International Book Chapter - ISBN: 978-623-09-7875-3

CHAPTER II

Safeguarding the Digital Sanctuary: How the Catholic Church Helps to Secure the Digital World in the Age of AI

Steven Wijaya (johnpaul2.cse@gmail.com)
Dorothy Binti Aging (dorothyaging@gmail.com)

STIKAS St. Yohanes Salib – West Kalimantan

Abstract

In an era where the digital landscape is expanding unprecedentedly, the artificial intelligence (AI) and cybersecurity intersection has emerged as a focal point of ethical deliberation. The relentless growth of AI technologies brings myriad challenges, posing profound questions about privacy, human autonomy, and the responsible development and deployment of intelligent systems. In this context, the role of ethical frameworks becomes pivotal in shaping the trajectory of technological advancements and their impact on individuals and societies. This paper seeks to explore a unique and often under-explored dimension of the discourse on AI ethics – the significant contributions of the Catholic Church to the security of the digital world. As an institution with deep-rooted theological and ethical traditions, the Catholic Church brings a rich and nuanced perspective to the ethical considerations surrounding AI and cybersecurity. This exploration is timely and relevant, given the increasing reliance on AI in various sectors and the ethical implications of its widespread adoption.

Keywords: Cybersecurity, Catholic Church, Artificial Intelligence, Ethics

Introduction

Integrating artificial intelligence in various spheres of society has triggered profound ethical considerations (Tronnier et al., 2022). Addressing public safety, security, and privacy concerns becomes increasingly urgent as AI systems advance in complexity and pervasiveness. Furthermore, the inseparable link between AI and cybersecurity has been a subject of growing discourse (Tao et al., 2021). While AI offers enormous prospects for growth and innovation, it also has inherent concerns, notably in cybersecurity (Stahl, 2021)

The Catholic Church, with its longstanding commitment to promoting human dignity and social justice, has actively engaged in the dialogue surrounding AI ethics and cybersecurity. This commitment is further emphasized by the Rome Call for AI Ethics, a statement arguing for human-centric AI ethics principles, indicating a nuanced approach to AI's ethical considerations (Sinibaldi et al., 2020). By actively participating in discussions and initiatives related to AI ethics, the Catholic Church aims to safeguard the digital sanctuary and ensure that technological progress is aligned with human well-being and the common good.

Considering the Church's significant contributions to ethical reflections on AI and cybersecurity, this paper seeks to delve into the ethical considerations put forth by the Catholic Church, providing a comprehensive understanding of the intersection between AI and cybersecurity from a moral and ethical standpoint. This research is critical as it enhances theological conversations about AI and contributes to the broader discussion on addressing the ethical challenges posed by AI and cybersecurity today.

Literature Review

Cybersecurity in the Age of AI

Cybersecurity protects against theft, damage, and unauthorized access to computer systems, networks, and data (Tronnier et al., 2022) (Formosa et al., 2021). As AI technology continues to evolve, it has the potential to enhance cybersecurity measures by detecting, preventing, and responding to cyber threats more effectively than traditional methods (Ghafoor & Khan, 2023).

Adopting AI in cybersecurity, on the other hand, creates additional issues and threats that must be handled. These dangers stem from the possibility that adversaries would use AI technology to launch new assaults and generate new security problems (Batista et al., 2021). Adopting AI in cybersecurity, in particular, raises worries about possible weaknesses and exploiting AI technology for malevolent reasons (Tronnier et al., 2022). As a result, it is critical to comprehend the potential dangers and problems that AI poses to cybersecurity to handle them properly.

Today, there are multiple types of cyber threats in the AI age, which are diverse and ever-evolving, posing complex challenges to the security of computer systems and networks. One of the notable threats is the deployment of AI in cyber-attacks, which enables adversaries to leverage intelligent systems to conduct automated and sophisticated attacks (King et al., 2019). AI-powered cyber-attacks

can autonomously exploit vulnerabilities, adapt to changing defenses, and perpetrate large-scale, targeted intrusions. Adversaries, for example, can utilize AI to develop sophisticated phishing assaults that are difficult to detect or to launch AI-powered malware that can evolve and adapt to security measures.

