How to cite this article:

Abdul Manap, N., & Abdullah, A. (2020). Regulating artificial intelligence in Malaysia: The two-tier approach. *UUM Journal of Legal Studies*, *11*(2), 183-201. https://doi.org/10.32890/uumjls.11.2.2020.8779

# REGULATING ARTIFICIAL INTELLIGENCE IN MALAYSIA: THE TWO-TIER APPROACH

**Nazura Abdul Manap & [1]Azrol Abdullah**
*Faculty of Law, Universiti Kebangsaan Malaysia*

[1]Corresponding author: azrolabdullah@gmail.com

Received: 13/2/2020 Revised: 3/5/2020 Accepted: 20/6/2020 Published: 31/7/2020

## ABSTRACT

*Artificial Intelligence (AI) has been developed under the field of computer science for more than 50 years. Somehow AI only gained prominence in the recent millennia when necessary tools to test the hypothesis on the nature of thought became available. Unfortunately, the absence of legal regulations on AI has caused AI to exist in a regulatory vacuum and nature abhors a vacuum. The law is at a state of confusion about who shall be blameworthy for the damage caused by AI. The prevalence of this problem triggers the expatiation of this review article in defining the scope of AI that must be regulated. The objective of this article is to suggest that AI with certain capabilities must be placed in the legal realm. This article will first begin by highlighting the problems associated with AI before directing the focus of the discussion to the various reasons that justify for AI to be regulated. This article will then explore the various approaches which can be adopted by the government in regulating AI. These approaches can be a workable formula to procure the two-tier method in regulating AI in Malaysia. The methodology devised for this article is based on doctrinal research where most of the materials were derived from text books, online* *resources and established academic databases. The findings made in this article suggest that AI must be regulated independently from existing legal frameworks. Reason being, AI capabilities are unique in its own sense and therefore cannot be treated like other previous technologies. The outcome of this article may also be able to contribute to issues relating to the legal liability of AI in Malaysia.*

**Keywords:** *AI, artificial intelligence, liability, regulating AI, risks.*

## INTRODUCTION

Artificial intelligence (AI) is changing human lives. AI has provided enormous benefits to humans for more than 50 years, ranging from voice assistance like Alexa and Siri, to self-driving vehicles, search engines that learn from our browsing habits and email systems which are capable of identifying spam emails. AI technology has the ability to perform cognitive functions like humans and able to solve problems in a way that may never have been thought of by humans (Gerstner, 1993). Whenever AI deals with a problem, it will look for solutions without depending on any teaching algorithm to solve problems (Poole & Mackworth, 2010).

Although AI may possess impressive capabilities and appears to be harmless, AI can pose a real threat to humans. Past incidents have demonstrated that AI is indeed fallible (Sipper & Moore, 2017). AI can be a threat if its design is flawed regardless of how small the purpose of its design (Omohundro, 2008). It is impossible to design an error-free code because on average, any software programme will have at least one to three bugs in every 100 statements (Ahamed, 2009). By taking into account these possibilities, AI cannot be left to exist in a regulatory vacuum.

The absence of regulatory framework on AI has now become a global concern that affects societies, individuals and may have shaken some of the legal frameworks (Cerka et al., 2015). Dearth of legal scholarships has resulted in potential approaches which can be adopted to regulate AI including stretching existing laws to accommodate AI (Calo, 2015). Existing laws are unable to address the legal conundrums created by AI due to the technological fluidity of AI (Cerka et al., 2015). Stretching the existing laws to AI will eventually reach a breaking point when AI systems become more autonomous and disconnected from humans who have control over it (Sullivan & Schweikart, 2019). Conventional approaches such as product liability, research and development oversight and tort liability are not suitable to manage the risks associated with AI (Scherer, 2016). This article will illustrate the importance of regulating AI, but does not intend to establish a blueprint or guideline template. Instead, this article will suggest important elements for the two-tier approach.

