Malaysian Journal of Social Sciences and Humanities (MJSSH) (e-ISSN : 2504-8562)
2022, Volume 7, Issue 7, e001609
DOI: https://doi.org/10.47405/mjssh.v7i7.1609

Bring Your Own Device (BYOD): Legal Protection of The Employee in Malaysia

Muammar Kamil Abd Mohsin[1*], Zuraini Ab Hamid[2]

[1]Harun M. Hashim Law Centre, Level 2, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, PO Box 10, 50728, Kuala Lumpur, Malaysia.
Email: muammar.kamil@gmail.com
[2]Department of Legal Practice, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, P. O. Box 10, 50728, Kuala Lumpur, Malaysia.
Email: zurainihamid@iium.edu.my

CORRESPONDING AUTHOR (*):
Muammar Kamil Abd Mohsin (muammar.kamil@gmail.com)

KEYWORDS:
BYOD
WFH
Employee
Internet

CITATION:
Muammar Kamil Abd Mohsin & Zuraini Ab Hamid. (2022). Bring Your Own Device (BYOD): Legal Protection of The Employee in Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH), 7*(7), e001609. https://doi.org/10.47405/mjssh.v7i7.1609

ABSTRACT

Due to the portability of the devices and the broad coverage of the Internet access provided by the telecommunication carrier, the usage of mobile devices is not only limited to personal matters but has also been used to perform work-related tasks. The practice has led to the emergence of Bring Your Own Device ("BYOD") practice. BYOD has become popular because the companies can extend their confidence and trust in the employee, leading to an efficient team of human resources. The arrival of the COVID-19 pandemic has driven millions of employees to change their working practice from being physically in the office to adapting Work from Home ("WFH") practice. Unfortunately, BYOD has shown its bias toward the employees when there is a violation of employees' rights on working hours and privacy issues. Employees believe that the current legal system in Malaysia is insufficient to safeguard them against unfair BYOD practices. This study investigates the BYOD practice of using employees' personal mobile devices for work purposes and the worry regarding the employee's data stored on the devices when used for work and personal purposes. This report also suggests introducing Malaysian binding guidelines or policies to include a device definition and standardise BYOD practice in the workplace. This strategy is critical for protecting both employers and employees when introducing a BYOD policy at work.

Contribution/Originality: This study is one of few studies that focusing on the legal relationship between mobile technology and employees in Malaysia. While there were studies on the mobile technology and other areas, such as privacy and security, studies on employee legal protection are severely lacking in Malaysia.

1. Introduction

Motorola introduced mobile devices to the public as a hand-held telephone in 1983 called "DynaTAC 8000X" (Harris & Cooper, 2019). However, the only available function is voice communication. Starting in early 2000, phone manufacturers began to equip their mobile phones with the capability of browsing the Internet, enabling employees to connect their phones to the company's Information Technology ("IT") network. Mobile devices, such as tablets, phablets, and smartwatches, were introduced to the consumer market in subsequent years. As a result, the employee has options of devices to connect to their company's network enabling them to work from anywhere and anytime (Franklin & Mohamed Ismail, 2015).

In the early years of mobile connectivity, there was no written policy to govern the practice until Intel Corporation introduced the Bring Your Own Device ("BYOD") policy to its organisation in 2009 by its Chief Security and Privacy Officer, Malcolm Harkins. The policy was introduced based on his observations that most employees bring their smartphones, tablets and mobile devices to assist their work. Despite the general concern about the potential loss of the company's data and loss of employee productivity, the policy he proposed was to embrace the BYOD practice and use it as a means of cost-cutting and improved productivity (Rahat, 2014).

While BYOD does have its advantages in maximising employee productivity, it also has many downsides (Madhavi, 2016). Most of the studies on BYOD focus on either the technical implementation of the BYOD (how-to) or the protection of the company's data and are leaning towards technological-based discussions rather than legal discussions. As a result, the employee's concerns and protection were not adequately addressed and examined, resulting in potential unfair treatment or even manipulation of the employee in BYOD practice by the company.