The emergence of hostile AI attacks is another cybersecurity concern in the age of AI (King et al., 2019). This threat involves the manipulation of AI algorithms through carefully crafted inputs aimed at deceiving or causing erroneous outputs in machine learning models. These manipulations can lead to exploiting vulnerabilities in AI systems, compromising their integrity and reliability. One striking example of adversarial AI attacks is the tampering of autonomous vehicles' perception systems, where malicious actors can trick the AI algorithms into misinterpreting road signs and causing accidents (Park et al., 2019). Furthermore, the proliferation of AI-driven phishing attacks and social engineering poses an imminent threat to cybersecurity (Sayegh, 2023). AI algorithms can generate compelling phishing emails and deceptive content that can evade traditional detection methods. Such advanced phishing tactics can potentially deceive users and organizations, leading to unauthorized access or data breaches.

Moreover, the ethical implications of bias and unfairness in AI systems present a critical cybersecurity threat (Ferrara, 2023). Biased AI algorithms may inadvertently perpetuate discriminatory practices, leading to security vulnerabilities and privacy breaches. For example, narrow AI systems used in facial recognition technology can misidentify individuals, leading to potential security risks and privacy violations. Individually, using AI in healthcare and handling medical data raises concerns about privacy, confidentiality, and discrimination (Hall & Ellis, 2023). For example, AI algorithms employed in medical record systems may access sensitive patient information, raising worries about data privacy and the possibility of unwanted access. Furthermore, using AI in medical decision-making and diagnosis can inadvertently perpetuate biased or discriminatory outcomes, disproportionately impacting specific populations (Esmaeilzadeh, 2020).

Finally, the growing reliance on AI in security systems raises concerns about the possibility of sophisticated adversaries manipulating or deceiving AI. This could result in AI bypassing security measures, gaining unauthorized access, or launching targeted attacks. Hence, AI has become a double-edged sword in cybersecurity (Mitchelson, 2023). In addition to these threats, according to (Lambert et al., 2021), the utilization of AI as a tool within cyber operations has

posed three problems: 1. inadvertent escalation of conflicts due to autonomous decision-making and lack of human oversight, 2. proliferation of the number of cyber operators since AI significantly reduces the human personnel and therefore costs associated with cyber operations, and 3. multiplication of attribution problems by the increasing number of these actors. Cyberspace, thus, thanks to AI, has become a crowded room full of actors with less and less ethics.

With all these threats and obstacles, an ethical framework to govern AI's development, deployment, and usage in cybersecurity is critical. In the following part, we will examine these frameworks in more detail.

Ethical Frameworks in Cybersecurity and AI: A Survey of Existing Literature

Current ethical frameworks in cybersecurity and artificial intelligence (AI) are critical in guiding the proper development, implementation, and usage of AI systems in cybersecurity. These frameworks are intended to address various ethical problems raised by the increased use of AI, such as bias amplification, data privacy, a lack of transparency, human oversight, and accountability (Papagiannidis et al., 2022).

One crucial ethical paradigm in artificial intelligence and cybersecurity is the consideration of the influence on human well-being and the common good (Ebers et al., 2021). This framework suggests the need to ensure that technological advancement, particularly in artificial intelligence and cybersecurity, aligns with human well-being and society's benefit. Another crucial ethical value to be held is transparency and responsibility in designing and deploying AI systems, emphasizing the importance of clear and transparent decision-making procedures and methods to ensure accountability in the event of any ethical or security breaches. (Sonboli et al., 2021).

Many ethical frameworks also address the potential for bias and unfairness in AI systems, particularly in the context of cybersecurity (Ferrara, 2023). These frameworks emphasize the need to detect and correct biases in AI systems to avoid discriminatory practices and security flaws. These frameworks emphasize the need to detect and correct biases in AI systems to avoid discriminatory practices and security flaws. They hence would enhance the security and reliability of AI-driven cybersecurity measures.

Today, a well-received ethical framework for AI and cybersecurity is the Ethics Guidelines for Trustworthy AI by the European Commission (Cannarsa,

2021). This framework emphasizes the principles of transparency, accountability, and fairness, aligning closely with the ethical considerations mentioned above. It aims to ensure that AI systems prioritize human well-being and contribute positively to society. Another notable framework is the Principles for Responsible Stewardship of Trustworthy AI by the Organisation for Economic Co-operation and Development (OECD, 2019). This framework emphasizes the need for transparent and accountable decision-making processes and addresses the potential for bias and unfairness in AI systems. It aligns with concerns about mitigating biases in AI algorithms to prevent discriminatory practices and security vulnerabilities.