## WHY REGULATE AI

The frequency of damage which can be inflicted by AI on humans corresponds to the increasing number of AI usage in human activities. In 2017, the European Parliament during its Plenary Sitting acknowledged that traditional rules will not suffice to give rise to legal liability for any damage caused by a robot (Delvaux et al., 2017). The majority of AI industry players are also advocating for specific regulations on AI. Even Tesla founder, Elon Musk has demanded for AI to be regulated because AI is akin to 'summoning a demon' if left uncontrolled (Yeoh, 2017). Similar sentiments was also expressed by Stephen Hawking when he drew an analogy about the importance of regulating AI after observing AI's ability to destroy society (Clifford, 2017). The conservatives however retorted that the time is still too early for AI to be regulated because existing laws are sufficient to deal with AI issues (Reed, 2018). The justifications to regulate AI are anchored on two grounds namely, (a) infringement of fundamental rights; and (b) loss or damage as a result of AI decision(s).

### Infringement of Fundamental Rights

The first justification to regulate AI is to prevent the infringement of human rights by AI. Some may ponder in what way(s) is AI capable of violating human rights? To answer this question, one must be able to appreciate the AI techniques itself. A symbolic reasoning AI may not be too threatening to humans as much as machine learning

AI. However, machine learning AI which collects data from past experiences and decisions will result in grave consequence on human rights. Machine learning techniques may cause AI's decisions to be biased and consequently violates fundamental human rights.

The court's decision in *State v Loomis*[1] became the leading case which illustrates the extent of damage that AI can cause on human rights. In this case, the accused pleaded guilty to the criminal charges made against him. The court had relied upon COMPAS risk assessment score to deny the accused probation and sentenced the accused to six years imprisonment and five years extended supervision. It was reported that COMPAS was prone to mistakenly label black offenders as likely to reoffend by flagging them with 45-24 per cent higher risk to reoffend than white people (Buranyi, 2017). The case went on appeal but the appeal was dismissed by the Wisconsin Supreme Court. Despite the dismissal, the Supreme Court acknowledged that the risk assessment score generated by COMPAS failed to explain the manner of data being employed to generate the results (Liu et al., 2019). The court's reliance on the conclusion made by COMPAS was a flagrant breach of the accused's right to be heard and right to be treated equally before the law.

Another controversial AI system which affected the issue of privacy is Alexa. Alexa is an AI application that functions as an intelligent personal assistant with the capability for interaction, listening, music playback, streaming, controlling smart appliances for home automation and to some extent, possess certain embedded skills. In November 2017, Alexa left to its own devices decided to hold a house party while its owner was away. Again, in May 2018, Alexa had recorded a conversation of its owner and shared the recorded conversation with a third party (Chokshi, 2018). Another incident was in November 2018 when Alexa sent 1,700 recordings to a complete stranger (McCarthy, 2018). These incidents have demonstrated a point; Alexa is capable of intruding on the user's right to privacy. Reports have suggested that the number of complaints lodged against Amazon relating to the mischievous behaviour of Alexa is on the rise (Photong, 2017). Alexa is like a problematic child, plunging Amazon in hot water.

[1] *State v Loomis* 881 N.W.2d 749 (Wis. 2016) 754 (US).

### Loss or Damage as the Result of AI's Decision

The second justification for regulation on AI is premised on a legal scheme where the liability is distributed on the tortfeasor to mitigate the damage and losses caused to others. The scholarship of articles approach this issue by suggesting that the time is apt for AI to be recognised as a subject of law and capable to bear its own legal liability. This line of suggestion is hinged on the revolutionised capability of AI which can function independently without having to rely on human interference. In some circumstances, this capability may entail disruptive effect if left unchecked (Manyika et al., 2013). Ever cheaper, faster, and more sophisticated AI systems are now able to do the work of people in a wide variety of fields and on an unprecedented scale (Abbott, 2018). As AI is becoming more ubiquitous and sophisticated, the question on how to mitigate the harm caused by AI is becoming more pertinent (Wagner, 2018). This article would be remiss for not mentioning some of the obvious harm caused by AI.

On 7 May 2016, Joshua Brown was killed in a crash while using the semi-autonomous driving system on his Tesla Model S. Brown was operating the car using the advanced driver assistance features Traffic-Aware Cruise Control and Auto steer lane keeping assistance (National Transportation Safety Board, 2016). The car struck and passed beneath a 2014 Freightliner Cascadia truck-tractor in combination with a 53-foot semitrailer killing Joshua Brown instantly (National Transportation Safety Board, 2016). On 19 March 2018, Elaine Herzberg, a 49-year-old pedestrian was killed by a self-driving car (Volvo XC90), operated by Uber while she was crossing at an intersection in San Francisco (Wakabayashi, 2018). Four days later, another incident occurred in Mountain View California where a Tesla Model X had crashed into a concrete divider on 23 March 2018 killing its driver, Walter Huang ("Tesla car," 2018).

