Linguistic and Philosophical Investigations
ISSN: 1841-2394, e-ISSN: 2471-0881
Vol 23 (1), 2024
pp. 386–396

Ethical Concerns in Computational Linguistic Field National Defense: A Philosophical Investigation of Language and Security

Mhd Halkis
Associate Professor of Philosophy, Indonesia Defense University
Jl. Salemba Raya, No. 14 Kenari District. Monday, Jakarta 10440.
https://orcid.org/ 0000-0003-0122-4594
Email: halkis@idul.ac.id

Abstract: This research examines ethical issues in computational linguistics that can be applied to national defense by analyzing philosophical and security language. The increasing use of language contexts, such as intelligence and communication data analysis, raises ethical and philosophical challenges related to privacy, control, and accuracy. This research aims to identify and analyze ethical issues, especially in the use of computational linguistics in defense applications, as well as their implications for the protection of individual rights and privacy. This method involves reviewing ethical technology references and analyzing the philosophical design of language and security. Deontological and utilitarian ethical theories are applied to evaluate the moral impacts and consequences of using the language of technology in a defense context. The results demonstrate that using linguistics in defense can pose privacy risks, misuse of data, and the potential for significant bias in decision-making. This often involves collecting data from multiple sources, creating challenges to ensure data is managed ethically and responsibly. Conclusion: This shows the need for a solid ethical and regulatory framework to ensure technology's fair and responsible use in context defense. Implications of the findings include the need for ongoing dialogue between technology developers, policymakers, and the public to mitigate ethical risks and ensure that application technologies comply with critical and security principles. With a comprehensive and responsible approach, technological linguistics can improve military safety and effectiveness without compromising individual rights and privacy.

Keywords: Computational Linguistic, Technology Ethics, National Defense, Privacy and Security, Philosophical Analysis

Received: 12 May 2024 **Revised:** 27 June 2024 **Accepted:** 15 July 2024

1. Introduction

The rapid growth of technological linguistics over the past few decades has brought changes in various fields, including defense. The technology, including natural language data analysis, machine translation, and voice recognition (Collins et al., 2023,p.19), is increasingly used in military applications such as intelligence analysis, communications strategy, and cyber operations. The application of technology in a defense context raises complex ethical challenges and requirements that are addressed in depth (Benotti et al., 2023,p.28).

First, one of the issues that arise from the use of computational linguistics in defense is privacy. Technology is the ability to analyze and store large amounts of personal data collected from various sources. According to Hovy and Spruit (2016), technological language experiences can significantly influence personal lives, mainly when data is used without unambiguous and informative consent (Hovy & Spruit, 2016, p. 591).

Additionally, Benotti et al. (2023) point out the importance of transparency in the data collection and analysis to ensure that individual privacy is not violated (Benotti et al., 2023, p. 4).

Apart from privacy, control of data and information is also receiving attention. The application of computational linguistics in defense contexts and often involves collecting data from multiple sources, which can lead to authority issues and data control. According to Klein et al. (2017), open tools for machine translation can help increase transparency and accountability in language data management; however, they still require strict regulation to avoid abuse (Klein et al., 2017, p. 28). In a military context, tight information is required to prevent possible data leaks that threaten security.

Accuracy and internal bias in decision-making are ethically important. Linguistic algorithms are often developed based on the likelihood that data sets contain inherent biases that are amplified by the algorithm (Vaccino-Salvadore S., 2023). Hovy and Spruit (2016) note that biases in language experiences can broadly impact society, including in military contexts, where biased decisions can be made, leading to unfair or discriminatory actions (Hovy & Spruit, 2016, p. 595). Therefore, bias mitigation is an essential step in development and implementation.

The implications are philosophical and computational linguistics in defense also deserves attention. The use of technology raises questions about the relationship between the state and citizens and between decision-makers and data subjects. State-controlled technology for military purposes can strengthen control over populations and potentially threaten individual freedoms. According to Benotti et al. (2023), it is essential to implement a framework that considers basic human ethical principles to prevent abuse of power (Benotti et al., 2023, p. 5).

Furthermore, transparency and accountability are essential in ensuring the responsible use of linguistic technology to compute answers. According to Analytics Steps (2023), technology developers must develop easy-to-understand and audit models to ensure technology is used ethically and responsibly (Analytics Steps, 2023). Transparency in operational algorithms and decision-making accountability can help reduce risk abuse and increase public trust in technology.