The focus of the study on BYOD policy is conducted for a few reasons. Firstly, the employer has always regarded BYOD as a technical topic. Since today's world is a technological era, people are constantly interfacing with devices and embracing new technology daily. Therefore, when BYOD was introduced in 2009, most of the mobile phone manufacturer's technological platform or capability was already created or supplied. Hence, the organisations saw it as the way to go forward as there is a minimal cost to implement it, and the employee is open to accepting it as a new work norm. BYOD was adopted and implemented without thoroughly examining its impact on employee rights because of the seamless integration.

Secondly, some organisations act to mitigate the risk by conducting an internal risk assessment. However, it is more towards mitigating the risk of security breaches and personal data exposure by the employee. Furthermore, it has created a market demand for security-related software. Some security software is available to manage the BYOD implementation, such as personal device management software like Mobile Device Management and security data protection software like Data Leakage Protection. However, this type of software has created another legal concern: the breach of employees' personal data on mobile devices.

Lastly, the BYOD implementation usually can be completed quickly, compared to if the company issued a corporate device to the employee where it involves higher cost and a longer implementation timeframe. The seamless integration of BYOD in the organisation

has led to a minimal study on its legal effect. As a result, the BYOD was implemented without being legally advised, especially regarding the employee's rights. Even though the organisation will eventually reduce the gap by coming out with a BYOD policy, it does not always address the employee's rights.

2. Literature Review

The purpose of this literature review is to analyse the history of BYOD and its definition, the factors behind its emergence across the nations, including Malaysia, the concern behind BYOD usage, the gap in regard between employee and employer's protection and legal issues concerning the employee pertaining with its usage.

Based on the literature review on BYOD conducted by the researcher, the existing studies focus on the behavioural impact of BYOD on the employee, data security of both organisation and employee, its technical implementation, and risk controls on the BYOD (Norhazilah & Nor'ashikin, 2018). However, there is a lack of study regarding employees' unfair BYOD practices, especially in Malaysia.

The discussion about BYOD will always be related to devices and technology. According to Merriam-Webster (Merriam-Webster, n.d.), a device is a piece of equipment or a mechanism designed to serve a special purpose or perform a special function. The definition is accurate given the history of the first portable phone, the Motorola DynaTACs model. It was the only hand-held phone available when most mobile phones were wired into automobiles (Harris & Cooper, 2019). Due to the rise of technology and the emergence of the Internet of Things ("IOT"), devices have expanded from hand-held phones to laptops and what we have today, the smartphone (Zennaro, 2014). As the technology improved every year, mobile device usage increased to over 6.25 billion devices in 2021 billion worldwide (Statista, 2022).

Due to the portability of the devices and the broad coverage of the Internet access provided by the telecommunication carrier, the usage of the mobile devices is not only limited to the personal matters, such as online shopping and social media, it has also been used to perform work-related tasks (Mordor Intelligence, 2022). The situation has led to the emergence of BYOD. According to Oxford Learner Dictionary (Oxford University Press, n.d.), BYOD is a policy that allows employees in a company or students at a school to use their phones, laptops, etc., at work or school. The definition is not entirely accurate as it is confined to BYOD as a policy, whereas it is a general practice that is not dependent on whether the company has established a policy or not. There is a better definition of BYOD, where BYOD is a concept that permits the employee to use their mobile devices such as smartphones, laptops and tablets to access systems, web applications or company information either from their Internet, inside or outside the company's network (Norhazilah & Nor'ashikin, 2018).

An article by Roman (2012) based on his interview with Intel Corp's Chief Information Security Officer ("CISO"), Malcolm Harkins, described the inception of Bring Your Own Device ("BYOD") practice in 2009 by Intel Corp, where it has seen a tremendous increase of mobile devices usage by its employees for work, compared with the company-issued mobile devices. Based on this definition, two categories of mobile devices are used for work-related purposes: personal devices and company-issued devices. This research will focus on the first category, BYOD, which refers to personal devices instead of company-issued devices.