## REGULATING NORMS

Considering the amount of AI threats, past incidents, legal deadlocks, the time is now ripe and justified for AI to be regulated. AI regulation will be able to address the emerging problems relating to AI. However, the desire to regulate AI is not just a complex terrain but it is uncharted territory for an age that is transferring human roles to machines that is capable of learning, automation, robotic manufacturing and deep learning (Spencer, 2019).

Generally there are three methods employed by regulators in drafting any regulation. The first method is legalistic (Petit, 2017). The legalistic approach starts from the legal system, and proceeded by drawing from lists of existing legal fields or issues affected by AIs and robots: liability, safety, privacy and cyber security (Leroux et al., 2012). Over reliance on the legalistic approach may undermine the necessary development of novel legal fields in the context of emerging technologies (Petit, 2017).

The second approach is the technological approach. The technological approach is more ontological which consists of an assessment of what the technology is all about and whether the technology displays human features (Petit, 2017). Thus the discussion is mostly directed to a reflection of oneself, and what makes us human. The point here is to envision legal issues from the bottom-up standpoint of each class of technological application: driverless cars, social robots and exoskeletons (Palmerini et al., 2016).

The third approach is regulatory capture. This approach however, is quite controversial and preferably to be abstained from becoming the foundation of any AI regulation. The idea of regulatory capture was comprehensively described by George Stigler in his seminal work on the *Theory of Economic Regulation* published in 1971. Regulatory capture can be described as the situation where the government's policy is steered by politicians and bureaucrats who would also pursue their own private goals such as prestige and wealth, and are prone to encounter the conflict of interests between their private goal and their public function (Boehm, 2007). Although Stigler never used the word 'regulatory capture' in his work, but it is common to see researchers citing his work for the past 40 years in the discussion on, 'regulatory capture' (Carrigan & Coglianese, 2016). Take for example, taxi drivers have requested additional protection from the competition of ride-sharing apps like Uber, and the hospitality sector has sought to steer municipalities across the world to undermine the operations of services like AirBnB or platforms like Booking.

com and Expedia (Petit, 2017). In this respect, a government which decides to adopt the technological approach to regulate AI will likely be exposed to rent-seeking scenarios by stakeholders from the technology community. Perhaps, the alternative method to avoid regulatory capture is by way of policy hacking which will be discussed next.

The uniqueness of AI demands for a different approach in framing regulations. The three methods mentioned cannot be exclusive. A mixed-methodology is to be devised so that the AI regulations can be sufficiently flexible in adapting to the dynamic changes of AI technology. In this respect, a combination between the legalistic and technological approach can be a workable formula in drafting a regulation on AI. This formula can be used as the main catalyst towards the idea of proposing a two-tier regulation approach which is chosen to be the central theme of this article.

## THE TWO-TIER REGULATION APPROACH

The regulating norms discussed above may not be able to deal with the emerging threats of AI. Therefore, the adoption of the two-tier regulation approach is appealing. This is an approach which requires the regulation on AI to be made by way of two levels. The first level or the first tier specifically refers to the promulgation of hard law by the Parliament i.e. a specific Act on AI. Whereas the second level or the second tier, refers to delegated legislations or policies passed by a specific ministry(s) of the government. Both levels will serve different objectives and purposes in regulating AI. The following discussion will not formulate a guideline or blueprint. Instead, it intends to highlight the crucial elements that must be incorporated in the legal provisions made by way of the two-tier approach.

### The First-tier Regulation

The first tier shall serve as the primary piece of legislation to govern only crucial matters on AI so that AI will not be left unchecked, will not lose control and will be safe. The first-tier refers to a specific Act of Parliament on AI. The intended specific Act on AI incorporates the following fundamental elements:

## Definition of AI

Some may have pondered on why we need to plumb the abyss in defining ‘What is AI?’ when humans can live with functional understanding on some abstract notion. For instance, we may understand what is ‘time’, ‘love’ and ‘happiness’ which are difficult to be defined but easy to be functionally understood. Natural law philosopher, Lon L. Fuller who pioneered the idea of ‘internal morality law’ said that in order for any law to be valid, its subjects must be able to understand the law (Tucker, 1965). Therefore, the definition of AI is a crucial issue as it determines to what extent AI will be regulated.

