IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 2, Ser. 4 (Mar. – Apr. 2024), PP 01-06
www.iosrjournals.org

Ethical And Regulatory Implications Of Ai In Cybersecurity

Badshah Ajminabanu[1], Fatai Kareem[2], Balogun Babatunde[3]
[2](Management And Accounting, Obafemi Awolowo University, Nigeria)
[3](Computer Engineering, Obafemi Awolowo University, Nigeria)

Abstract
In the rapidly changing field of cybersecurity, artificial Intelligence (AI) is seen as a hope and a worry for ethics and rules. This complete research paper explores the possible effects of using AI technology to secure cyberspace. It mainly looks at ethical difficulties and regulatory issues that come with incorporating these technologies into cybersecurity methods. As AI systems are used more often to find, avoid and handle cyber dangers, it raises important questions about privacy, favoritism, responsibility and whether current law arrangements are enough. This article points out the built-in privacy worries associated with AI-powered cybersecurity mechanisms that use data by looking carefully at present practices. It also investigates the potential for algorithmic prejudice and its effects on fair security measures; it dives into a complicated world of responsibility when AI systems go wrong or don't work as expected. This paper also checks worldwide rules, finding places where they might be missing and suggesting clever recommendations to ensure using AI in cybersecurity fits with morals and is controlled by flexible, solid regulations. This article aims to add to conversations about managing the balance between innovative possibilities offered by AI in cybersecurity along with the need for ethical integrity and regulatory adherence. It brings understanding and suggestions for those who create policy, work in technology fields or study ethics while navigating through these complex areas.

Key Word: *Cybersecurity; Artificial Intelligence; Regulatory implications*

Date Of Submission: 11-04-2024 Date Of Acceptance: 21-04-2024

I. Introduction

The beginning of Artificial Intelligence (AI) in cybersecurity ushers a new period where there are improved abilities to fight against more complex cyber dangers. AI's unmatched speed and power in handling large data quantities, finding patterns, and doing predictive analysis are hopeful ways to strengthen cybersecurity methods (Coeckelbergh, 2019). However, using AI technologies in cyber security is challenging. This research article discusses the moral and regulatory effects of using AI in cybersecurity. It highlights the complicated elements that come with merging these two fields.

Artificial Intelligence, which refers to imitating human intelligence processes by machines, especially computer systems, involves learning, reasoning, and self-correction abilities. Cybersecurity can automate the detection of cyber threats, analyze system security in real time, and predict possible weaknesses before bad actors use them. However advantageous this may sound, deploying AI in cybersecurity brings up crucial ethical queries like privacy concerns, maintaining data integrity, avoiding algorithmic prejudice, and holding someone responsible for any damage caused - among other issues (Timmers, 2019). Additionally, because of the increasing popularity of AI-powered cybersecurity tools, the laws and rules about it are finding it difficult to catch up (Jackson, Matei, & Bertino, 2023). This leads to a constantly changing area of legal and ethical discussions.

The primary reason this research is conducted is to explore the complex connection between AI and cybersecurity, giving attention to ethical problems and controlling systems in place. Studying these elements aims to understand how AI can be included in cybersecurity methods ethically and legally. The study has two aims: one is observing the moral factors that come with using AI for protecting against cyber attacks like privacy issues, bias risk and difficulties related to responsibility; secondly, analyzing present as well as future rules which intend to lessen these moral worries while encouraging responsible use of AI technology in cyberspace security domain. This involves not only adapting existing regulations but also fostering a deeper understanding of AI's role within cybersecurity to mitigate potential risks effectively (Cath, 2018).

II. Background And Literature Review

The meeting point between Artificial Intelligence (AI) and cybersecurity is an important study area in the overall conversation about digital safety and the moral use of technology. This section explains how AI works

in cybersecurity, lists the main ethical worries, and looks at current rules and regulations using academic and industry references to provide context for ongoing arguments.

AI in Cybersecurity

Artificial Intelligence (AI) is a group of technologies such as machine learning (ML), natural language processing (NLP), and deep learning—these help systems to do tasks that usually need human Intelligence. In cybersecurity, AI's ability to quickly handle and examine big data sets gives an essential edge in finding irregularities or anomalies, foreseeing possible dangers, and reacting instantly to cyber incidents. The main contributions in this field are automated threat detection systems, where ML algorithms recognize patterns that show signs of a cyberattack, and predictive analytics, which predict upcoming threats by studying past information.

