SEYBOLD Report
ISSN: 1533 - 9211
https://seyboldreport.net/

# EMERGING ISSUES ON THE RIGHTS OF PRIVACY IN ARTIFICIAL INTELLIGENCE TECHNOLOGY ADOPTION IN MALAYSIA

**S. Kamaruddin[1], Z. Hamin,[2] N.N. Mohd Saufi [3], W. R. Wan Rosli [4], A.R. Abd Rani [5] A.M. Mohamad [6]**

[1]Faculty of Management & Economics, Sultan Idris Education University, 35950, Perak
[2 4 5] Faculty of Law, Universiti Teknologi MARA, Shah Alam 40100, Selangor Darul Ehsan
[3] Faculty of Business Management & Professional Studies, Management & Science University, Shah Alam 40100, Selangor Darul Ehsan
[6] Faculty of Law, University Utara Malaysia
.Email: * [1]saslina@fpe.edu.my, [2]zaiton303@uitm,edu.my [3]nadia_nabila@msu,edu.my [4]rosalili@uitm.edu.my, [5]ridhwanrani@uitm.edu.my and [6]animunirah@uum.edu.my

**ABSTRACT:**
The adoption of artificial intelligence (AI) is rapidly taking hold across global businesses. There was an increase of 32 percent in planned AI adoption in Malaysia since 2017 due to more significant smart cities' initiatives and applications in public safety and intelligent transportation. However, such AI development is beset with privacy and data breaches since the existing data protection law merely protects against personal data's inappropriate use for commercial purposes. The recent trends indicate the failure of the current legal modality to deal with such breaches and the severe gaps in data management and protection. Given the above, this paper aims at examining the legal issues of privacy and data protection and the challenges attached to the adoption of artificial intelligence technology in Malaysia. This research adopts a doctrinal research methodology, a systematic means of legal reasoning, including analyzing the primary and secondary resources. The findings indicate that artificial intelligence evolves; it magnifies the ability to use personal information that may intrude on privacy. Thus, the breach of privacy and the use of personal data without legal supervision or proper governance could result in the deprivation of privacy and abuse of personal data which could be used to commit cybercrime.

**KEYWORDS**: Artificial Intelligence, Privacy, Data Protection, Data Breach, Covıd19 and Malaysia

## 1.0 INTRODUCTION

Artificial intelligence (AI) impersonates certain operations of the human mind, and the term is used when machines can complete tasks that typically require human intelligence (Tegmark, 2017; Makridakis, 2017; Ertel,2018 & Sterne, 2017). At the same time, AI may be misused or behave in unpredicted and potentially harmful ways. The adoption of artificial intelligence (AI) has begun in most service delivery. (Turkle, 2017; Mancini, 2017 & Garcia, 2017). However, in most cases, it augments what humans do and frees them up to take on higher-level tasks such as support in e-commerce, data gathering to name a few (Asaro, 2011; Wallach & Allen, 2008 & Duffy, 2008). The advent of artificial intelligence has triggered several unresolved issues such as software and robot liabilities (Davenport, 2018) privacy and data protection (Buttarelli,

2016; CIPL, 2018). The literature indicates that in AI technology data protection and privacy have become similar concerns for companies and governments (Lafrate, 2018). The data protection laws and norms are currently challenged by the significant advances in modern computers and AI's analytical capacity (Schwab, 2017). Inevitably, it has a serious implication for informational privacy (Moreham, 2008; Mason, 2017; Schwab, 2017). In Malaysia, since 2017, planned AI adoption has increased by 32 per cent due to smart cities initiatives and applications in public safety and intelligent transportation. However, such AI development is beset with privacy and data breaches since the existing data protection law merely protects against the inappropriate use of personal data for commercial purpose. Anand (2018) rightly contends that data privacy protection in the country is hindered by the absence of any privacy law and the courts' reluctance to recognize privacy invasion principles.
Similarly, from the constitutional perspective, Mohd Yusoff (2014) observes that despite the Federal Constitution's recognition of the citizens' fundamental rights, the Constitution does not protect any privacy right. What is clear is that the literature suggests that the existing legal model is inadequate and deficient to protect private information and the intrusion of privacy (Anand, 2018; Mohd Yusoff, 2014; Foong, 2016). Perhaps, the alternative yet of limited protection is through applying foreign principles, particularly the English Common Law principles (Mohd Yusoff, 2014).