The difficulty in giving an acceptable definition to AI is not on the concept of artificiality but on the concept of intelligence (Scherer, 2016). Alan Turing has devised a test that eliminates the need to define intelligence in terms of what one does when one acts intelligently (Stevens, 1985). Unfortunately, the definition offered by Turing is only capable of proving that AI is able to mimic human thinking but insufficient to deal with modern AI technology which is now widely used by humans.

The term *artificial intelligence* was first coined in 1956 by John McCarthy during the Dartmouth Sumer Project (Kaplan, 2016). McCarthy defined AI based on intelligence (McCarthy, 2007). However, this definition was found to be unhelpful (Buiten, 2019). Some have called for the unpredictability of AI’s behaviour to be the main feature in defining AI (Scherer, 2016). However, this form of definition is unsustainable because computer programmes will continue to develop. Moreover, what humans perceived as unpredictable 10 years ago is considered to be nothing special today (Buiten, 2019). The underlying problem with AI is that, as soon as an AI technique works, it is no longer considered AI and becomes a spin-off in its own field such as character recognition, speech recognition, machine vision, robotics, data mining, medical informatics and automated investing (Kurzweil, 2006).

Some have suggested that defining AI must be grounded on its anthropomorphic character namely, the ability to: think humanly, think rationally, act humanly and act rationally (Russel & Norvig, 2010). The question now is whether giving definitions of AI based on human traits is appropriate because the way humans think is totally different from the way AI thinks. Turing test and other mimicry metrics may be less relevant in today's practical applications of AI. The way humans think is different from AI because humans have amygdala which stimulates future happenings and visual cortex that transforms data from the eyes to images (Husain, 2017). AI works under a different model. The AI machine works on silicon substrate as compared to humans which rely on carbon substrate. This has resulted in the intrinsic strengths of the machine mind such as speed, limitless recall, and unconstrained energy consumption. The essence of intelligence is the ability to make appropriate generalisation based on limited data. Learning is one of generalisation processes which take into consideration data of past experiences to aid future analyses (Kaplan, 2016). The exponential development in AI technology has now lured AI researchers to move into deep learning, which is another sub-field of AI.

Alternatively, AI system should be allowed to define itself according to the massive data available today. Any AI programme can be designed to take up this task. This will put AI's ability to the test by resolving the simplest issue(s) which has left researchers grappling for decades. Perhaps what was said by some AI researchers that the word 'AI' is a name given to a technological process which we do not understand bears some weight. Against this chequered landscape, this article suggests to define AI as an *autonomous entity that is able to make its own judgement through an independent evaluation of choices*. This is reasonably sufficient to proffer a general description about AI without having to contract the controversial word, 'intelligence' as part of the definition.

## Certification Requirements

The certification process demands AI designers to produce full documentation on the historical background of the AI programme coupled with the ability to detect any misbehaviour of AI (Schirmer et al., 2018). Certification process on AI is justified by law and will encourage the demand for ethical use of AI (Ravid & Hallisey, 2018). Certified AI will ensure the reliability and trust on the AI industry. This will stimulate further growth and development of AI technology (Ravid & Hallisey, 2018). AI programmes which are not certified shall be legally presumed to be unsafe for commercial and consumer use. It shall be an offence under this Act. With this requirement the regulators can impose on AI designers to build AI capable of observing moral principles. For instance, in the design of AI voice assistant, it must be able to distinguish which part of the conversation is to be considered as confidential and which part of the conversation can be publicly shared.

## Special Zone for AI

For certification under this Act, all AI intended for commercial and consumer purposes must be placed in a special zone. Special zone is a controlled area designated within real society. General regulations on the use of AI are being applied in order to allow for the presence of experimental AI which has proven to be safe in laboratories. Special precautions are taken in order to prevent serious accidents and undesired outcome (Santoni de Sio, 2016).

The special zone system or the AI kingdom is to observe the coexistence between human society and AI. The special zone serves as a shock buffer for supporting new human-AI ecology (Weng et al., 2015). Some say that performing AI experiments with real people in real cities is morally prohibited until the technology is proven to be safe (Santoni de Sio, 2016). Therefore, the special zone will allow regulators and manufacturers to identify foreseeable risks before it is released into the real world. It allows for the assessment on how far the system(s) may react in different contexts and to determine whether robots and other AI agents are able to meet human needs (Pagallo, 2018).