These and other frameworks seek to define rules and principles that businesses and governments can utilize to assure responsible and ethical research, implementation, and use of artificial intelligence (AI) in cybersecurity in their particular sectors or regions. However, implementing ethical frameworks for AI and cybersecurity globally poses significant challenges. One of the main difficulties is the varying ethical standards and cultural norms across different regions and countries. What may be considered righteous in one part of the world might not necessarily align with the values and principles of another (Tidjon, 2022).

This makes establishing a universally accepted ethical framework that can be uniformly applied globally is complex. Another challenge lies in the rapid pace of technological advancement and innovation, which often outpaces the development of ethical guidelines and frameworks. As AI and cybersecurity technologies evolve, ethical considerations must keep pace with these advancements, creating a continuous challenge to ensure these frameworks remain relevant and practical (Rudzicz & Saqur, 2020).

Furthermore, enforcement and compliance with ethical standards across borders and jurisdictions present significant obstacles (Cath, 2018). The lack of a unified governance structure for AI and cybersecurity makes it challenging to enforce ethical guidelines consistently, especially when dealing with transnational issues such as data privacy, security, and human rights. Moreover, global networks' sheer complexity and interconnection make properly addressing the ethical implications of AI and cybersecurity extremely difficult. The potential impact of AI and cybersecurity on society, the environment, and human well-being varies across different regions and cultures, making it difficult to develop a one-size-fits-all ethical framework that can address these diverse challenges effectively (Cath, 2018).

Finally, the conflict between privacy and security hinders the global application of ethical frameworks (Agbese et al., 2023). Balancing the need for confidentiality with security measures often involves trade-offs subject to different interpretations and priorities across regions, making reconciling these conflicting interests in a single ethical framework difficult. Therefore, collaboration and cooperation among governments, organizations, and stakeholders become crucial in harmonizing standard ethical practices and enforcing cyber ethics compliance globally. After all, cyberspace is a global ecosystem that transcends borders and jurisdictions. This is the challenge that the Catholic Church, as a universal body with a worldwide reach, can play a significant role in addressing.

Discussion

Historical Perspectives on Technology and Ethics in the Catholic Church

The Catholic Church has a long history of addressing technology-related ethical concerns. Throughout history, the Catholic Church has acknowledged the significance of ethics in technology and its influence on society. Before the rise of artificial intelligence, the Church had wrestled with ethical issues regarding using numerous technologies, including the printing press, radio, television, and the internet. Recognizing the enormous influence of technical breakthroughs on human existence, the Catholic Church has highlighted the need for ethical contemplation and societal concerns in each century.

When the printing press was first introduced in the 15th century, the Church faced moral and ethical dilemmas regarding the potential consequences of mass-produced texts on religious knowledge and interpretation. The dissemination of information through printed materials raised questions about authority, understanding, and the potential for misinformation. In response, the Church emphasized the importance of ethical use of the printing press, advocating for responsible publication and dissemination of religious texts to ensure doctrinal integrity (Penner, 2017). The Church's engagement with ethical reflection during the printing press era demonstrates its commitment to upholding ethical standards while embracing technological advancements for the greater good of society.

Similarly, when radio and television were later introduced, the Catholic Church recognized the power of these technologies to reach and influence large audiences. The Church urged prudent and ethical use of radio and television programs, highlighting the role of these media channels in promoting moral

principles and establishing cultural norms. The Church's involvement in ethical concerns about the use of radio and television reflected its to ensure that these technologies were used for the good of human society rather than the propagation of harmful or immoral content (Pontifical Council of Social Communication, 2000).