In view of the above, the purpose of this paper is to discuss the legal issues of privacy and data protection and the challenges associated with the implementation of artificial intelligence technology in Malaysia. In the first section, the concept of artificial intelligence is discussed. The second segment examines international law and relevant artificial intelligence agreements. The third part is the core of the study and discusses the relevant Malaysia Artificial Intelligence Law. The debate in the fourth section discusses emerging issues centered on the privacy and data protection environment, including the implementation of artificial intelligence technologies during the Covid 19 pandemic, and the final part of the paper concludes the paper.

## 2.0 CONCEPTUALISING ARTIFICIAL INTELLIGENCE

The concept of Artificial intelligence (AI) has been defined differently by different authors. The Council of Europe defines AI as a compilation of sciences, theories, and techniques to reproduce the cognitive ability of a human being through a machine. For example, current developments aim to be able to entrust complex tasks previously delegated from a human to a machine. Tegmark (2021) defines AI as strong and weak AI. It is specifically designed to perform a narrow task on weak AI such as facial recognition or only internet searches or only driving a car.

On the other hand, the Strong concept of AI can be focused on the long-term goal and would outperform humans at nearly every cognitive task (Tegmark, 2021). Also, Negnevitsky (2005) describes AI as a machine, learning how to learn (Negnevitsky, 2005; Stigoe,2018). Humans write initial algorithms for a device that allows the computer to write algorithms afterwards, without additional human supervision or interaction (Negnevitsky, 2005). This process helps

AI always learn from and solve new problems inside an ever-changing world, based on its ongoing data collection (Stilgoe, 2018). The fact that AI systems would also possibly produce large quantities of knowledge is also well known (Luher, 2015; Stilgoe, 2018).

Since AI meaning differs according to the author's concept and understanding, Vas (1999) talk about remarkable developments in AI applications that have led in the public and private sectors to effective use of AI (Vas, 1999). As noted in the 2017 AI Report of the House of Lords of the United Kingdom, "AI is a tool that is already deeply embedded in our lives." As a computational method that can enhance many decision-making processes, the literature indicates that AI enables subject-matter experts in all industries to provide better services and make remarkable breakthroughs (Lauterbach & Bonime-Blanc, 2018). Nowadays, AI technology promotes commercial experiences and customized services and goods, a trend that is highly requested by buyers and customers (Felten, 2016; Lauterbach & Bonime-Blanc, 2018).

On the technological operation of AI, Luger (2005) suggests that AI technology consists of machine learning, based on algorithms that capture, process, and adapt data from the real world (Rubinstein, 2012; Zhuang et al.,2017). The literature available indicates the need for a continuous data supply is significant as AI cannot thrive without a steady supply of data to expand its knowledge base to supplement its development (Luger, 2005; Rubinstein, 2012). Similarly, algorithms without large quantities of personal data cannot reliably learn from their environment. Therefore, the new literature means that AI controllers need to obtain vast quantities of user personal information for algorithms to be taught (Rubinstein, 2012). (Zhuang et al.,2017). Magrani (2019) highlights the importance of law and contemporary ethics in increasing communication and symbiotic contact between people and intelligent machinery. She questions if the machinery has moral character, and which ethical principles for its setting should be followed.

## 3.0 THE INTERNATIONAL LAW ON ARTIFICIAL INTELLIGENCE

The first International Conference on AI and Law was held in Boston in May 1987, the law and AI have steadily developed. The International Conference on Artificial Intelligence and Law (ICAIL) was the explanation for creating the AI and the Law Community. ICAIL has played an essential role in the growth of AI and Law. Many of the field's main ideas were presented at the ICAIL conference and further evolved at successive conferences. Besides, some international organizations have recommended best practices and recommendations rather than legislation. These standards have started to be developed for robotics and have grown into AI standards and principles (Truby,2020).