To face ethical challenges, a solid regulatory framework is needed to ensure fair and responsible use of technology and language in context defense. Regulations must include privacy protection, strict data controls, bias mitigation, and enforcement of transparency and accountability. For technological applications to safeguard society's interests and security principles, it is also critical to promote constant communication between technology developers, legislators, and society (Verdonik , D. 2023).

In a military context, technological developments in linguistics must always be accompanied by deep ethical considerations to avoid potential misuse and negative impacts on individuals and society (Peters, M. E., et al. (2018).. This research provides insight into the comprehensive challenges and ethical intersections and offers recommendations for addressing issues to ensure that linguistic technologies are used responsibly and ethically in defense applications.

2. Literature Review

The literature on ethics in linguistics is computational. For application defense, researchers have identified various challenges and solutions. This study combines perspectives from multiple fields, including the language of technology, philosophy, and ethics, to explore the ethical and philosophical implications of using the language of technology in a military context.

The ethical considerations of computational linguistic technology has attracted attention in many studies. Hovy and Spruit (2016) emphasize that the social impact of Natural Language Processing (NLP) is quite significant, especially in the military context Brown, T. B., et al. (2020).. These technologies can amplify or reduce social bias depending on how the algorithms are developed and implemented (Limatta, A. 2023) . They highlighted the importance of identifying and reducing bias in data sets and algorithms to ensure fair and accurate results (Hovy & Spruit, 2016, p. 591). Benotti et al. (2023) added that ethics in NLP writing and reviewing is essential to ensure the technology is used responsibly. Transparency in the technology development is essential to minimize risk abuse and increase accountability, especially in the military context (Benotti et al., 2023, p. 4).

Privacy and data control are two issues frequently discussed in the linguistics literature. Klein et al. (2017) demonstrated that open machine translation tools can help increase transparency and accountability in language data management Clark K. et al. (2019). However, they still require strict regulations to prevent abuse. In the military context, protecting individual privacy is even more critical because data misuse for such purposes is unethical (Klein et al., 2017, p. 28). Analytics Steps (2023) highlighted the importance of a multifaceted approach to addressing ethical challenges in NLP, including engineering bias reduction and explainable AI. They emphasize that technology developers should focus on developing more effortless and more accessible models to ensure that technology is used ethically and responsibly (Analytics Steps, 2023).

Accuracy and internal bias in decision-making are critical to the ethics of using technological linguistics in defense. Hovy and Spruit (2016) noted that biases in technological language experiences can have far-reaching social impacts, including in military contexts, where biased decisions can be made, leading to unfair or discriminatory actions. Therefore, bias mitigation is essential in technology development and implementation (Hovy & Spruit, 2016, p. 595). McCrae and Cillessen (2021) found that using interoperable lexical data can help reduce internal bias. This shows the importance of accurate data that is free from the defense of applying an internal bias to ensure fair and informed decisions (Mccrae & Cillessen, 2021, p. 8).

The philosophical implications of using computational linguistics in defense are also essential to consider. These technologies raise questions about the relationship between states and citizens and between decision-makers and data subjects. Ethical theories, both deontological and utilitarian, can be applied to evaluate the moral impacts and consequences of using the language of technology in context defense. According to ethical theory, an action is considered ethical if it is by predetermined moral obligations without regard to consequences. In context, using these technologies violates language privacy or reinforces social bias (Yang, Z., et al. 2019). This cannot be ethically justified, even though it may result in strategic military benefits. In contrast, utilitarianism and judgment ethics are based on the results or consequences of actions (Devlin, J., et al.,2019). Implementing computational linguistic technology means using technology that optimizes safety and security while minimizing negative impacts on individuals and society, which can be considered ethical (Benotti et al., 2023, p. 5; Analytics Steps, 2023).

Transparency and accountability are essential aspects of the use of linguistic technology, including language gestures (Chen, Y., & Adolphs, S. 2023). According to Analytics Steps (2023), technology developers should focus on developing easy-to-understand and auditable models to ensure that technology is used ethically and responsibly. Transparency in algorithm operation and accountability in decision-making can help reduce risk abuse and increase public trust in technology. Benotti et al. (2023) emphasized the importance of transparency in technology development to minimize risk abuse and increase accountability. In the military context, transparency is essential because decisions made based on language data analysis can have far-reaching consequences (Benotti et al., 2023, p. 6).