Subsequently, in the late 20th century, new ethical considerations emerged for the Catholic Church with the advent of the internet and digital technologies. Considering this, in February 2002, the Pontifical Council for Social Communications released a document titled Ethics in Internet, which addressed the ethical challenges posed by the Internet and highlighted the importance of protecting human dignity and promoting the common good in the digital realm (Pontifical Council of Social Communication, 2002a). The document emphasized that while the internet presented a remarkable opportunity for global communication and access to information, it also brought about ethical concerns, such as disseminating harmful content, privacy issues, and the potential for exploitation. The Church's involvement in ethical questions in the digital age demonstrates its dedication to fostering responsible and ethical use of technology for the benefit of society.

The Pontifical Council for Social Communications also produced a paper titled The Church and the Internet in the same year, emphasizing the need to eliminate the digital divide and give equitable access to technology to all people, particularly those in disadvantaged groups (Pontifical Council of Social Communication, 2002b). In the statement, the Church acknowledges the importance of technology in influencing society and argues for the equitable allocation of digital resources to promote social justice and inclusivity. The Church also addressed ethical concerns over the use of social media, highlighting the necessity of using technology to foster human connection and promote authentic dialogue.

Why did the Catholic Church take so much interest in actively and proactively engaging with the ethical considerations and challenges of the digital world? The reason behind the Catholic Church’s active and proactive engagement with the ethical considerations and challenges posed by the digital world can be found in the document Gaudium et Spes from Vatican II. Here, the Church emphasizes the importance of its involvement in the contemporary world with its joys and hopes (Vatican II, 1965, Gaudium Et Spes [GS], 1). As technology advances at an unprecedented pace, the Church recognizes that it cannot remain indifferent or passive in the face of these developments.

The Church also recognizes in Gaudium et Spes the potential of technology to foster prosperity, peace, and mutual understanding among peoples while acknowledging the risks and ethical concerns associated with them (GS, 57). It emphasizes the need for honest reflection and consideration of the societal implications of technological advancements, aligning with the Church's long-standing tradition of engaging with ethical issues related to technology. Therefore, the Church's active engagement with the ethical considerations of the digital world is rooted in its mission to ensure that technological advancements serve the well-being of humanity and uphold fundamental moral principles. This same mission, which Pope Francis again emphasized in his Encyclic Laudato Si (Francis, 2015), also drives the Church's commitment to safeguarding the digital world in the age of artificial intelligence.

Catholic Church and AI Ethics

Just as the Church has historically been a proponent of ethical reflection in the face of technological advancements, it continues to actively contribute to the ongoing dialogue on the ethical implications of AI. Pope Francis stated in his presentation to the 25th Anniversary General Assembly of the Pontifical Academy for Life in 2019 that artificial intelligence, robotics, and other technological innovations must be so employed that they contribute to the service of humanity and the protection of our common home, rather than to the contrary, as some assessments unfortunately foresee. (Francis, 2019).

The Church stresses the importance of ensuring that AI is developed and implemented in a manner that serves humanity and maintains fundamental ethical principles, with an emphasis on solidarity, justice, and the common good, while also emphasizing the dignity of human beings, created in the image and likeness of God, distinct from any machine or artificial intelligence (Sinibaldi et al., 2020). In this regard, the Church underlines the significance of multidisciplinary collaboration and discourse in navigating the complex ethical terrain of AI and ensuring that its development and usage are consistent with human values and dignity (Sinibaldi et al., 2020).

Focusing on cybersecurity, the Church acknowledges AI's potential risks and challenges, including privacy, autonomy, and the concentration of power (Vatican News, 2021). For the church, ensuring privacy in the age of AI is a paramount concern that cannot be overlooked. The advancement of AI-driven technologies has raised numerous ethical and privacy issues, particularly about

data collection, surveillance, and the potential for infringement on individual autonomy. Integrating AI into various aspects of society, including healthcare, finance, and law enforcement, has raised concerns about protecting personal data and the potential for discriminatory practices based on algorithmic decisions. The Church recognizes the importance of addressing these issues and advocates for robust ethical frameworks and legal safeguards to protect individuals' privacy rights and promote equitable access to and control over AI technologies.

Moreover, the concentration of power in the hands of AI systems, particularly in determining access to resources, opportunities, and information, raises questions about fairness, justice, and preserving human freedom. AI systems are not neutral. They run on algorithms and are trained to achieve specific goals set by their designers or operators, whether for maximizing profit, influencing opinions, or maintaining political control (Stinson, 2022). This underscores the need for ethical considerations in designing, deploying, and regulating AI, acknowledging the potential for abuses and unintended consequences.