The United Nations Interregional Crime and Justice Research Institute (UNICRI) founded the AI and Robotics Center at the start of 2015 to build on knowledge from the United Nations' broad artificial intelligence in a single organization. In this regard, the UN Interregional Institute for Crime Science and Justice was created, which focuses on defining and addressing the risks and benefits of AI and robotics from crime and security through awareness-raising,

education, and information sharing and stakeholder harmonization (Garcia,2020). UNICRI has also collaborated with the International Criminal Police Organization (INTERPOL), the International Telecommunications Union (ITU), the Institute of Electrical and Electronics Engineers (IEEE), the Foundation for Responsible Robotics, the World Economic Forum and the Center for Future Intelligence (Garcia,2020).

Similarly, the International Telecommunications Union (ITU) has also been established as a United Nations specialized agency for information and communication technologies (Balbi, & Fickers, 2020). The main objective of ITU is to provide a neutral forum for governments, industry and academia to establish a common understanding of the capabilities of emerging AI technologies and the consequent needs for technical standardization and policy guidance. They also focused on developing strategies to ensure the efficient, secure, and inclusive implementation of AI technologies and equitable access to their benefits (Balbi, & Fickers, 2020).

Also, the Organization for Economic Co-operation and Development (OECD) has made attempts to restrict AI's use in addition to United Nations efforts to regulate or establish the system for AI. The OECD establishes the Artificial Intelligence Suggestion (AI). The OECD Council, on 22 May 2019, approved this as the first Intergovernmental Standard for AI. It is intended that by encouraging the responsible management of trustworthy AI while upholding human rights and democratic principles. The Recommendation seeks to encourage creativity and trust in AI. The Recommendation is designed to support current OECD requirements such as data protection, digital safety risk management and responsible corporate behavior, and to set a framework that is implementable and versatile enough to stand the tests on time in a changing field. The Recommendation addresses AI-specific issues (Puaschunder, 2019). Five complementary value-based concepts for responsible stewardship for trustful AIs and transparency of AI actors have been established in the OECD Recommendation. Inclusive growth, sustainable development and well-being, human-centered principles and justice, openness and robustness of description, protection and security and accountability are among the values (Vöneky, 2020).

In 2018, the next change that could be seen in the legal and regulatory system of AI at the international level was at the European Union (EU). The EU has adopted what has been described as the 'most comprehensive legislation on privacy and security in the world,' the General Data Protection Regulation (GDPR). Several data protection principles are enshrined in the GDPR and regulate entities that 'process personal information of EU citizens or residents' or 'offer products or services to such persons' irrespective of whether those entities are located within the EU. To promote compliance, the GDPR requires the data protection authority of each EU Member State "independent public authorities monitoring" the operation of the GDPR to fine violators, up to EUR 20 million or 4 per cent of the company's worldwide annual revenue from the preceding financial year (Kesa, & Kerikmäe, 2020). Additionally, the GDPR is

encompassed with various principles and rights including the principles of accountability of data users and transparency of such users, the rights of access to personal data, right of data to be forgotten and the right to an explanation of data being collected and stored (Meyer, 2018; Madge, 2018). Ashford (2018) argues that AI developers and suppliers need to adopt a risk-based AI approach, which requires data controllers who process personal data to assess the risks for the data subjects and be accountable for how they handle that data.

## 4.0 GOVERNING AI UNDER THE MALAYSIAN LAW

In Malaysia, it has been pointed out that there is no clear legislation governing artificial intelligence (AI). Early AI software systems will be handled in the same way as other consumer goods. In the case of a failure, liability will be dealt with by the Sales of Goods Act 1957 ('SOGA'), the Consumer Protection Act 1999 ('CPA') and the Torts law, which together serve as a forum for product safety and consumer protection (Lim,2019). The manufacturer or supplier of AI software will also be responsible for any malfunction that results in a violation of these required tacit terms. However, such responsibility would depend on the level of non-compliance with the manufacturer's representations and promises to the supplier and the supplier to the customer in respect of the AI software program (Lim,2019).

The SOGA and the CPA 1999 have enforced some implicit concepts that cannot be omitted when dealing with customers. Implied assurances and conditions include title and lack of encumbrances, communication with definition, adequate or reasonable standard, fitness for purpose, price, and repairs and spare parts (Lim,2019). The CPA's strict liability provision, on the other hand, would have a major effect on negating the defense. However, with the rapid advancement of AI, such as the advent of Google Duplex, AI may no longer be merely a product, but one capable of human mimicry. In such a situation, the legal stance on AI will change significantly (Lim,2019).