Special zones have been implemented in Japan for robot testing known as *Tokku* (Pagallo, 2018). *Tokku* is a Special Zone for Robotics Empirical Testing and Development (RT special zone) which originated in Japan for more than a decade and has proved to be effective in creating new ecology between humans and robots. Tokku can be adopted as the benchmark for the setting up of a special zone(s) so that fundamental issues relating to AI can be empirically tested.

In April 2019, a strategic collaboration was entered between local Malaysian company with two Chinese companies to develop AI park in Malaysia (Bernama, 2019). The AI park will be built in Technology Park Malaysia covering 686 acres of land (Inn, 2019). No doubt the AI park will provide exposure to Malaysians about AI. But to what end? Will there be any transfer of technology which Malaysians can benefit? So far responsible parties have remained reticent about the details of the whole programme. It is unknown whether the proposed AI park will embody the characteristics of the AI special zone. If it does, the Malaysian government is allowing China to perform its AI technology experiments on Malaysian soil and offering Malaysians to become experimental subjects. The data collected may enable China to further improve their AI technology. giving China the biggest portion of the cake, especially when data is becoming a new precious commodity of the present day.

## Digital Peculium

The ability of AI to be independent from human influence in decision-making, demands for a new form of liability scheme. In this sense, AI ought to bear some responsibility under the law for its decisions. The responsibility must also be coupled with the ability to compensate any injured party in a situation where AI has gone bad. But how can AI be able to compensate? Digital peculium can be a promising option to be incorporated into the AI Act. Digital peculium is a mixture between the new form of accountability for the behaviour of AI and traditional ways of distributing risk through insurance models or authentication systems. However, Digital peculium is relevant if AI is unable to hold its own legal personality. The legal personality of AI is outside the scope of this article.

The mechanism of peculium explained in the Digest of Justinian is an old Roman mechanism which permitted slaves who were being deprived of personhood to be held responsible for his/her own conduct and to act as estate managers, bankers or merchants (Watson, 1988). The peculium was the sum of money or property granted by the head of the household to a slave or son-in-power. The master's liability was limited to the value of their slave's peculium. This approach can be adopted to resolve issues relating to compensation or to mitigate losses caused by any AI system.

If this mechanism is to be applied, a distinction has to be made about the type of use of the AI system like what the Romans did for the activities and status of the slaves (Pagallo, 2013). The adoption of this concept will be able to bypass the legal discussion on the personhood of AI in relation to liability in tort cases. The amount required to be allocated for any particular activity will be determined by the Act. Panoply of scholarships suggests that AI must be insured through conventional insurance scheme in order to compensate the injured party. What makes digital peculium different from conventional insurance? Apart from the technicalities of the insurance policies, the conventional insurance scheme can be an acceptable approach to provide coverage for harm caused by AI. However, the owner and the designers of AI can still be exposed to legal suit by the victim (Pagallo, 2013). Further, high insurance premiums shall add to the operating costs and will prove unattractive for businesses to employ AI systems.

## The Second-tier Regulation

The second-tier regulation refers to the soft laws comprising policies and directives issued by the government. Soft laws are considered to be a crucial tool to cushion the exponential development of AI technology. What is considered to be cutting edge technology today may be an outdated technology by, tomorrow. In reality, statutory laws may take a long time to be passed by the Parliament. By the time the law is passed, the problem may have been resolved or become obsolete. Issues on AI demands prompt legal response in order to satisfy industrial expectations. Therefore, soft laws are the most suitable mechanism to deal with emerging issues on AI. The most effective method to come up with soft laws is by way of policy hacking and pitch.