To address ethical challenges, a solid regulatory framework is needed to ensure the fair and responsible use of technology and language in the context of national defense. Regulations must include privacy protection, strict data controls, bias mitigation, and law enforcement transparency and accountability. Additionally, it is essential to encourage ongoing dialogues between technology developers, policymakers, and society to ensure that application technologies comply with critical and security principles (Liu, Q. et al. 2020). Benotti et al. (2023) demonstrated that active participation from various stakeholders can help create a more comprehensive and responsive framework for development technologies (Benotti et al., 2023, p. 7).

3. Methodology

This study aims to identify and analyze the main ethical issues arising from the use of computational linguistics in application defense and its philosophical implications for security and human rights. The methodology used in this research involves a qualitative approach with three main steps: literature review, concept analysis, and case study.

The first step in this research was a comprehensive literature review. Overview: It covers relevant ethical technologies, computational linguistics, and defense application literature. Sources used include journals, books, research reports, and conference articles. We searched the literature using academic databases such

as Google Scholar, IEEE EXplore, SpringerLink, and ACL Anthology. The References review focuses on identifying recognized ethical challenges in using technological language in military contexts and solutions proposed by previous researchers. Hovy and Spruit (2016) emphasize the importance of understanding the social impact of natural language processing (NLP) and how technological biases can influence outcomes and decisions (Beinborn, L. and Hollenstein; N., 2024). They highlight the need for transparency and accountability in developing NLP algorithms. Additionally, Benotti et al. (2023) emphasize the importance of ethics in NLP writing and reviewing to ensure that the technology is used responsibly and moderately.

The second step is concept analysis, where ethical theories, deontological and utilitarian, are applied. Computational linguistic technology can be used to evaluate or assess the moral consequences it causes. The deontological ethical theory proposed by Immanuel Kant emphasizes the importance of appropriate actions with moral obligations without considering the consequences. In context, violating individual technological privacy or reinforcing social bias is considered unethical, even though this may provide strategic advantages for the military. In contrast, the Utilitarian ethical theory popularized by John Stuart Mill assesses ethics based on the results or consequences of actions. This approach considers optimizing the safety and security of technology nationally and minimizing negative impacts on individuals and society as ethical actions. This analysis helps in understanding the implications of using technological language in a defense context and provides a basis for more ethical evaluation.

The third step is to study cases conducted to illustrate the application of computational linguistic technologies in defense contexts and to challenge emerging ethics. A case study is selected based on relevance and availability of sufficient data for analysis. This includes analysis of data from operations involving the military that use technology—the language for intelligence, surveillance, and strategic communications (Lipton, Z. C. 2018). Each case study is analyzed to identify specific ethical challenges, such as privacy, data control, accuracy, bias, transparency, and accountability. For example, research by Klein et al. (2017) regarding machine translation tools shows how essential regulations are to prevent the misuse of language data during military operations (Doshi-Velez, F., and Kim, B. 2017). The analysis also evaluates how technology impacts the relationship between the state and citizens and between decision-makers and data subjects.

The internal data collection process involves literature and data from various secondary sources. Academic databases are used to access journals, books and study reports (Liu, Y., et al. 2019. Additionally, non-academic sources such as policy reports, government documents, and news articles were also used to gain more perspectives on ethical issues in the use of language technology in the field of defense and security. Once the data is collected, it is analyzed qualitatively to identify major thematic patterns that are relevant to the study questions. Analysis This includes content analysis and thematic analysis techniques to effectively evaluate data and provide in-depth and productive comprehensive insights into the issues and ethics discussed.

Data triangulation is essential to ensure the validity and reliability of the findings. Data triangulation involves using multiple data sources and analysis methods to ensure consistency and accuracy (Tang, Z., & Surdeanu , M. 2023). Data from academic literature was compared with data from non-academic sources to validate results and identify possible inconsistencies (Jurgens, Tsvetkov and Jurafsky, 2017). Additionally, peer review and consultation with experts in the fields of ethical technology and computational linguistics were conducted to ensure that academic and ethical standards studied the analysis and findings. Approach This helps ensure that the study findings are reliable and relevant for developing responsible policies and practices regarding the use of technological language in defense.