Existing research has indicated that within the growth of the AI industry several jurisdictions in the world share similar apprehension about balancing the interests in AI and data protection and privacy issues involved in such technology (Schwab, 2017; Mason, 2017). Processing personal information is not prohibited, but it inevitably affects the individual's rights and interests concerned by the data (Chassang, 2017). The tensions between promoting ICT development and protecting human rights, here personal data of citizens, is also felt in Malaysia as the literature on the existing governance framework or legal model of data protection suggeststhat despite the existence of a personal data protection law in Malaysia, critical legal lacuna remained and balancing such rights are problematic. For example, Kandiah (2017) argues that the new Personal Data Protection Act 2010, which the Commissioner of the Department of Personal Data Protection implemented, imposes stringent conditions on everyone who collects or processes personal data and grants individual rights to data subjects. However, Foong (2016) suggests that the legal model does not include federal and state administrations. A further disadvantage of the existing PDPA governance system is the

exemption from the Personal Data Protection Act (PDPA) for credit reporting agencies (Foong, 2016; Kandiah, 2017). In the past, credit reporting agencies were not monitored in Malaysia and made severe criticisms of inaccurate credit reporting (Kandiah, 2017).

Furthermore, the literature implies that cybersecurity issues resulting from the data breach, let alone from the accumulation of big data in AI technology have not been addressed. The problematic situation of law lagging the technology is noted by Bhasin (2016) who commented that the regulatory framework on PDPA in Malaysia had not developed any specific rules to deal with data privacy issues created by cookies, online tracking, cloud computing, the Internet of things (IoT) or big data. Azmi (2017) contends that Malaysia lacks transparency about what data was involved, which users were affected, and what the public can do about the problem when a breach of personal data incident occurred in cyberspace. Such a situation is caused when the institutions and the current legal model do not provide any protection. Despite the existence of the Personal Data Protection Act 2010, it is less clear whether there is any provision in the said model to find out how personal data has been stolen and whether there is any provision to compensate the victims in the case of a data breach (Kandiah, 2017; Azmi, 2017).

As of April 2017, the Data Information Commissioner has received over 330 official complaints since the law came into force (Kandiah, 2017). Unsurprisingly, approximately 85 per cent of the complaints relate to data processing in the electronic environment (Kandiah, 2017). In 2017, there was a massive data breach affecting the customer data of more than 46 million Malaysian mobile subscribers to an online community forum (Yong, 2018). In late 2018, UiTM students' massive information has been leaked, raising some serious questions about data protection in public sector institutions and organizations (New Straits Times, 2018). Such incidents indicate that despite the data protection law's existence, severe gaps in data management and protection remained (Yong, 2018). Notably, the PDPA 2010 only protects against personal data's inappropriate use for commercial purposes (Yong, 2018; Kandiah, 2017; Foong, 2016). UNICRI

## 5.0 ISSUES ON AI AND RIGHTS OF PRIVACY IN MALAYSIA

As highlighted above, the Personal Data Protection Act 2010 governs artificial intelligence technology and its data processing framework. The lack of a comprehensive legal and regulatory model or standards protecting personal data, particularly in AI technology, has grave implication for data or informational privacy. Existing literature suggests that privacy, in general, is a fundamental human right that warrants legal protection stemming from the principles of human dignity and autonomy (Bloustein, 1964; Parent, 2017; Moreham, 2008). Privacy invasion occurs when there is a failure to show proper regard for human dignity (Mason, 2017). Schwartz (2017) argues that privacy is important because it supports other values essential for human flourishing. Likewise, Bloustein (2018) viewed privacy as an element of human dignity where the award of damages cannot remedy the damage and injury incurred by the breach of privacy and the harm caused by the violation of privacy affects the person and human dignity.

Within the context of AI, the encroachment of privacy has led to significant concerns, mainly because it is no longer the case that a simple few detail about an individual private and professional life are being recorded and stored in metal filing cabinets (Zhuang et al., 2017). Privacy infringement would happen when individuals' lives are being continuously documented, usually without their knowledge, and stored indefinitely due to big data technology and the proliferation of sensors as society moves towards big data and the Internet of things (IoT). Such data are not merely raw data due to the inferences made increasingly by AI and machines that can learn (Zhuang et al., 2017).