In conclusion, the Church's active participation in the current discourse on the ethical implications of AI emphasizes the significance of ethical thought, interdisciplinary collaboration, and societal engagement in addressing the many issues of AI's ethical application. The Church recognizes the importance of a human-centered approach to AI ethics that values human dignity and supports the common good. Through initiatives such as the Rome Call for AI Ethics, the Church aims to foster a dialogue that integrates religious perspectives and values into developing and using AI technologies (Sinibaldi et al., 2020).

Rome Call for AI Ethics: The Church's Formal Contributions to Cybersecurity

In February 2020, the Catholic Church organized an event called Renaissance: A Human-Centric Artificial Intelligence at the Vatican (Sinibaldi et al., 2020). In this historic event, the Church brought together experts from diverse domains, fostering an inclusive dialogue emphasizing the centrality of human dignity, solidarity, and the common good in developing and deploying AI technologies. The formal result of this event is the Rome Call for AI Ethics, signed by PAV's president (Archbishop et al.), Microsoft's president (Brad Smith), IBM's executive vice president (John Kelly III), the Food and Agriculture Administration's director general (Dongyu Qu), and the Minister of Italian Government for Technological Innovation and Digitalization (Paola Pisano).

Central to the Rome Call for AI Ethics is the recognition that new technology must be researched and produced by criteria that ensure it truly serves the entire human family, respecting the inherent dignity of each of its members and all-natural environments, and taking into account the needs of those who are most vulnerable. (RenAIssance Foundation, 2020). This recognition aligns with the Church's long-standing teachings and principles on human dignity and social justice, where the Church's ethical imperative prioritizes the value of the human being for whom technological advancements are intended to benefit. This emphasis on anthropocentrism places human beings at the forefront of moral consideration, promoting human flourishing and limiting harmful intervention.

The Rome Call for AI Ethics proposes six principles for establishing an algorithmic vision that stresses the ethical usage of AI and dramatically contributes to the enhancement of cybersecurity in the AI era. These six principles are:

1. **Transparency**: AI systems must be understood by everyone. This principle ensures that AI-based algorithmic agents' decision-making criteria, purpose, and objectives are transparent and accessible to users. In addition, each individual must be aware that he or she is engaging with a machine. This comprehension will keep people from being misled or influenced by AI systems, resulting in a more secure cyber environment.
2. **Inclusion**: AI technology and cyberspace must reflect the requirements of all individuals without discrimination. Individuals should be given the best possible opportunities to express themselves and develop, with particular emphasis on inclusive access to education and the use of AI to assist those with impairments. This dedication to inclusivity creates a more secure cyber landscape by ensuring all users are considered and safeguarded, lowering the danger of targeted discrimination and exploitation.
3. **Responsibility**: AI creators and deployers must be accountable and transparent in their acts, bearing responsibility for the AI systems' behaviors. All that AI accomplishes is ultimately governed by human accountability. AI inventors and operators are accountable for the outcomes of their work, both purposefully and unintentionally. This idea is strongly related to cybersecurity since accountability and transparency are critical in ensuring that AI systems are built and implemented with integrity and resilience against evil intent, creating a sound foundation for law enforcement.
4. **Impartiality**: AI systems must not produce or behave based on bias to protect fairness and human dignity. The emphasis on impartiality

emphasizes the significance of fairness and equitable treatment in ensuring that AI systems do not replicate or magnify existing social prejudices or discrimination. This is especially true for data used to train machine learning programs, which must be fair and accessible to biases to reduce the possibility of discriminatory behaviors and unethical exploitation of user data by AI systems.

5. **Reliability**: AI systems must be dependable. This approach directly contributes to cybersecurity by ensuring that AI systems fulfill their intended activities consistently and adequately. A reliable AI system lowers the danger of system vulnerabilities and malfunctions, resulting in a more secure digital environment.
6. **Security and privacy**: AI systems must be secure while respecting users' privacy. This principle increases overall cybersecurity by prioritizing user data protection, limiting illegal access to AI systems, and addressing privacy concerns in designing and deploying AI technology.