4. Research Results and Discussion

This study identifies and analyzes the main ethical issues arising from using computational linguistics in application defense. The following research results are discussed in depth based on the main findings:

4.1 Privacy

One of the main ethical issues discovered in this research is privacy. Computational linguistic technologies used in national defense often involve collecting and analyzing language data from various sources,

including personal communications data and intelligence data. According to Hovy and Spruit (2016), language processing experiences can significantly influence individuals due to the technology's ability to access and analyze personal data without the explicit consent of the individual concerned (Hovy & Spruit, 2016, p. 591). Unauthorized use of data can raise profound concerns about what that data looks like. Collected, stored and used, and who has access to it.

Additionally, Benotti et al. (2023) highlight the importance of transparency in data collection and analysis to protect individual rights (Benotti et al., 2023, p. 4). Transparency in the use of technology is essential to build trust between users and service providers. With sufficient transparency, users may feel that their data is being misused or used in a way that is in line with their wishes.

In a military context, privacy violations can occur when data is used for unethical purposes or without adequate oversight. If strict regulations exist, the use of technological, linguistic, and computational surveillance can result in violations of citizens' privacy. Excessive surveillance can result in unnecessary data collection and dangerous misuse of information. Therefore, it is important to implement policies and regulations that protect individuals and ensure that data use is carried out transparently and ethically.

For example, using computational linguistics technology in intelligence analysis requires collecting data from various sources, including private and public communications data. With proper oversight, this data can be used for unethical purposes and with the consent of the individuals involved. Klein et al. (2017) show that the use of machine translation tools can increase the transparency and accountability of language data management, even broader semantic understanding (Kraska- Szlenk , I., & Wójtowicz , B. 2023); however, they still require strict regulations To avoid abuse (Klein et al., 2017, p. 28).

Therefore, it is essential to implement policies and regulations that protect individuals' privacy and ensure that data use is carried out transparently and ethically. Benotti et al. (2023) also show that data collection and analysis transparency can help reduce risk abuse and increase public trust in technology (Benotti et al., 2023, p. 6). Transparency can be achieved through transparent reporting about how data is collected, stored and used and who has access to the data. This way, users feel more secure and confident that their data will not be misused.

The use of technological linguistics in military contexts also raises challenges related to data monitoring and control. Data collected for objective defense is often sensitive, capable, and contains valuable information. Therefore, it is important to ensure that this data is managed carefully and only used for lawful purposes. Strict regulations are needed to ensure that data is not misused and individual privacy is protected.

Additionally, it is important to consider the ethical implications of data collection and use in a military context. Data for objective surveillance or intelligence must be used by considering individual privacy and ensuring that the data is used responsibly. For example, collecting data from private communications without permission could be considered a serious invasion of privacy and should be avoided. Benotti et al. (2023) emphasize that technology developers must ensure that data collection and analysis is carried out transparently and ethically (Benotti et al., 2023, p. 6).

Privacy breaches can also occur when data is used for unauthorized purposes or without adequate oversight. For example, using computational linguistic technologies to monitor communications can result in data misuse and personal privacy breaches. Therefore, it is important to ensure that data use is carried out in a transparent and ethical manner and that strict regulations are implemented to protect individual privacy.

Overall, privacy is an ethical issue in the use of linguistic technology in military contexts. Protective policies and regulations must be implemented to protect individual privacy and ensure that data use is conducted transparently and ethically. Technology can increase safety and effectiveness in military operations without compromising individual privacy.

4.2 Data Control

Control of data collected and analyzed using linguistic technologies is also an ethically significant issue. Klein, et al. (2017) show that open machine translation tools can help increase transparency and

accountability in language data management; however, strict regulations are needed to prevent abuse (Klein et al., 2017, p. 28). In-app defense, strict data controls are necessary to ensure that the data collected is only used for legitimate purposes and is not misused for the benefit of others.

The use of technology in the military often involves collecting data from various sources, including private and public data. The the public's emotional state also needs to be understood more deeply. (Mohammad, 2022). This raises the challenge of ensuring that data is managed ethically and responsibly. Strict regulations and strict oversight are needed to ensure data is not misused and individual control over personal data (Saif, M. 2022).

Data collection from various sources includes highly informative sensitive information that, if not managed properly, poses significant risks to individual privacy and security. According to Benotti et al. (2023), transparency in the data collection and analysis process is essential to ensure that individual rights are protected and that such data is used ethically (Benotti et al., 2023, p. 6). Strict oversight is necessary to prevent data misuse and ensure that data is used only for forgotten purposes, as agreed to by the individual concerned.