Policy hacking or hack and pitch is a contemporary mantra which has been found to be an effective remedy to cure technology problems by devising innovative solutions. The purpose is to accommodate the fluid changes and challenges that occur within the AI stream. The policy hack converge innovation ecosystem representatives to design solutions for a specific challenge that has been identified from the policy standing or from the government’s perspective. Policy hacking is an effective tool in preventing any regulatory capture but continues to encourage cooperation between the government and the AI industry players. For instance, the UNESCO Mahatma Ghandi Institute of Education for Peace and Sustainable Development partnered with Dell technology for a first of a kind hackathon to challenge teachers to come up with innovative solutions to solve their classroom problems ("UNESCO," 2019). Tesla has also adopted policy hacking in its problem-solving method. Tesla CEO, Elon Musk turned to intensive collaboration between programmers in a hackathon to resolve its Tesla Model 3 production bottleneck due to over reliance on the automation system (Korosec, 2018). Similarly, Startup Europe Comes to Silicon Valley (SEC2SV) mission created and organised by Mind the Bridge (MTB) as part of the Startup Europe Partnership initiative and co-organised with EIT Digital brought together a group of entrepreneurs, investors, and policy experts from both sides of the Atlantic in the Bay Area (Mind the Bridge, 2016). The success in policy hacking led MTB to organise a policy hack for the Directorate-General for Research and Innovation of European Commission on 27 February 2020. The challenge was to find solutions to achieve climate-neutral and smart cities by 2030 using smart mobility solutions and smart construction solutions (Mind the Bridge, 2020). Perhaps, it is apropos for policy hacking to be extended in resolving AI issues especially for regulations on AI.

## CONCLUSION

AI needs its own set of regulations because existing laws may not be able to withstand the challenging legal issues on AI. Stretching the application of conventional laws on AI issues will eventually break at one point. Therefore, AI cannot continue to be left ungoverned by any legal framework because nature abhors a vacuum. However, formulating a feasible AI regulatory framework is more challenging than advocating the rhetorical aspect of regulations. The classical method in drafting regulations based on pure single legal theory is found to be inappropriate in drafting a regulatory framework on AI. Reason being, AI comes with a new set of potential risks which demand proactive regulatory intervention. The kind of regulations intended to be introduced must not only be agile to support the exponential change in the development of AI technology but also, should not constrain the future development of AI. The two-tier formulation in framing AI regulations is therefore necessary and convenient to address current issues on AI. It is a combination between hard law and soft law, where both perform different roles and functions. The first tier will set out the law on the techniques of AI that is to be regulated, the design, experiments, registration, and outlines the liability scheme of AI. Meanwhile the second tier comprising the soft laws, are to be used in dealing with matters which are continuously changing. AI is also susceptible to exponential changes and technological advancements especially those which operate on machine learning techniques. Humans will not be able to foresee the future behaviour of AI because of AI's independence to learn from data. AI's unpredictability will inevitably cause new AI related issues to emerge which demand swift response from the government. These issues can be resolved expeditiously by employing the policy hack and pitch method under the second-tier heading. However, AI will always come with its own set of unpredictable peculiar issues that will challenge the minds of regulators.

## REFERENCES

Abbott, R. (2018). The reasonable Computer: Disrupting the paradigm of tort liability. *The George Washington Law Review, 86*(1).

Ahamed, S. S. R. (2009). Studying the feasibility and importance of software testing: An analysis. *International Journal of Engineering Science and Technology, 1*(3), 120.

Bernama. (2019, April 26). G3 Global and Chinese firms to build AI park in Malaysia. *News Straits Times online*. Retrieved from https://www.nst.com.my/business/2019/04/483219/g3-global-and-chinese-firms-build-ai-park-malaysia

Boehm, F. (2007). Regulatory capture revisited-lessons from economics of corruption. *Research Gate*. Retrieved from https://www.researchgate.net/publication/228374655_Regulatory_Capture_Revisited-Lessons_from_Economics_of_Corruption, 3

Buiten, M. C. (2019). Towards intelligent regulation of artificial intelligence. *European Journal of Risk Regulation*, 43-44.

Buranyi, S. (2017, August 8). Rise of the racist robots-how AI is learning all our worst impulses. *The Guardian UK*. Retrieved from https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses

Calo, R. (2015). Robotics and the lessons of Cyberlaw. *California Law Review, 103*, 513.

Carrigan, C., & Coglianese, C. (2016). George J. Stigler, 'The theory of economic regulation'. In M. Lodge, E. C. Page, & S. J. Balla (Eds.), *Oxford Handbook of Classics in Public Policy and Administration* (p. 287). United Kingdom: Oxford University Press.

Cerka, P., Grigiene, J., & Sirbikytè, G. (2015). Liability for damages caused by Artificial Intelligence. *Computer Law & Security Review*, 2.