Scholars Toubiana et al. (2020) and Nguyen et al. (2019) say that AI can change and improve cybersecurity defenses. Toubiana et al. discuss in their paper how ML algorithms can better adjust to evolving cyber risks than customary software approaches. On the other hand, Nguyen et al. highlight how AI helps automate the identification and reduction of phishing attacks—among the topmost cybersecurity dangers.

Ethical Implications of AI in Cybersecurity

In cybersecurity, the combination of Artificial Intelligence (AI) brings up a lot of ethical matters that must be handled with caution. As AI becomes more crucial in discovering, stopping, and dealing with cyber dangers, its effects on privacy, prejudice, and responsibility are vital aspects considered essential ethical matters. This section deeply looks at these implications, using current literature and practices to point out the moral problems caused by AI in cybersecurity.

Privacy Concerns

A significant ethical outcome of utilizing AI in cybersecurity is the possible violation of privacy. AI systems often need to use vast amounts of data to find and reduce digital dangers. This information may contain private personal details, which raises worries about user privacy and safeguarding data. The ethical problem comes from the conflict between using AI to protect cybersecurity effectively and maintaining individual privacy rights (Tiwari, 2023).

Privacy concerns increase when AI systems can analyze and deduce personal details from data patterns, possibly revealing more about a person than they have agreed to reveal. The ethics issue is ensuring that AI-managed cybersecurity tools follow the principles of minimal data use and privacy through design. They should only access and handle necessary data with appropriate agreement.

Bias and Fairness

Another important ethical issue is the chance of prejudice within AI algorithms, which might cause unjust or discriminatory results. The training process for AI systems in cybersecurity involves using datasets that could have natural biases due to historical or societal imbalances. If not properly monitored, these prejudices might continue and get magnified by AI, resulting in misbalanced threat evaluations or discriminatory security actions (Naik et al., 2022).

The ethics problem concerns making sure that AI-powered cybersecurity solutions are fair and just. This involves actively looking for biases in training databases and algorithm construction and promoting impartiality to avoid biased outcomes. It is also very important to ensure that AI systems are open, their decisions can be explained, and they don't show bias. This issue underscores the need for ethical frameworks that not only address privacy but also ensure fairness and non-discrimination in AI applications (Gupta, 2023).

Accountability and Transparency

In cybersecurity, the implementation of AI raises concerns about responsibility and openness. This becomes crucial when AI systems make choices that can have serious impacts. The "black box" feature seen in numerous AI algorithms, where the decision-making process is not easily comprehensible by people, makes it difficult to establish accountability for actions guided by these artificial intelligence models (Shubham, Saloni, & Sidra-Tul-Muntaha, 2023).

The important ethical concerns are to ensure a clear understanding of who should answer for the choices made by AI systems and to have methods in place for auditing and reviewing these artificial intelligence decisions. Maintaining transparency about how AI algorithms work and decide things is vital. This becomes more critical when security actions could affect people's rights or ability to use services, highlighting the need for robust ethical governance and international cooperation (Hoffmann et al., 2018).

Regulatory Implications and Responses to AI in Cybersecurity

The increasing blending of Artificial Intelligence (AI) with cybersecurity solutions brings about a fresh time for sophisticated detection and reduction of threats, but it also creates complicated regulatory problems. These difficulties come from requiring rules to control the moral applications of AI, safeguarding the rights of people and maintaining security at national and worldwide levels. This part goes deeply into the consequences of regulation on AI used in cybersecurity. It looks at current structures, finds out where there are holes or missing parts and suggests ways to handle complex rules around this area.

Regulatory Landscape

The legal issues in AI-based cybersecurity are as intricate as the moral problems. Various regions are starting to create regulatory structures to control the utilization of AI, concentrating on guaranteeing privacy, safety, and responsibility. The General Data Protection Regulation (GDPR) of the European Union is frequently mentioned as a prominent law that deals with specific worries related to AI and data privacy. But, according to Scherer (2016), the current rules might not consider exceptional problems created by AI in cybersecurity. These include global collaboration to regulate AI-propelled cyber defenses and maintain equilibrium between advancement and moral restrictions (Scherer, 2016).