Additionally, previous research has highlighted the absence of privacy law and the attendant reluctance of the Malaysian courts to accept the existence of a general principle of privacy invasion that has considerably hindered data privacy protection (Anand, 2018). Mohd Yusoff (2014) observes that despite recognizing the individual rights and liberties in the Federal Constitution, the right to privacy does not have similar express constitutional recognition. Similarly, the research has suggested that the current legal modalities are inadequate and deficient to protect private information and privacy intrusion (Anand, 2018; Mohd Yusoff, 2014; Foong, 2016). The importation of foreign principles through English Common Law's reception offers only limited protection (Mohd Yusoff, 2014). Several commentators have highlighted the dire need for a new and comprehensive legal model governing AI technology (Fiander,2016; Miller, 2018; Zhuang et al., 2017). They argue that the governance frameworks around AI should be technology-neutral and light-touch and should provide regulatory clarity for developing AI technologies and translating them into AI solutions. Also, the recent report of the Centre for Information Policy Leadership (CIPL) suggests that clarifying the application of data protection law is also critical to ensure that scarce resources are not wasted on protecting data that does not impact individuals' privacy rights or otherwise create a risk of harm to them (Centre for Information Policy Leadership, 2018).

Research by Tang (2019) also indicates that Malaysia was ranked fifth-most in securing the personal data of its people, in line with the survey conducted by leading tech firms. The study further underscored that Malaysia had some protections but weakened the category of security. Key evaluation parameters in that survey include constitutional security, legislative protection, privacy protection, data sharing, visual surveillance, identification cards and biometrics, and government access to data. The study results have highlighted Malaysia's participation in a range of significant data breaches involving financial and medical issues (Tang,2019). Among the data breach cases is the massive leakage of personal data from customers of telecommunications service providers, the leakage of almost 20,000 patient records and the leakage of personal data from Malindo Air customers (Tang,2019).

The rights of privacy and data protection are heavily disturbed during the COVID-19 pandemic, which has affected the whole world since late 2019. The COVID-19 pandemic has changed the

way we work, socialize and think, influencing almost every part of our economy, culture and mental health. We think of our privacy, and the significance we attach to our data's security has also had a significant influence on this extreme case. As it has put other constitutional rights into perspective, which until then we would never have allowed being limited by state measures, the pandemic has forced us to balance privacy with health and safety (Ventrella, 2020). According to Rascão (2020), privacy and the right to privacy of data are fundamental rights without guarantees. According to ethical practice, a right is absolute when it surpasses all other considerations, including other rights and freedoms, including the moral obligation of protecting human life and ensuring the economic system's productivity. In the past, emergency states, national interests and exceptional circumstances have allowed for a temporary limitation of constitutional rights. Having been described by the Director-General of the World Health Organization (WHO) as a threat to every country, the COVID-19 pandemic is an unprecedented situation that has led countries worldwide to declare states of emergency. Thus, the pandemic Covid-19 has modified the rights of privacy and data protection of individuals within a country. (Rascão, 2020).

Among the breach of privacy that happens during the pandemic covid, 19 are the processing of certain types of personal data (such as name, home address, workplace, travel information) may be useful in knowing whether an individual may have visited the infected areas or encountered people exposed to the virus, among other items, as a result of a violation of privacy that occurred during a pandemic 19. (Ahmad & Chauhan, 2020). Secondly, it is essential to decide whether the person has infection-related symptoms when processing special categories of Personal Data (such as health data and diagnostic test results). Next, a violation of confidentiality and information data takes the form of utilizing location data and automated contact monitoring. The COVID-19 pandemic encouraged disseminating these methods and instruments, using location data to help pandemic response and monitoring contacts of infected individuals to restrict the virus spread (Ahmad & Chauhan, 2020).

## 6.0 CONCLUSION

It is a truism that the advent of artificial intelligence is generating new ways of conducting our lives, such as business transaction, medical treatment, transportation and delivery of goods and services, to name a few. In the pandemic Covid19 era, AI technology adoption is, without doubt, more beneficial than ever to society. For example, in China, AI-based instruments are deployed at over 30 hospitals that immediately detects chest CT scans suspicious for Covid19, which would enable the medical team to isolate and test those patients quickly. However, like all technological advancement, AI technology is a double-edged sword, which would compromise an individual's personal data, including sensitive personal data and informational privacy when no measures are taken to protect such matters. Hence, to protect Malaysians against data breaches and privacy invasion, Malaysia should create a specific law regulating the use of AI technology and robotics by any industry, sector, or company and also amend and enhance the current Personal Data Protection Act 2010 to be in tandem with the GDPR on the world most

adopted standards governing the processing of data by the artificial intelligence and its technology.

