journal of Cyber Criminology, 1(2), 7-9.
19. Jayabalan, P., Ibrahim, R., & Manaf, A. A. (2014). Understanding Cybercrime in Malaysia: An Overview. Sains Humanika, 2(2).

20. Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. Journal of Crime and Justice, 42(5), 569-581.
21. Lai, A. (February 26, 2018). Ex-Perodua employee pleads not guilty to 311 charges of unauthorised computer system access. The Star. Retrieved May 1, 2020 website: https://www.thestar.com.my/news/nation/2018/02/26/ex-perodua-employee-pleads-not-guilty-to-311charges-of-unauthorised-computer-system-access/
22. Lang, A. (2015). New Legal Realism, empiricism, and scientism: the relative objectivity of law and social science. Leiden Journal of International Law, 28(2), 231-254.
23. Lee, M. K. (1990). Hacking and computer viruses-the legal dimension Viruses and their Impact on Future Computing Systems, IEE Colloquium on (pp. 6/1-6/4): IET.
24. Martinu, O., & McEwen, G. (2019). Crime in the Age of Technology. European Law Enforcement Research Bulletin, (4 SCE), 23-28.
25. Mohamed, D. (2013). Combating the threats of cybercrimes in Malaysia: The efforts, the cyberlaws and the traditional laws. Computer Law & Security Review, 29(1), 66-76.
26. Mohammed, A. A. S., Nawang, N. I., & Mustaffa, A. (2019). Criminal Attempt In The Malaysian Computer Crimes Act 1997 (Act 563). International Journal, 4(15), 01-07.
27. Nardin, T. (2017). The new realism and the old. CritiCal review of international SoCial and PolitiCal PhiloSoPhy, 20(3), 314-330.
28. Nazlina, M. (April 20, 2018). Businesswoman charged under Computer Crimes Act. The Star. Retrieved May 1, 2020, website: https://www.thestar.com.my/news/nation/2018/04/20/businesswoman-charged-under-computer-crimesact
29. Olsen, H. P., & Toddington, S. (2017). Legal Realism: In Search of a Science of Law. University of Copenhagen Faculty of Law Research Paper, (20017-36).
30. Pound, R. (1930). Call for a Realist Jurisprudence, The. Harv. L. Rev., 44, 697.
31. Priel, D. (2019). Legal Realism and Legal Doctrine. Judges and Adjudication in Constitutional Democracies: A View from Legal Realism (Pierluigi Chiassoni & Bogan Spaić eds., forthcoming 2020).
32. Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). Is your cat infected with a computer virus? Pervasive Computing and Communications, 2006. PerCom 2006. Fourth Annual IEEE International Conference on (pp. 10 pp.-179): IEEE.
33. Rouse, M. (2017). Cybercrime. Retrieved April 26, 2020, from Search Security website: https://searchsecurity.techtarget.com/definition/cybercrime
34. Sagar, M. (2019, June 18). Singapore Cyber Crime Cases Increase but Common Cyber Threats are Down. Retrieved April 26, 2020, from Open Gov Asia website: https://www.opengovasia.com/singapore-cyber-crime-cases-increase-but-common-cyber-threats-aredown/
35. Saha, S., Das, A., Kumar, A., Biswas, D., & Saha, S. (2019, August). Ethical Hacking: Redefining
36. Security in Information System. In International Ethical Hacking Conference (pp. 203-218). Springer, Singapore.
37. Shaffer, G. (2015). The New Legal Realist Approach to International Law. Leiden Journal of International Law, 28(2), 189-210.
38. Spaak, T. (2018). Legal Realism and Functional Kinds: Michael Moore's Metaphysically Reductionist Naturalism. Available at SSRN 3103299.

39. Sun, D. (January 29, 2020), 120 Gojek drivers suspended for usingmodified app that helps them bypassverification, The Straits Times, Retrieved 18 March 2020, website
40. https://www.straitstimes.com/singapore/gojek-to-suspend-120-drivers-for-fake-app-use.
41. Tamanaha, B. (2018). The Turn to Pluralist Jurisprudence. Jotwell: J. Things We Like, 1.
42. Tesauro, G. J., Kephart, J. O., & Sorkin, G. B. (1996). Neural networks for computer virus recognition. IEEE Expert, 11(4), 5-6.
43. Tivey, J., & Pearson, F. (2015). Protecting yourself from cloud-based risks. Computer Fraud & Security, 2015(6), 18-20.
44. Urbas, G. (2008). An Overview of Cybercrime Legislation and Cases in Singapore. In Asia Law Institute. Retrieved from https://law.nus.edu.sg/asli/pdf/WPS001.pdf
45. Woo-Sik, B., Han, K.-H., & Lee, S.-H. (2014). An Authentication System for Safe Transmission of Medical Information International Conference on Convergence Technology (Vol. 4, pp. 1-2).
46. Worthy, J., & Fanning, M. (2007). Denial-of-Service: Plugging the legal loopholes?. Computer Law & Security Review, 23(2), 194-198.