Recent literature suggests a delicate way to control AI in cybersecurity, highlighting the importance of regulatory systems being flexible and adjustable as technology grows. Farber and Holzinger (2018) propose that a multi-stakeholder method could help regulate AI. This includes policymakers, industry leaders and civil society to create AI governance structures representing various interests and viewpoints (Farber & Holzinger, 2018)..

Overview of Global Regulatory Responses

Around the world, reactions from regulators to AI in cybersecurity are very different. This shows various legal heritages and norms regarding the importance of privacy and security. The General Data Protection Regulation (GDPR) of the European Union (EU) is an important example that can inspire the handling of some worries linked to AI's effect on privacy. It highlights data protection, consent, and explanation as critical elements in dealing with these concerns. Especially significant are GDPR rules about automated decisions and profiling, which ask for openness and responsibility in processes driven by artificial intelligence (AI) within cybersecurity efforts (European Union General Data Protection Regulation, 2016).

Regulations worldwide have diverse reactions to AI use in cybersecurity, showing a range of legal traditions, attitudes towards privacy, and security priorities. European Union (EU), through its General Data Protection Regulation (GDPR), sets a standard or form for dealing with some worries associated with the impact of artificial intelligence on people's personal lives, especially when considering its effect on privacy matters because it focuses strongly on aspects such as safeguarding data - not only from breaches but also requiring explicit consent before using any individual information -, providing understandable reasons behind decisions made by machines which fall under this category called 'right to explanation'—also stating that when a person disagrees, they can request human review plus possible intervention into confident machine-based choices like those found within areas such as law enforcement or public authority roles where there needs transparency without just depending solely upon algorithms or automated methods alone.

In the United States, regulatory responses are more fragmented. Sector-specific regulations deal with cybersecurity risks, but there isn't a complete legal structure made specifically for AI. The National Institute of Standards and Technology (NIST) offers guidelines and frameworks to improve cybersecurity and privacy via risk management; these indirectly influence AI applications in cybersecurity (NIST, 2018).

Growing economies and global organizations are also dealing with the control of AI in cybersecurity. Activities such as the African Union's Convention on Cyber Security and Personal Data Protection and guidelines from the International Telecommunication Union (ITU) try to find a middle ground between innovation, privacy, and safety.

Case Studies of Regulatory Challenges

Many things could be improved in the regulatory arena. This is shown through famous instances such as data breaches, unfair algorithms, and AI employed for cyberattacks. Such cases focus on the problems related to assigning responsibility for AI-driven actions, safeguarding from AI-supported cyber dangers, and guaranteeing transparency and fairness when applying AI within the cybersecurity field.

A notable problem is controlling AI in independent cyber defense systems. These systems, which can identify and counteract threats in cyberspace without human intervention, create critical legal issues about responsibility, utilizing strength, and observing worldwide law.

III. Methodology

This research article uses mixed methods to investigate ethics and regulation-related issues associated with Artificial Intelligence (AI) in cybersecurity. This methodology aims to comprehensively understand different aspects, such as AI technology, practices in the cybersecurity field, possible ethical concerns or rules, and regulatory structures. The mixed approach includes methods such as qualitative analysis, systematic literature review, and thematic synthesis to examine the present situation of AI in cybersecurity, recognize moral difficulties, and assess regulatory surroundings.

Systematic Literature Review

The basis of this study is a systematic literature review. It was done to assemble and examine scholarly articles, legal papers, and business reports about AI's use in cybersecurity, the ethical effects of AI tech, and current or suggested rules for regulation in these fields. The steps followed during the literature review are

1. Database and Source Selection: Choosing the databases and sources that are suitable, such as IEEE Xplore, ACM Digital Library, PubMed, SSRN and legal databases. This approach helps to cover a broad range of disciplinary viewpoints.
2. Search Strategy: Create a solid search plan by selecting words or phrases linked to AI, cybersecurity, ethics, and regulation. Some typical examples of these search terms are "AI use in cybersecurity," "ethical aspects of artificial intelligence," "AI rules," and "data protection in AI systems."
3. Inclusion and Exclusion Criteria: Explain the standards used to include or exclude documents, considering their publication date (for current information), relation to research queries, and scholarly seriousness.
4. Data Extraction: Planned extraction of essential data from chosen sources; this includes author(s), time of publishing, aims of the study, the way it was done (methodology), main discoveries and conclusions.