Chokshi, N. (2018, May 25). Alexa listening? Amazon echo sent out recording of couple's conversation. *The New York Times.* Retrieved from https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html

Clifford, C. (2017, November 8). Hundreds of A.I. experts echo Elon Musk, Stephen Hawking in call for a ban on killer robots. *CNBC.* Retrieved from https://www.cnbc.com/2017/11/08/ai-experts-join-elon-musk-stephen-hawking-call-for-killer-robot-ban.html

Delvaux, M., Mayer, G., & Boni, M. (2017). Report: With recommendations to the commissions on civil law rules on robotics. *European Parliament*, A8-0005, 7.

Gerstner, M. E. (1993). Liability issues with Artificial Intelligence software. *Santa Clara Law Review, 33*(1), 239.

Holley, P. (2015, January 29). Bill Gates on danger of artificial intelligence: 'I don't understand why some people are not concerned.' *The Washington Post.* Retrieved from. https://www.washingtonpost.com/news/the-switch/wp/2015/01/28/bill-gates-on-dangers-of-artificial-intelligence-dont-understand-why-some-people-are-not-concerned/

Husain, A. (2017). *The sentient machine-the coming age of Artificial Intelligence.* New York, USA: Scribner, 3.

Inn, T. H. (2019, October 14). TPM set to house AI park. *The Star Online*. Retrieved from https://www.thestar.com.my/business/business-news/2019/10/14/tpm-set-to-house-ai-park

Kaplan, J. (2016). *Artificial Intelligence what everyone needs to know*. USA: Oxford University Press, 5-13.

Korosec, K. (2018). Elon Musk is using a hackathon to solve the Tesla model 3 bottleneck. *Fortune.* Retrieved from http://fortune.com/2018/05/14/elon-musk-hackathon-tesla-model-3/

Kurzweil, R. (2006). *The singularity is near-when humans transcend biology*. USA: Viking, Penguin Group, 265.

Leroux, C., et al. (2012, December 31) Suggestion for a green paper on legal issues in robotics-contribution to deliverable D3.2.1 on ELS issues in robotics. *The European Robotics Coordination Action*, 41-54.

Liu, H. W., Lin, C. F., & Chen, Y. J. (2019). Beyond State v Loomis: Artificial Intelligence, government algorithmization and accountability. *International Journal of Law and Information Technology*, *7*.

Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). Disruptive Technologies: Advances that will transform life, business, and the global economy. *McKinsey Global Institute*, 4-19.

McCarthy, J. (2007). *What is Artificial Intelligence*? Stanford University. Retrieved from http://www-formal.stanford.edu/jmc/whatisai.pdf

McCarthy, K. (2018, December 20). 2018 ain't done yet…Amazon sent Alexa recordings of man and girlfriend to stranger. *The Register*. Retrieved from https://www.theregister.co.uk/2018/12/20/amazon_alexa_recordings_stranger/

Mind the Bridge. (2020). Policy Hack 2020. Bruxelles, February 27. *Mind the Bridge*. Retrieved from https://mindthebridge.com/hacking-policy/

Mind the Bridge. (2016). Policy hack-exploring innovative ways to advance policy reform. *Mind the Bridge*. Retrieved from https://mindthebridge.com/hacking-policy/

National Transportation Safety Board. (2016, July 26). Preliminary Report. Highway HWY16FH018N, Executive Summary. *NTSB*. Retrieved from https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY16FH018-preliminary.aspx

Omohundro, S. (2008). *The basic AI drives*. Proceedings of the 2008 Conference on Artificial General Intelligence. Amsterdam: IOS Press, 483-492.

Pagallo, U. (2013). *The laws of robots: Crimes, contracts and torts*. Law Governance and Technology. Series 10. New York: Springer Dordrecht Heidelberg, 105.

Pagallo, U. (2018). Vital, Sophia and Co.-the quest for the legal Personhood of robots. *Information*, *9*(230), 8.

Palmerini, E., Bertolini, A., Battaglia, F., Koops, B-J., Carrevale, A., & Salvini, P. (2016). Robolaw: Towards a European framework for robotics regulation. *Robotics and Autonomous Systems*. Retrieved from http://dx.doi.org/10.1016/j.robot.2016.08.026, 78-85

Parnas, D. L. (2017). Inside risks: The real risks of Artificial Intelligence, incidents from the early days of AI research are instructive in the current AI environment. *Communications of the ACM*, *60*(10), 27-31.