While there is a lot of research regarding BYOD, the focus is mainly on technology, privacy and protection for the employers. The researcher found none of the legal analysis on BYOD in Malaysia was conducted from employees' perspectives. An article discussed a little bit about the legal aspect of BYOD (Madhavi, 2016). However, it was mainly on the technicalities of BYOD, such as technology and architecture, tools and system, data authentication and security method. In another article (Fara et al., 2020), the discussion is on the company's data security protection rather than the employee's protection. In another article (Rose, 2013), the legal liability's coverage was only made in the form of questions rather than a deep and focused discussion.

Other areas of concern were missing or incomplete, such as protecting the employee's contract or employment area. The existing research described available research regarding BYOD's data protection (Veljkovic et al., 2014). Therefore, based on the current articles and research, there is an imbalance between the mitigation of the company's data exposure and the protection of the employee from BYOD usage. It seemed that discussion on BYOD mainly favours the company rather than safeguarding the employee. In addition, the above authors and researchers proposed a policy to govern BYOD. However, no attempt is made to discuss the Malaysian legal framework relevant to BYOD.

3. Methodology

This study adopts qualitative research methods, such as content analysis and critical legal studies of Malaysia's employment and contract laws, legislation, statutes, and policies. Then, the secondary data was gathered by researching textual materials such as textbooks, official reports, statistics, seminar papers, and articles from refereed publications. The material is also sourced from published electronic sources, particularly government websites and reputable organisations. Secondary data has assisted the researcher in obtaining knowledge unavailable from primary data. This type of analysis is necessary since it allows the researcher to interpret the texts mentioned and comprehend the research problem.

4. Results and Discussions

4.1. The push factor for BYOD

According to a report, BYOD has become popular because firms can extend their faith and confidence in their employees, resulting in a more effective human resource team (Mordor Intelligence, 2022). This report is supported by a finding (Schulze, 2021), wherein in 2021 a total of 82% of companies allowed BYOD to some extent, and 70% of the employee brought mobile devices into the workplace, followed by other groups like contractors (26%), partners (21%), customers (18%), and suppliers (14%).

BYOD was further amplified by the recent Covid-19 pandemic, where companies were forced to adapt Work from Home ("WFH") practice. In another report (Brynjolfsson et al., 2020), entitled "Covid-19 and Remote Work: An Early Look at US Data", the arrival of the COVID-19 pandemic has driven millions of employees to change their working practice from being physically in the office to be at their homes for work. A study in the United States revealed that before the Covid19 pandemic, 5% to 15% of Americans worked from home. After the pandemic, at least 50% of the Americans employed pre-Covid19 had to

embrace WFH starting from April 2020. The situation has led to the rise of BYOD practice as employees have to use their devices for work.

4.2. BYOD in Malaysia

In Malaysia, the law protecting employee rights regarding BYOD practice is not clearly regulated or expressed in any binding guidelines. The situation is different from other countries such as Switzerland and those in the European Union ("EU"), where they have adequate control over the usage of mobile devices by the employee in the organisation. Their legal framework does recognise BYOD as a practice in the workforce. However, they put a control to regulate it to protect the employee's rights by establishing the needs for an organisation to implement BYOD and what extent to which BYOD is allowed.

EU, consisting of 27 European countries, has also come out with its regulation to protect both employers and employees, called General Data Protection Regulation ("GDPR"), which came into force on May 25 2018. This regulation significantly increases employers' obligations and responsibilities concerning how they collect, use, and protect personal data. Under the Employer's Obligations section of the GDPR (the legal basis for processing personal data, among others), processing the data is necessary to fulfil parts of the employee's contract.