For example, in a military context, data collected for intelligence analysis must be managed very carefully to prevent misuse of available information and compromise individual privacy. Strict oversight is necessary to ensure that this data is only used for lawful purposes and to protect authorized individuals. According to Hovy and Spruit (2016), technological language experiences can significantly influence individuals. Therefore, strict data control is needed to prevent misuse (Hovy & Spruit, 2016, p. 591).

Additionally, regulations are needed to ensure the data collected is used responsibly. Klein et al. (2017) emphasize that strict regulations are needed to prevent data misuse and ensure data is managed transparently and accountably (Klein et al., 2017, p. 28). This regulation should include adequate oversight mechanisms to ensure that data is not misused and that individuals have control over their data.

Strict regulations are also policies that must be implemented to protect individual privacy and ensure that data is only used for lawful purposes. Benotti et al. (2023) emphasize that transparency in data collection and analysis is essential to ensure that individual rights are protected and that data is used ethically (Benotti et al., 2023, p. 4). Strict regulations are needed to ensure that data is misused and that individuals have control over personal data.

To face these challenges, a multifaceted approach is needed to develop further models that are easy to understand and audit to ensure that the technology is used ethically and responsibly (Step, 2023). Transparency in algorithm operation and accountability in decision-making can help reduce risk abuse and increase public trust in technology.

Data control is an ethically significant issue in the use of computational linguistic technologies in the context of National Defense. Strict policies and regulations must be implemented to protect individual privacy and ensure that data is used transparently and ethically. Strict oversight and regulations are necessary to ensure that data is not misused and that individuals have control over their personal data. Only with a comprehensive and responsible approach can technology be used to improve military safety and effectiveness without compromising individual privacy.

4.3 Accuracy and bias in decision making

Accuracy and internal bias in decision-making are other ethics found in this research. Hovy and Spruit (2016) note that bias in technological language experiences can have far-reaching impacts, including in military contexts, where biased decisions can be made, leading to unfair or discriminatory actions (Hovy & Spruit, 2016, p. 595). Technology Linguistics is often developed based on the likelihood that data sets contain inherent biases, which algorithms can then amplify. Therefore, bias mitigation becomes an important step in developing and applying computational linguistics to ensure that decisions based on data analysis are fair and accurate.

McCrae and Cillessen (2021) investigated the integration between WordNet and Wikidata and found that using interoperable lexical data can help reduce internal bias when making decisions regarding language (Kim, E.-Y. 2023). Interoperable lexical data may constitute a more holistic and accurate analysis, which in

turn helps identify and reduce internal biases in decision-making. This shows the importance of accurate data free from internal bias to ensure fair and informed decisions (Mccrae & Cillessen, 2021, p. 8).

Implementing more transparent and capable audited algorithms is also an important step in reducing bias and increasing accuracy in decision-making. Transparency in the algorithm means third parties can check and verify the decision-making process, which helps identify and correct possible biases Alamillo, A. R., et al. (2023). According to Benotti et al. (2023), transparency in the development and implementation of NLP technology is essential to ensure that the technology is used responsibly and minimizes the risk of internal bias when making decisions (Benotti et al., 2023, p. 6).

Additionally, there is a more holistic and multifaceted approach to building technology. Computational Linguistic can help identify and reduce bias. Analytics Steps (2023) highlights the importance of these approaches, including engineering bias reduction and explanatory AI, to ensure fair and accurate data-based decision-making (Analytics Steps, 2023).

In a military context, decisions based on biased data analysis can have significant consequences, including unfair or discriminatory actions. Therefore, it is important to ensure that the data used for analysis is accurate and free of bias and that the algorithms used to make decisions are transparent and auditable. Hovy and Spruit (2016) emphasize that bias in technological language experiences can have far-reaching impacts, including in military contexts, where biased decisions can be made, leading to unfair or discriminatory actions (Hovy & Spruit, 2016, p. 595).

In addition to mitigating bias, improving decision accuracy is also important in using linguistic technology. Implementing a more transparent and capable audit algorithm can help increase accuracy in decision-making with the possibility of verification and validation by third parties. Transparency in the algorithms and data used allows for a more accurate and reliable decision-making process. According to McCrae and Cillessen (2021), the use of interoperable lexical data can help ensure that the data used is accurate and free of bias, which in turn increases accuracy in decision-making (McCrae & Cillessen, 2021, p. 8).