Qualitative Analysis

The examination of the gathered literature included qualitative analysis, where data was coded under thematic categories tied to the ethical and regulatory impacts of AI in cybersecurity. This aided in spotting similar themes, patterns, and voids within the literature. For qualitative analysis, NVivo software assisted with coding and theme development.

Thematic Synthesis

After the qualitative analysis, I conducted a thematic synthesis to combine what we found in the literature review. This process was done with the intention of condensing the identified ethical worries and regulatory difficulties from the literature into clear themes. The goal here is to give an organized summary of current knowledge in this area, pointing out where there are agreements, differences, or missing parts on AI's ethical and control impacts within the cybersecurity field.

Ethical Considerations

Since this study concentrated on previously published literature and publicly accessible documents, it did not include gathering primary data from human participants. Nevertheless, moral concerns were crucial in choosing and understanding the sources, making sure to show respect for intellectual ownership and maintain the honesty of the scholarly work that was reviewed.

IV. Discussion

The discussion about the moral and regulatory effects of Artificial Intelligence (AI) in cybersecurity shows a detailed understanding of what can be achieved and the problems that come with this kind of technological combination. This part brings together what has been found in the previous sections, discussing ethical thoughts and rules situations. It also thinks about how much control is needed for new ideas to grow while looking forward to possible future directions in AI and cybersecurity.

Balancing Innovation and Regulation

A critical and current issue where AI and cybersecurity meet is to discover a suitable equilibrium between encouraging technological creativity and ensuring there is enough ethical and regulatory supervision (Coeckelbergh, 2019).. The fast growth of AI, along with its use within cybersecurity, requires a regulatory method that can be flexible but also strong, one which changes with new improvements while maintaining protection for privacy, fairness and responsibility (Cath, 2018).

The previous ethical consequences raised, such as worries about privacy, prejudice, and responsibility, emphasize the necessity for an ethical structure to steer the growth and implementation of AI in cybersecurity (Taddeo & Floridi, 2018). This framework should promote openness and accountable utilization of AI, making certain that technologies are created with moral factors foremost in mind.

Likewise, the regulatory difficulties and answers mentioned indicate a divided picture where various local methods in AI control could obstruct worldwide teamwork and responses to cyber dangers. The suggestion of worldwide rules and better cooperation between public and private sectors shows a way to align these attempts, pushing for unified views on using AI ethically in cybersecurity (Jackson, Matei, & Bertino, 2023).

Anticipating Future Trends

With the development of AI technologies, changes in cybersecurity ethics and regulations will indeed happen. A new pattern is coming up, which includes using AI for self-governing cyber defence systems. Even though this is a positive thing because it helps better recognize and react to threats, important ethical and regulatory issues are associated with it. These problems mainly relate to decision-making independence and possible unplanned impacts.

The double use of AI technologies is also problematic. This means that progress made for defensive cybersecurity can be changed to offensive cyber operations. The concept of dual-use in AI highlights how crucial worldwide collaboration and control are to avoid the misapplication of artificial intelligence technology in cyber warfare and cybercrime.

Moreover, the rise of quantum computing will bring about future problems for AI in cybersecurity. This could make existing encryption techniques useless and require a reassessment of how data is protected and ensure privacy (Abushgra, 2023). The moral and controlling structures discussed should be flexible enough to adjust for these and other unexpected technological progressions that may occur soon.

Ethical AI as a Competitive Advantage

A change in thinking that stands out is how important it has become to view ethical AI practices as a competitive edge within the cybersecurity sector. Recognizing companies that focus on ethics when using AI can set them apart from others, creating trust between users and those involved in their services. This trend shows an encouraging path towards a future where the demonstration of correct ethics and regulation compliance becomes a trademark for creativity and superiority in AI-supported cybersecurity solutions (Du & Xie, 2020).