Article 3(1) of the GDPR extends its locality principles to businesses outside the EU, including Malaysia. Therefore, a subsidiary company in Malaysia cannot process the personal data of its employees in Malaysia and transfer the personal data to its parent company located in the EU. Unfortunately, the GDPR does not apply to a temporary EU presence of a controller outside the EU (Skrine, 2020).

In addition, BYOD in Malaysia also captured companies' attention after it became a trend in Higher Learning Institutions. A study reported that various aspects of BYOD practice observed in Higher Learning Institutions include the level of BYOD awareness, the use and purpose of BYOD, the problems users face and the level of user satisfaction in college with BYOD (Franklin & Mohamed Ismail, 2015).

The finding further shows that using personal devices in the workplace increases productivity and flexibility. In Malaysia Cyber Security Strategy ("MCSS") 2020 to 2024, the government has acknowledged the practice of BYOD (National Cyber Security Agency, 2020). However, the government has emphasised the relevant stakeholders to control the employees, vendors' and data access. In the Malaysian Public Sector ("MPS"), the main document for supporting Information Technology is Information Security Policy document or officially named "*Dasar Keselamatan ICT*" ("DKICT"). It contains rules that must be read and adhered to by the employee in using the Information and Communication Technology ("ICT") assets (Norhazilah & Nor'ashikin, 2018). The policy explains the users' responsibilities and roles in protecting the organisation's ICT assets. However, it does not explicitly address the BYOD practice in detail and what is the legal action that it is referring to.

In Malaysia, few Acts govern employees' issues and rights. Among them are Employment Act 1950 and Contract Act 1955, which aim to protect the employee's contract terms, and Personal Data Protection Act 2010 which safeguards employee data protection. Though the existence of the related Acts and the BYOD is recognised in Malaysian practices, there is no specific legal framework or binding guidelines governing employment terms and

rights in BYOD practice. The introduction of the binding guidelines or policies is vital in adopting BYOD practice because the unfair practice can breach the employee's contract regarding the employee's terms, including working hours, remuneration, and compensation as expressed in Employment Act 1955. The employer will have 24-hour communication access with the employee since everything is on the fingertip.

Depending on several scenarios, there will also be a privacy breach of employees' personal data on the devices. For example, when the employee is required to install applications on their devices, or actions of wiping the organisation's data on the devices could affect their personal data (Rice, 2016). Some authors further define privacy risk as the degree to which people who adopt BYOD jeopardise their personal life (Weeger et al., 2016). Data privacy infringement is also a concern to employees who find BYOD challenging to use (Chountalas & Karagiorgos, 2015). The problem occurs because employees use their device to work, which contains personal and employer data. Employees are concerned about companies that utilise technology to manage them, such as monitoring personal data usage and wiping personal data if the device is lost or stolen (Zhang at el., 2017).

In addition, the unfair BYOD treatment affects the employee in terms of their legal capacity. Thus, it could also lead to other significant issues. For example, BYOD also leads to employee burnout due to the after-hours work connectivity. In a survey by a reputable media (B.Suresh, 2019), 53% of respondents got less than 7 hours of sleep in 24 hours due to increased after-hours work connectivity.

4.3. Legal Issues on BYOD Practice

Since BYOD has been practised for many years now, certain countries have taken the initiative to address the legal concern of BYOD. In an article regarding Switzerland's employment contracts and BYOD policies (Schneider, 2016), employers must provide the employees with any devices they require for professional purposes unless the parties agree otherwise. The requirement is mentioned in Article 327(1) of the Federal Code of Obligations. As a result, BYOD may be introduced only with the consent of the concerned employee. Furthermore, consent is considered valid only if given freely after adequate information has been provided.

The protection also specifies rules about the device usage, such as safeguarding employee data after the termination of employment. Article 321a(4)) and Article 328b of the same Code put a limit on data processing by the employee and Article 327(2) stated that appropriate compensation is required for the professional use of the device. Most importantly, Article 328(1) has also covered the working hours and timeframe limit. Employers should set clear rules regarding the timeframe in which devices may be used for professional purposes. This action is required to ensure that the employer can protect employees' personality rights, have due regard to employees' health, and maintain proper moral standards.