## ACKNOWLEDGMENTS

This research was supported by the Ministry of Education (MOE) through the Fundamental Research Grant Scheme (FRGS/1/2020/SSI0/UPSI/02/12)

## REFERENCES

1. Buttarelli, G (2016) Privacy in an age of hyper-connectivity, available online at https://edps.europa.eu/sites/edp/files/publication/16-11-07_speech_gb_austria_en.pdf
2. Cath, C., Wachter, S., Mittelstadt, B., Taddeo, M., & Floridi, L. (2018). Artificial intelligence and the 'good society': the US, EU, and UK approach. Science and engineering ethics, 24(2), 505-528.
3. Centre for Information Policy Leadership, (2018) First Report: Artificial Intelligence and Data Protection in Tension, available online at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_tepdf
4. Datatilsynet, (2018), Artificial intelligence and privacy, available online at https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf
5. Davenport, T. H. (2018). The AI Advantage: How to Put the Artificial Intelligence Revolution to Work. MIT Press.
6. Deloitte Insight, (2016) Over 100,000 legal roles to be automated, available online at https://legaltechnology.com/deloitte-insight-100000-legal-roles-to-be-automated/
7. Garcia, D. (2017). Preparing for Artificial Intelligence in the Legal Profession. Lexis Practice Advisor Journal,6
8. Iafrate, F. (2018). Artificial Intelligence and Big Data: The Birth of a New Intelligence. John Wiley & Sons.
9. Tegmark, M. (2021). *Benefits & Risks of Artificial Intelligence - Future of Life Institute*. Future of Life Institute. Retrieved 1 February 2021, from https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/?cn-reloaded=1
10. Bench-Capon, T., Araszkiewicz, M., Ashley, K., Atkinson, K., Bex, F., Borges, F., ... & Wyner, A. Z. (2012). A history of AI and Law in 50 papers: 25 years of the international conference on AI and Law. *Artificial Intelligence and Law*, *20*(3), 215-319.
11. Truby, J. (2020). Governing Artificial Intelligence to benefit the UN Sustainable Development Goals. *Sustainable Development*, *28*(4), 946-959.
12. Garcia, E. (2020). Multilateralism and Artificial Intelligence: What Role for the United Nations?. *The Global Politics of Artificial Intelligence*, 1-20.
13. Puaschunder, J. M. (2019, October). The legal and international situation of AI, robotics and big data with attention to healthcare. In *the report on behalf of the European Parliament European Liberal Forum*.

14. Vöneky, S. (2020). Key Elements of Responsible Artificial Intelligence–Disruptive Technologies, Dynamic Law1. *Ordnung der Wissenschaft,(1)*, 9-22.
15. Kesa, A., & Kerikmäe, T. (2020). Artificial Intelligence and the GDPR: inevitable nemeses?. *TalTech Journal of European Studies*, *10*(3), 68-90.
16. Tang, A., (2019). Study: Malaysia the fifth-worst country for personal data protection., available at https://www.thestar.com.my/news/nation/2019/10/16/study-malaysia-the-fifth-worst-country-for-personal-data-protection
17. Ventrella, E. (2020, December). Privacy in emergency circumstances: data protection and the COVID-19 pandemic. In *ERA Forum* (Vol. 21, No. 3, pp. 379-393). Springer Berlin Heidelberg.
18. Rascão, J. P. (2020). Freedom of Expression, Privacy, and Ethical and Social Responsibility in Democracy in the Digital Age. *International Journal of Business Strategy and Automation (IJBSA)*, *1*(3), 1-23.
19. Ahmad, N., & Chauhan, P. (2020). State of Data Privacy During COVID-19. *IEEE Annals of the History of Computing*, *53*(10), 119-122.
20. Yogesh Hole et al 2019 J. Phys.: Conf. Ser. 1362 012121