V. Conclusion

Examining the ethical and regulatory aspects of artificial intelligence (AI) for cybersecurity shows it is a complicated but hopeful situation. This research has emphasized the possible changes AI can bring to improve safety measures, bringing new skills like identifying threats, forecasting them and reacting effectively against them. Yet it also highlights critical moral worries such as privacy problems, potential prejudice risks, and concerns about responsibility and openness. As discussed, the regulatory environment is changing currently. Different places use different methods to balance encouraging creativity and guaranteeing moral rules while safeguarding data.This article has given an overview of the role of AI in cybersecurity and its effects on ethics and regulations. A systematic literature review, qualitative analysis and thematic synthesis aimed to identify the main themes and challenges related to these ethical and regulatory aspects. This review can guide policymakers, technologists, and ethicists in dealing responsibly with AI's abilities within the field of cybersecurity.

Proposals

Solving the regulatory problems caused by AI in cybersecurity is complex and requires a many-sided method that incorporates national and worldwide strategies. Some suggestions for future regulation are as follows:

Establishing International Rules: Working together via worldwide organizations to set up uniform rules for the ethical usage of AI in cybersecurity. This method would assist in aligning regulations over different areas, making cooperation and sharing easier.

Boosting Transparency and Responsibility: Making it a legal obligation to be transparent about the AI algorithms and decision-making methods applied in cybersecurity. This might include requiring audit trails, assessments of impact, and public reporting on security measures related to artificial intelligence.

Building Collaborative Relationships: By developing partnerships between governments, industry, academia and society, platforms can be created for sharing knowledge about best practices and ethical guidelines. Such collaborations would greatly aid in policy-making processes. Partnerships between public and private entities could also contribute to educating human resources on the ethical use of AI within cybersecurity.

Alteration of Regulations: Adjusting current legal systems to handle AI's distinct difficulties, like data protection, prejudice, and self-governing decision-making. This could possibly mean forming fresh regulatory organizations or mechanisms, particularly for AI and cyber security.

Future Work

Heading into the future, this will help us comprehend better and give a practical understanding of the accountable combination of AI in cybersecurity:

International Regulatory Cooperation: For the upcoming research, the ways to improve international cooperation in AI regulation within cybersecurity needs to be investigated. It should involve creating worldwide norms and structures that facilitate easy sharing of data across borders along with cyber threat knowledge, respecting each country's independence while guaranteeing a united global reaction against cyber dangers.

Ethical AI Development Frameworks: In-depth research is required on how to use ethical frameworks while developing AI, especially in cybersecurity. This includes looking into suitable methods for including privacy by design, ensuring algorithm fairness and increasing transparency within AI systems.

Impact of Emerging Technologies: The possible influence of new technologies like quantum computing on AI-powered cybersecurity solutions offers great potential for upcoming investigation. Research should examine how these technologies could change the cybersecurity field, including the difficulties and opportunities they bring to AI applications.

AI for Training in Cybersecurity: AI's involvement in cybersecurity is rising, creating a requirement to investigate how adequately training the coming group of professionals can be. This may involve assessing what skills and understanding are necessary for working efficiently with AI technologies and then creating educational programs and training modules that meet these requirements.

Ethical AI for a Competitive Edge: More studies can examine how considering ethics in AI creation and use could become a competitive advantage for cybersecurity businesses. This might involve looking at real situations, like companies that have incorporated ethical AI methods and what effect it has had on their place in the market or trust from stakeholders.

References

[1] Abushgra, A. (2023). How Quantum Computing Impacts Cyber Security. 2023 Intelligent Methods, Systems, And Applications (Imsa), 74-79. Https://Doi.Org/10.1109/Imsa58542.2023.10217756.

[2] Bostrom, N., & Yudkowsky, E. (2014). "The Ethics Of Artificial Intelligence." In K. Frankish & W. M. Ramsey (Eds.), *The Cambridge Handbook Of Artificial Intelligence*. Cambridge: Cambridge University Press, Pp. 316-334. Https://Doi.Org/10.1017/Cbo9781139046855.020

[3] Cath, C. (2018). Governing Artificial Intelligence: Ethical, Legal And Technical Opportunities And Challenges. Philosophical Transactions Of The Royal Society A: Mathematical, Physical And Engineering Sciences.

[4] Coeckelbergh, M. (2019). Artificial Intelligence: Some Ethical Issues And Regulatory Challenges. , 2019, 31-34. Https://Doi.Org/10.26116/Techreg.2019.003.