Also, the EU's General Data Protection Regulation ("GDPR") elaborates explicitly on the employer and employee's relationship, detailing the responsibilities and protection available for each group, specifically under the Data Controller section (GDPR).

In contrast with BYOD practice in Malaysia, these terms or protection were absent from the Employment Act ("EA") 1955 or Contract Act ("CA") 1950. In EA 1955 s10(1), it stated that:

> "A contract of service for a specified period of time exceeding one month or for the performance of a specified piece of work, where the time reasonably required for the completion of the work exceeds or may exceed one month, shall be in writing."

The section is quite general, and there is no further definition of how to handle BYOD practices by the company and its employee. Currently, the standard employment term set in the contract includes work scope, work location, wage rate, wage period, and employment benefits. It further provides a framework regarding the holidays, annual and sick leave and matters related to preserving health and safety.

Compared with Switzerland's Federal Code of Obligations, there are no specific or binding guidelines governing BYOD in Malaysia, including in existing legal frameworks governing the employer-employee relationship. The absence of any legal framework governing BYOD could lead to excessive work periods by the employee due to their own devices for work purposes, especially during off-office hours (B.Suresh, 2019).

Section 60A (1)(d) of the Employment Act further states that an employee shall not be required to work more than 48 hours a week under his contract of service unless under certain exceptions. Therefore, due to the absence of BYOD protection for the employee, there will be a breach under this section regarding the working hours. The 24-hour access to recourses given to the employee via devices has created a vast opportunity for the employer to impose a 24-hours working environment.

5. Conclusion

In conclusion, there are gaps regarding BYOD practice in Malaysia, specifically in the employee's legal protection. The practice relating to the BYOD policy is improperly governed under Malaysian existing policies, guidelines, or laws. The situation is different from other countries that recognise the BYOD practices, such as Switzerland's Federal Code of Obligations or the European Union (EU") 's General Data Protection Regulation ("GDPR"). The absence of any legal framework governing BYOD in Malaysia has created uncertainty for Malaysian employees' rights. To a certain extent, it has created an unfair BYOD practice by the employers toward the employees in Malaysia.

In the era of technology, whereby almost everything now relies on systems and online data, the nation depends on skilled employees, especially in the technology sector. Although it has been proven that BYOD has led to productivity improvement, it could also lead to the opposite if the employees feel that the employer is unfairly treating them in the BYOD practice. The employees are manipulated, and their life is threatened with non-stop working hours because of the BYOD without reasonable compensation or additional allowance to use their own devices.

Leaving the decision to the employer or company to decide the best BYOD policy or practice will not guarantee that the employees' rights will be protected. The problems can be addressed or remedied by having a specific, binding guideline or legal framework governing BYOD in Malaysia. The inclusion should govern the definition of a device,

general standard BYOD practices in the workplace and address employee-employer protection.

Funding

This study received no funding.

Conflict of Interests

The authors declare no conflict of interest in this study.

References

Chountalas P. & Karagiorgos A. (2015). Bring Your Own Device philosophy from the user's perspective: An empirical investigation. *Proceedings of the 2nd HOBA International Conference*. Patras, March 7-8, 1-12.

Brynjolfsson, E., Horton, J. J., Ozimek, A., Rock, D., Sharma, G., Tuye, H.-Y., & Upwork, A. O. (2020). *COVID-19 and Remote Work: An Early Look at US Data*. National Bureau of Economic Research.

B.Suresh Ram. (2019, November 15). Survey: Malaysian employees are overworked, sleep deprived, unhealthy. *New Straits Times*. Retrieved from https://www.nst.com.my/news/nation/2019/11/539026/survey-malaysian-employees-are-overworked-sleep-deprived-unhealthy

Franklin Onyechere Ugochukwu, & Mohamed Ismail Z. (2015). The Future of BYOD in Organisations and Higher Institution of Learning. *International Journal of Information Systems and Engineering, 3*(1), 110–28.