Thus, accuracy and bias in decision-making are ethically significant issues in the use of linguistic technology in military contexts. Mitigating bias and improving accuracy are important steps to ensure fair and accurate decisions based on data analysis. Transparency in the algorithms and data used, as well as a holistic approach to developing technology, will help reduce bias and increase accuracy in decision-making. Just ensure that the data used is accurate and free of bias and that the algorithms used are transparent and auditable. This technology can be used ethically and responsibly in the field of National Defense.

4.4 Philosophical implications

The use of linguistics is computational in application defence has implications for the deep philosophical relationships between states and citizens and between decision-makers and data subjects. According to ethical theory, an action is considered ethical if it is carried out in accordance with predetermined moral obligations without paying attention to the consequences. Currently, the use of technology that violates individuals' language privacy or reinforces social bias is considered unethical, even though doing so may result in strategic benefits for the military (Hovy & Spruit, 2016, p. 591; Benotti et al., 2023, p. 4).

In contrast, Utilitarian ethics in judgment ethics are based on the results or consequences of actions. In the application of computational linguistic technology, the use of technology that optimizes national defense and national security while minimizing negative impacts on individuals and society can be considered ethical. This analysis helps understand the implications of using language technology in context defense and provides a basis for a more in-depth ethical evaluation (Benotti et al., 2023, p. 6; Analytics Steps, 2023).

The philosophical implications involve issues of control and power. States'States' use of linguistic technologies can strengthen their control over populations, thereby threatening individual and fundamental human rights. According to theoretical ethics, deontological violations of basic rights such as privacy can be justified even if the goal is defense and national security. In this case, applying technological language that does not respect individual privacy and freedom is considered unethical (Klein et al., 2017, p. 28).

On the other hand, from a utilitarian perspective, an action can be considered ethical if its consequences

are greater for the safety and security of society as a whole. However, careful evaluation is needed to determine how negative impacts on individuals are balanced by collective benefits. Utilitarian theory demands that overall benefits must exceed individual harms for actions to be considered ethical (McCrae & Cillessen, 2021, p. 8).

In addition, transparency and accountability in the use of technology are important philosophies. Transparency means that decisions regarding capturing and using data can be audited and verified by parties, which helps ensure that technology is used ethically and responsibly (Benotti et al., 2023, p. 6). Accountability ensures that responsible parties answer questions about technology use.

Other philosophical implications include considerations of the balance between security and freedom. In a military context, the military often presents a tension between the need to maintain security and the obligation to protect individual rights. Deontological ethical theories emphasize that the moral obligation to respect individual rights must be a priority, while utilitarian theories emphasize the importance of favourable outcomes for safety and security.

Use of Computational Linguistic Technology in Context National defense and security demands clear policies and strict regulations to ensure that ethical principles are respected. Such policies should include privacy protections, oversight of data use, and mechanisms to reduce bias and increase accuracy when making decisions (Hovy & Spruit, 2016, p. 595; Analytics Steps, 2023).

Thus, the philosophical implications of technological linguistics in defense application are complex and demand a careful and responsible approach. Ethical theories, deontological and utilitarian, offer useful frameworks for evaluating the moral impact and consequences of technology use. Only by considering the ethical and philosophical aspects of computational linguistic technology can it be used responsibly and ethically in national defense and state security.

4.5 Transparency and Accountability

Transparency and accountability are important aspects of the use of linguistic technology. Analytics Steps (2023) emphasizes that technology developers must focus on developing more easy-to-understand and auditable models to ensure that technology is used ethically and responsibly (Analytics Steps, 2023). Transparency in algorithms' operation and decision-making accountability can help reduce risk abuse and increase public trust in technology.

Benotti et al. (2023) emphasize the importance of transparency in the technology development process to minimize risk of abuse and increase accountability. In the military context, transparency is important because decisions based on language data analysis can have far-reaching consequences (Benotti et al., 2023, p. 6; Lan, Z., et al.,2020). The absence of transparent decisions can give rise to distrust and potential abuse of power, which can negatively impact relations between the military and society.