Incorporating these principles into the development, deployment, and regulation of AI systems will significantly contribute to a more secure cyber landscape, offering protection against potential vulnerabilities, discriminatory practices, and unauthorized access. As AI evolves, incorporating these ethical standards will be critical in protecting digital infrastructure and ensuring that AI technologies are used responsibly and ethically.

The Road Ahead

In the wake of the Rome Call for AI Ethics, the Church has proactively promoted the six algo-ethic principles by engaging with policymakers, industry leaders, and international organizations. The Rome Call has garnered significant support from diverse stakeholders and has become a leading global reference point for AI ethics. Several key initiatives and developments have emerged as a result, including The Abrahamic Commitment to the Rome Call in January 2023, where representatives of the Muslim and Jewish faiths joined the Vatican in signing a commitment to the Rome Call, highlighting the importance of ethical AI development from a religious perspective (RenAIssance Foundation, 2023).

The Rome Call has also catalyzed international collaboration on AI ethics. Several countries and organizations have adopted or developed their AI ethics frameworks, drawing inspiration from the principles outlined in the document. Moreover, many private tech companies have implemented AI ethics principles

and guidelines, demonstrating their commitment to responsible AI development. Despite its significant impact, the Rome Call has challenges. Some critics argue that the document is too vague and lacks concrete recommendations. While the Rome Call for AI Ethics puts forward a human-centric perspective that prioritizes the protection of human dignity and the common good, differing viewpoints emphasize AI's considerable potential to benefit society (Pflanzer et al., 2023).

Proponents of allowing AI to develop without stringent ethical oversight argue that AI technologies have the potential to revolutionize various sectors, including healthcare and finance, leading to significant advancements and improvements in the quality of life for individuals. They believe that overly restrictive ethical guidelines may hinder the full potential of AI, resulting in missed opportunities for innovative solutions to complex societal challenges. They highlight the need for flexibility in AI development, arguing that strict ethical frameworks may stifle creativity and exploration and asserting that AI technology should evolve and adapt without being overly constrained by ethical considerations (Agbese et al., 2023).

This tension between technology and ethics is not unique to AI development but has been a recurring theme throughout history. For instance, the development of nuclear energy raised similar debates about the balance between technological progress and ethical responsibility. The rapid progression of biotechnology also raises similar questions about the ethical boundaries of scientific advancement. In all of these cases, the Church always strives to balance the potential benefits of technology and the ethical implications that arise from its advancements (Congregation for the Doctrine of the Faith, 2008). The Church has always been guided by the eternal principle of human dignity and the common good. It will be vital in fostering dialogue and driving the responsible development and use of technology, including AI.

In conclusion, the Rome Call for AI Ethics has undoubtedly sparked crucial conversations and initiatives, laying the groundwork for a shared global understanding of ethical AI development. It has catalyzed international collaboration, emphasizing the significance of ethical considerations in AI and inspiring various countries and organizations to adopt similar frameworks. Despite ongoing debates and differing viewpoints regarding the ethical implications of AI, the Rome Call has provided a human-centric perspective aimed at prioritizing the protection of human dignity and the common good. As AI technology continues to evolve, the ethical principles outlined in the Rome Call will remain instrumental in guiding responsible AI development and use, aligning with the enduring

commitment to principles of human dignity and moral responsibility upheld by the Catholic Church.

Conclusion

The rise of artificial intelligence has undeniably brought about many benefits and advancements. However, it has also ushered in new cybersecurity risks and challenges, such as AI-powered cyber-attacks, biased AI algorithms, and the over-reliance on AI in security systems, which could pose a double-edged sword.

To face these challenges, ethical frameworks in AI development are essential to mitigate potential risks and ensure responsible utilization of AI technologies. Specific organizations have established several frameworks to address these concerns, including the Ethics Guidelines for Trustworthy AI by European Commission and Principles for Responsible Stewardship of Trustworthy AI by OECD. However, these guidelines tend to be bound to their respective fields and territories. Challenges remain to implement a global framework of AI ethics universally.