[5] European Union General Data Protection Regulation. (2016). Retrieved From Https://Eur-Lex.Europa.Eu/Eli/Reg/2016/679/Oj

[6] Farber, D. A., & Holzinger, M. G. (2018). Regulation Of Artificial Intelligence: The United States And European Union Approaches.

[7] Gupta, N. (2023). Artificial Intelligence Ethics And Fairness: A Study To Address Bias And Fairness Issues In Ai Systems, And The Ethical Implications Of Ai Applications. Revista Review Index Journal Of Multidisciplinary. Https://Doi.Org/10.31305/Rrijm2023.V03.N02.004.

[8] Hleg Ai. (2019). "Ethics Guidelines For Trustworthy Ai." High-Level Expert Group On Artificial Intelligence Set Up By The European Commission. Https://Ec.Europa.Eu/Futurium/En/Ai-Alliance-Consultation/Guidelines#Top

[9] Hoffmann, A., Roberts, S., Wolf, C., & Wood, S. (2018). Beyond Fairness, Accountability, And Transparency In The Ethics Of Algorithms: Contributions And Perspectives From Lis. Proceedings Of The Association For Information Science And Technology, 55, 694 - 696. Https://Doi.Org/10.1002/Pra2.2018.14505501084.

[10] Jackson, D., Matei, S., & Bertino, E. (2023). Artificial Intelligence Ethics Education In Cybersecurity: Challenges And Opportunities: A Focus Group Report. Arxiv, Abs/2311.00903. Https://Doi.Org/10.48550/Arxiv.2311.00903.

[11] Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). "The Ethics Of Algorithms: Mapping The Debate." Big Data & Society, 3(2). Https://Doi.Org/10.1177/2053951716679679

[12] Modhoriye, P., Yadav, P., & Jadhav, D. (2023). Ai Transformation In Business: Unveiling The Dual Effects Of Advancement And Challenges. Interantional Journal Of Scientific Research In Engineering And Management. Https://Doi.Org/10.55041/Ijsrem27359.

[13] Naik, N., Hameed, B., Shetty, D., Swain, D., Shah, M., Paul, R., Aggarwal, K., Ibrahim, S., Patil, V., Smriti, K., Shetty, S., Rai, B., Chłosta, P., & Somani, B. (2022). Legal And Ethical Consideration In Artificial Intelligence In Healthcare: Who Takes Responsibility?. Frontiers In Surgery, 9. Https://Doi.Org/10.3389/Fsurg.2022.862322.

[14] National Institute Of Standards And Technology (Nist). (2018). Framework For Improving Critical Infrastructure Cybersecurity, Version 1.1. Available At: Https://Nvlpubs.Nist.Gov/Nistpubs/Cswp/Nist.Cswp.04162018.Pdf

[15] Pagallo, U. (2018). The Laws Of Robots: Crimes, Contracts, And Torts. Springer. Https://Link.Springer.Com/Book/10.1007/978-94-007-6564-1

[16] Ryan, M., & Stahl, B. C. (2020). Artificial Intelligence Ethics Guidelines For Developers And Users: Clarifying Their Content And Normative Implications. Journal Of Information, Communication And Ethics In Society, 18(2), 159-178. Https://Doi.Org/10.1108/Jices-09-2019-0102

[17] Scherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, And Strategies. Harvard Journal Of Law & Technology, 29(2), 353-400

[18] Shubham, S., Saloni, S., & , S. (2023). Data And Science Engineering: The Ethical Dilemma Of Our Time-Exploring Privacy Breaches, Algorithmic Biases, And The Need For Transparency. World Journal Of Advanced Research And Reviews. Https://Doi.Org/10.30574/Wjarr.2023.18.1.0677.

[19] Taddeo, M., & Floridi, L. (2018). Regulate Artificial Intelligence To Avert Cyber Arms Race. Nature, 556(7701), 296-298. Https://Doi.Org/10.1038/D41586-018-04602-6

[20] Tilanus, W. (2018). Best Practices For Gdpr Compliant Deployment Of Xmpp. Https://Xmpp.Org/Extensions/Inbox/Gdpr.Html

[21] Timmers, P. (2019). Ethics Of Ai And Cybersecurity When Sovereignty Is At Stake. Minds And Machines, 29, 635 - 645. Https://Doi.Org/10.1007/S11023-019-09508-4.