Petit, N. (2017). Law and regulation of Artificial Intelligence and robots: Conceptual framework and normative implications. *SSRN*. Retrieved from https://dx.doi.org/10.2139/ssrn.2931339

Photong, J. (2017, October 31). Alexa plays music without command. *Amazon forum*. Retrieved from https://www.amazonforum.com/forums/devices/echo-alexa/2643-alexa-plays-music-without-command

Poole, D. L., & Mackworth, A. K. (2010). *Artificial Intelligence: Foundations of computational agents*. United Kingdom: Cambridge University Press, 71.

Ravid, S. Y., & Hallisey, S. K. (2018). Equality and privacy by design: Ensuring Artificial Intelligence (AI) is properly trained and fed: A new model of AI data transparency & certification as safe harbour procedures. *SSRN Electronic Journal*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278490

Reed, C. (2018). How should we regulate Artificial Intelligence. *Philosophical Transactions Royal Society*, 2.

Russel, S. J., & Norvig, P. (2010). *Artificial Intelligence a modern approach* (3rd ed.). New Jersey, USA: Prentice Hall, 2.

Santoni de Sio, F. (2016). Ethics and self-driving cars - A white paper on responsible innovation in automated driving system. Department Values, Delft University of Technology. *Technology and Innovation*, 19- 20.

Scherer, M. U. (2016). Regulating Artificial Intelligence systems: Risks, challenges, competencies and strategies. *Harvard Journal of Law and Technology*, *29*(2), 354, 356, 360.

Schirmer, S., Torens, C., Nikodem, F., & Dauer, J. (2018, September 18). Considerations of Artificial Intelligence safety engineering for unmanned aircraft. SAFECOMP 2018 Workshops. Sweden, Proceedings. *SpringerLink*. Retrieved from https://link.springer.com/chapter/10.1007%2F978-3-319-99229-7_40

Sipper, M., & Moore, J. H. (2017). Artificial Intelligence: More human with human. *Bio Data Mining, 10*(34), 1.

Spencer, M. (2019, March 2). Artificial Intelligence regulation may be impossible. *Forbes*. Retrieved from https://www.forbes.com/sites/cognitiveworld/2019/03/02/artificial-intelligence-regulation-will-be-impossible/#e9a87411ed0b

Stevens, L. (1985). *Artificial Intelligence: The search for the perfect machine*. USA: Hayden Book Company, 4.

Sullivan, H. R., & Schweikart, S. J. (2019). Are current tort liability doctrines adequate for addressing injury causes by AI? *AMA Journal of Ethics, 21*(2), 163.

Tesla car that crashed and killed driver was running on Autopilot, firm says. (2018, March 31). *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/mar/31/tesla-car-crash-autopilot-mountain-view

Tucker, E. W. (1965). The morality of law, by Lon L. Fuller. *Indiana Law Review, 40*(2), 274.

UNESCO MGIEP partners with Dell for its Policy Hackathon targeted at teachers in India. (2019, January 18). *UNESCO MGIEP*. Retrieved from https://mgiep.unesco.org/article/unesco-mgiep-partners-with-dell-for-its-policy-hackathon

Wagner, M. O. (2018, February 7). You can't sue a robot: Are existing tort theories ready for Artificial Intelligence? *Frost Brown Todd LLC Attorneys*. Retrieved from https://www.frostbrowntodd.com/resources-you-cant-sue-a-robot-are-existing-tort-theories-ready-for-artificial-intelligence.html

Wakabayashi, D. (2018, March 19). Self-driving Uber car kills Pedestrian in Arizona, where robots roam. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html

Watson, A. (1988). *The digest of Justinian*. Volume 1. Philadelphia, USA: University of Pennsylvania Press. XXV.

Weng, Y. H., Sugahara, Y., Hashimoto, K., & Takanishi, A. (2015). Intersection of 'Tokku' special zone, robots, and the law: A case study on legal impacts to humanoid robots. *International Journal of Social Robotics*, *7*.

Yeoh, O. (2017, August 6). SAVVY: Is AI a danger to humankind? *News Straits Times*. Retrieved from https://www.nst.com.my/lifestyle/sunday-vibes/2017/08/264661/savvy-ai-danger-humankind