Harris, A., & Cooper, M. (2019). Mobile Phones: Impacts, Challenges, and Predictions. *Human Behavior and Emerging Technologies, 1*(1), 15–17.

Fara Jamal, Mohd. Taufik, Azizol Abdullah, & Zurina Mohd. Hanapi (2020). A Systematic Review of Bring Your Own Device (BYOD) Authentication Technique. *Journal of Physics: Conference Series, 1529,* 042071.

Madhavi Dhingra. (2016). Legal Issues in Secure Implementation of Bring Your Own Device (BYOD). *Procedia Computer Science, 78 (January)*, 179–84.

Merriam-Webster. (n.d.). Device. In *Merriam-Webster.com dictionary*. Retrieved February 28, 2022 from https://www.merriam-webster.com/dictionary/device

Mordor Intelligence. (2022). BYOD Market | 2022 - 27 | Industry Share, Size, Growth. *Mordor Intelligence*. Retrieved from https://mordorintelligence.com/industry-reports/byod-market

National Cyber Security Agency (NACSA). (2020). Malaysia Cyber Security Strategy 2020-2024.

Norhazilah Mahat & Nor'ashikin Ali. (2018). Empowering Employees through BYOD: Benefits and Challenges in Malaysian Public Sector. *International Journal of Engineering & Technology, 7*(4.35), 643-649. www.sciencepubco.com/index.php/IJET

Oxford University Press. (n.d). BYOD. In *OxfordLearnersDictionaries.com*. Retrieved February 28, 2022 from https://www.oxfordlearnersdictionaries.com/definition/english/byod?q=BYOD

Rahat Afreen. (2014). Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges Elliptic Curve Cryptography for Embedded Systems

View Project. *International Journal of Emerging Trends & Technology in Computer Science, 3*(1), 233-236.

Rice, A. L. (2016). Best Practices for Secure BYOD. *Uoregon*. Retrieved from https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/22340/Rice%20Week%207%20FINAL.pdf?isAllowed=y&sequence=1

Roman, J. (2012, January 11). BYOD: Get Ahead of the Risk. Intel CISO: Policy, Accountability Created Positive Results. *Bank Info Security*. Retrieved from https://www.bankinfosecurity.com/byod-get-ahead-risk-a-4394

Rose, C. (2013). BYOD: An Examination Of Bring Your Own Device In Business. *Review of Business Information Systems (RBIS), 17*(2), 65–70.

Schneider, J. (2016). BYOD: Employment and Privacy Law Issues. *Lexology*. Retrieved from https://www.lexology.com/library/document.ashx?g=efb6e65d-1974-4119-ad02-cca560b2b750

Schulze, H. (2021). BYOD Security Report. *Cybersecurity Insiders*. Retrieved from https://www.cybersecurity-insiders.com/portfolio/2021-byod-security-report-bitglass/

Skrine. (2020, November 23). Protection of Employee's Personal Data in Malaysia - General Data Protection Regulation ("GDPR") and Personal Data Protection Act 2010 ("PDPA"). *Skrine*. Retrieved from https://www.skrine.com/insights/alerts/november-2020/protection-of-employee's-personal-data-in-malaysia

Statista. (2022). Smartphone users 2026. *Statista*. Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Veljkovic, I., Mitrovic, Z., Whyte, G., & Thompson, K. (2014). *The 1st Namibia Customer Service Awards & Conference*. Windhoek, Namibia.

Weeger, A., Wang, X., & Gewald, H. (2016). IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *Journal of Computer Information Systems, 56*(1), 1-10.

Zennaro, M. (2014). *Introduction to the Internet of Things*. The AbdusSalam International Centre for Theoretical Physics. Trieste, Italy.