In this regard, the Catholic Church, a universal body with global reach, can play an important role. As it has been at the forefront of resolving ethical challenges in other technical developments throughout history, including the printing press, television, and internet, the Church continues to play an active role in shaping the ethical landscape of AI. The Rome Call for AI Ethics has undoubtedly been a significant formal contribution of the Catholic Church to cybersecurity. By emphasizing six algorithmic principles (transparency, inclusion, responsibility, impartiality, reliability, and security and privacy), the Rome Call provides a solid foundation for ethical AI development and use and contributes to creating a more secure digital world.

However, putting these ethical ideas into action is not without difficulties. The conflict between weighing the potential advantages of AI technology against its possible dangers and ensuring that ethical issues are addressed in the development process persists. As the conversation continues, the Catholic Church, motivated by its commitment to defending human dignity and promoting the common good, will always be a vital advocate for safeguarding the digital sanctuary in the future.

References

Agbese, M., Mohanani, R., Khan, A. A., & Abrahamsson, P. (2023). *Implementing AI Ethics: Making Sense of the Ethical Requirements*. https://doi.org/ 10.1145/ 3593434.3593453

Batista, E., Moncusi, M. A., López-Aguilar, P., Martínez-Ballesté, A., & Solanas, A. (2021). *Sensors for Context-Aware Smart Healthcare: A Security Perspective*. https://scite.ai/reports/10.3390/s21206886

Cannarsa, M. (2021). Ethics guidelines for trustworthy AI. *of Lawyering in the Digital Age*.

Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. In *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* (Vol. 376, Issue 2133). https://doi.org/10.1098/rsta.2018.0080

Congregation for the Doctrine of the Faith. (2008). *Instruction Dignitas Personae on Certain Bioethical Questions*. https://www.vatican.va/roman_curi a/ congregate-tions/cfaith/documents/rc_con_cfaith_doc_20081208_dignitas-personae_en.html

Ebers, M., Hoch, V. R. S., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. (2021). *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*. https://doi.org/10.3390/j4040043

Esmaeilzadeh, P. (2020). *Use of AI-based tools for healthcare purposes: a consumer survey study*. https://doi.org/10.1186/s12911-020-01191-1

Ferrara, E. (2023). *Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies (Preprint)*. https://doi.org/ 10.2196/preprints.48399

Formosa, P., Wilson, M., & Richards, D. (2021). *A principlist framework for cybersecurity ethics*. https://doi.org/10.1016/j.cose.2021.102382

Francis. (2019). *Letter of the Holy Father Francis to the President of the Pontifical ...*
https://press.vatican.va/content/salastampa/en/bollettino/pubblico/2019/01/15 /190115a.html

Ghafoor, L., & Khan, M. (2023). *A Threat Detection Model of Cyber-security through Artificial Intelligence*. https://scite.ai/reports/10.31219/osf.io/fq5jy

Hall, P., & Ellis, D. J. (2023). *A systematic review of socio-technical gender bias in AI algorithms*. https://doi.org/10.1108/oir-08-2021-0452

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2019). *Artificial Intelligence*

Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. https://doi.org/10.1007/s11948-018-00081-0

Lambert, D., Thelisson, E., Reichberg, G. M., & Ghanem, A. A. (2021). Human Fraternity in the cyberspace: ethical challenges and opportunities. *Available at SSRN*.

Mitchelson, D. (2023). *The double-edged sword of artificial intelligence in cyber security*. World Economic Forum. https://www.weforum.org/agenda/2023/10/the-double-edged-sword-of-artificial-intelligence-in-cybersecurity/

OECD. (2019). *OECD Principles on Artificial Intelligence - Organisation for Economic Co-operation and Development*. OECD Web Page.

Papagiannidis, E., Enholm, I. M., Dremel, C., Mikalef, P., & Krogstie, J. (2022). *Toward AI Governance: Identifying Best Practices and Potential Barriers and Outcomes*. https://scite.ai/reports/10.1007/s10796-022-10251-y

Park, J., Wen, M., Sung, Y., & Cho, K. (2019). *Multiple Event-Based Simulation Scenario Generation Approach for Autonomous Vehicle Smart Sensors and Devices*. https://doi.org/10.3390/s19204456

Penner, J. (2017). The printing press and religion: A study in reciprocity. In *Ubc*. https://blogs.ubc.ca/etec540sept12/2012/10/27/the-printing-press-and-religion-a-study-in-reciprocity/