Transparency in operating algorithms means third parties can audit and verify the decision-making process. This allows for independent oversight to ensure the algorithm is used fairly and ethically. Accountability in decision-making ensures that the responsible party answers questions about the use of technology (Rajpurkar , P., Jia, R. and Liang, P. 2018). These can be identified and questioned if abuse occurs. Therefore, transparency and accountability are carried out thoroughly to create fair and acceptable trust.

Research shows that using linguistic technology in national defense and security raises several complex ethical challenges. These challenges include privacy, data control, accuracy, bias, transparency, and accountability. Ethical, deontological, and utilitarian theoretical approaches offer practical frameworks for evaluating technology use's moral impact and consequences. Deontological ethical theories emphasize the importance of actions by moral obligations without considering the consequences, and temporary theories of Utilitarian ethics assess ethics based on the results or consequences of actions (Hovy & Spruit, 2016, p. 591; Benotti et al., 2023, p. 4).

Fair and responsible use of language technology requires an intense regulatory framework and ongoing dialogue between technology developers, policymakers and society (Radford, A., et al. 2018; Liu, Q., et al. 2020)). Strong regulation will ensure individual privacy is protected, strict data controls are implemented, and mitigation can be implemented effectively. In addition, transparency and accountability in decision-

making will increase people's trust in technology and ensure that technology is used ethically and responsibly (Klein et al., 2017, p. 28; Analytics Steps, 2023).

In a military context, it is important to implement clear policies and strict regulations To ensure that ethical principles are adhered to. The policy should include privacy protections, oversight of data use, and mechanisms to reduce bias and increase accuracy when making decisions. With answers to a comprehensive and responsible approach, technology linguistics can be used to increase national defense and effectiveness in military operations without compromising individual privacy (McCrae & Cillessen, 2021, p. 8; Hovy & Spruit, 2016, p. 595).

5. Conclusion

This study examines ethics in computing linguistics to be applied in national defense through philosophical and security language analysis. From the results of this research, we can conclude that the potential of computational linguistics technology not only greatly enhances the effectiveness of military operations but also raises a number of significant ethical challenges and needs that are addressed comprehensively. The challenges include privacy, data control, accuracy, bias, transparency and accountability, and more, and require specific and precise regulations.

Privacy is one of the main issues in the use of linguistic technology in the context of national defense and security. Technologies that enable the collection and analysis of personal data on a large scale may result in violations of individual privacy, if it's not properly set. In addition, strict data controls are required to ensure that the data collected is only used for legitimate purposes and is not misused for the benefit of others. The use of technology often involves collecting data from multiple sources, creating challenges in ensuring that data are managed ethically and responsibly. Bias mitigation and increasing accuracy in decision-making are also important to ensure that technology is used fairly and responsibly.

The implications are philosophical, and the use of technology is important to consider. Using computational linguistics in national defense raises questions about the relationship between states and citizens, as well as between decision-makers and owners' data. Ethical theories, deontological and utilitarian, provide a useful framework for evaluating the moral impact and consequences of technology use. Deontological ethical theories emphasize that violating the privacy of individual actions or reinforcing social biases cannot be ethically justified, even though they may result in strategic advantages for the military. In contrast, utilitarian ethics assumes that technology is optimized for safety and security interests. National law is ethical as long as the negative impact on individuals and society can be minimized.

Facing ethical challenges requires a solid regulatory framework that can guarantee fair and responsible use of technology and language in a national defense context. Regulations must include privacy protection, strict data controls, bias mitigation, and law enforcement transparency and accountability. Additionally, it is important to encourage ongoing dialogue between technology developers, policymakers, and society to ensure that application technologies comply with fundamental human rights and security. Overall, research has shown that despite the technology linguistics is computational, its potential is quite large to improve abilities in field operations and national defense. However, the application of technology must be accompanied by deep ethical considerations and strict regulations to avoid impacts on individuals and society.

References

[1] Benotti, L., Fort, K., Kan, M.Y., & Tsvetkov, Y. (2023). Understanding Ethics in NLP Authoring and Reviewing. Proceedings of the 17th Conference of the European Chapter of the Association for Computational Linguistics: Tutorial Abstracts. doi:10.18653/v1/2023.eacl-tutorials.4

[2] Collins L, Brezina V, Demjén Z, Semino E, Woods A. Corpus linguistics and clinical psychology: Investigating personification in first-person accounts of voice-hearing. Int J Corpus Linguist. 2023 Jan;28(1):28-59. doi : 10.1075/ijcl.21019.col. Epub on Apr. 29, 2022. PMID: 37090241; PMCID: PMC7614468.