Pflanzer, M., Traylor, Z., Lyons, J. B., Dubljević, V., & Nam, C. S. (2023). Ethics in human–AI teaming: principles and perspectives. *AI and Ethics*. https://doi.org/10.1007/s43681-022-00214-z

Pontifical Council of Social Communication. (2000). *Ethics in Communications*. Vatican. https://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20000530_ethics-communications_en.html

Pontifical Council of Social Communication. (2002a). *Ethics in Internet*. https://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_en.html

Pontifical Council of Social Communication. (2002b). *The Church and Internet*. https://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_church-internet_en.html

Renaissance Foundation. (2020). *Rome Call for AI Ethics*. https:// www.romecall.org/wp-content/uploads/2022/03/RomeCall_Paper_web.pdf

Renaissance Foundation. (2023). *AI Ethics: An Abrahamic Commitment to the Rome Call*. https://www.romecall.org/wp-content/uploads/2023/01/AI-Joint-

Decla-ration-5-Jan1-1.pdf

Rudzicz, F., & Saqur, R. (2020). *Ethics of Artificial Intelligence in Surgery*. https://scite.ai/reports/10.48550/arxiv.2007.14302

Sayegh, E. (2023). *Almost Human: The Threat Of AI-Powered Phishing Attacks - Forbes*. https://www.forbes.com/sites/emilsayegh/2023/04/11/almost-human-the-threat-of-ai-powered-phishing-attacks/

Sinibaldi, E., Gastmans, C., Yáñez, M., Lerner, R. M., Kovács, L., Casalone, C., Pegoraro, R., & Paglia, V. (2020). *Contributions from the Catholic Church to ethical reflections in the digital era*. https://doi.org/10.1038/s42256-020-0175-4

Sonboli, N., Smith, J. J., Berenfus, F. C., Burke, R., & Fiesler, C. (2021). *Fairness and Transparency in Recommendation: The Users' Perspective*. https://doi.org /10.1145/3450613.3456835

Stahl, B. C. (2021). *Ethical Issues of AI*. https://doi.org/10.1007/978-3-030-69978-9_4

Stinson, C. (2022). Algorithms are not neutral. *AI and Ethics*, *2*(4), 763–770. https://doi.org/10.1007/s43681-022-00136-w

Tao, F., Akhtar, M. S., & Zhang, J. (2021). *The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey*. https://doi.org/10.4108/eai.7-7-2021.170285

Tidjon, L. N. (2022). *The Different Faces of AI Ethics Across the World: A Principle-Implementation Gap Analysis*. https://doi.org/10.48550/arxiv.2206.03225

Tronnier, F., Pape, S., Löbner, S., & Rannenberg, K. (2022). *A Discussion on Ethical Cybersecurity Issues in Digital Service Chains*. https://doi.org/10.1007/978-3-031-04036-8_10

Vatican II. (1965). *Gaudium et Spes*. https://www.vatican.va/archive/hist_councils/ii_vatican_council/documents/vat-ii_const_19651207_gaudium-et-spes_en.html

Vatican News. (2021). *Vatican meeting explores challenge of artificial intelligence*. https://www.vaticannews.va/en/vatican-city/news/2021-10/vatican-symposium-challenge-artificial-intelligence-society.html

Author Profile:

STEVEN WIJAYA, born in Palembang, 29 December 1987, domiciled in Landak, West Kalimantan - Indonesia, email: johnpaul2.cse@gmail.com. Education: graduated from the Bachelor of Theology Program at STIKAS Santo Yohanes Salib, Bandol in 2022. The current functional position is a postgraduate student in the Master of Theology Program at STIKAS Santo Yohanes Salib, Bandol.

Author's Profile

Dorothy Binti Aging, born in Sabah, Malaysia on March 5, 1972, domiciled in Landak, West Kalimantan – Indonesia, email: dorothyaging@gmail.com Education. Graduated from the Bachelor of Theology Program at the STFT Widya Sasana Malang, Indonesia in 2008. Graduated from the Master's Program at the Pontifical University of Teresianum, Rome in 2012. Work experience: from 2013 until now working as a lecturer at STIKAS Santo Yohanes Salib