[3] Hovy , D., & Spruit, S. L. (2016). Social impact of natural language processing. Annual Meeting of the Association for Computational Linguistics, 591-598. doi:10.18653/v1/P16-2096

[4] Jurgens, D., Tsvetkov, Y., & Jurafsky , D. (2017). Incorporating dialectal variability into socially equitable language identification. Annual Meeting of the Association for Computational Linguistics, 51-57. doi:10.18653/v1/P17-2009

[5] Klein, G., Kim, Y., Deng, Y., Senellart , J., & Rush, A. M. (2017). OpenNMT: Open-Source Toolkit for neural machine translation. ArXiv.

[6] Kraska- Szlenk , I., & Wójtowicz , B. (2023). Derivation and semantic autonomy: A corpus study of Polish głowa "head" and its diminutive główka. International Journal of Corpus Linguistics, 28 (1), 1-27. doi:10.1075/ijcl.28.1

[7] Limatta, A. (2023). Register variations across text lengths: Evidence from social media. International Journal of Corpus Linguistics, 28 (2), 202–231. doi:10.1075/ijcl.28.2

[8] Vaccino-Salvadore S. (2023). Exploring the Ethical Dimensions of Using ChatGPT in Language Learning and Beyond. Languages 8 (3), 191. doi:10.3390/languages8030191

[9] Beinborn, L. and Hollenstein, N. (2024). Cognitive Plausibility in Natural Language Processing. Computational Linguistics, 50 (1). https://direct.mit.edu/coli/issue/50/1

[10] Tang, Z., & Surdeanu , M. (2023). It Takes Two Flints to Make a Fire: Multitask Learning of Neural Relation and Explanation Classifiers. Computational Linguistics, 49 (1), 117-156. https://doi.org/10.1162/coli_a_00419

[11] Chen, Y., & Adolphs, S. (2023). Toward a corpus-based description of speech gesture units of meaning: The case of the circular gesture. International Journal of Corpus Linguistics, 28 (2), 172-201. doi:10.1075/ijcl.28.2

[12] Kim, E.-Y. (2023). A corpus-based study of anglicized neologisms in Korea: A diachronic approach to Korean and English word pairs. International Journal of Corpus Linguistics, 28 (2), 125–143. doi:10.1075/ijcl.28.2

[13] Verdonik , D. (2023). Annotating dialogue acts in speech data: Problematic issues and basic dialogue act categories. International Journal of Corpus Linguistics, 28 (2), 144-171. doi:10.1075/ijcl.28.2

[14] Châu, Q. H., and Bulté , B. (2023). Comparison of automated and manual analyses of syntactic complexity in L2 English writing. International Journal of Corpus Linguistics, 28 (2), 232-256. doi:10.1075/ijcl.28.2

[15] Alamillo, A.R., Moreno, D.T., González, E.M., Acosta, M.T., & Taroni , A. (2023). Analysis of Synonymy and Antonymy in Discourse Relations: An Interpretable Modeling Approach. Computational Linguistics, 49 (2), 429-464. https://doi.org/10.1162/coli_a_00425

[16] Brown, T.B.; Mann, B.; Ryder, N.; Subbiah, M.; Kaplan, J.; Dhariwal, P.;... & Amodei, D. (2020). Language models are few-shot learners. Advances in Neural Information Processing Systems, 33, 1877-1901.

[17] Devlin, J., Chang, M.-W., Lee, K., & Terranova, K. (2019). BERT: Pretraining of Deep Bidirectional Transformers for Language Understanding. Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers), 4171-4186. doi:10.18653/v1/N19-1423

[18] Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., ... & Stoyanovi, V. (2019). Roberta: Robustly Optimized BERT Pretraining Approach. arXiv preprint arXiv:1907.11692

[19] Radford, A., Narasimhan, K., Salimans , T., & Sutskever , I. (2018). Improving language understanding via generative pretraining. OpenAI Blog.

[20] Rafael, C., Shazeer, N., Roberts, A., Lee, K., Parang, S., Matena, M., ... & Liu, P. J. (2020). Exploring the Limits of Transfer Learning with Unified Text-to-Text Transformer. Journal of Machine Learning Research, 21 (140), 1–67.

[21] Yang, Z., Dai, Z., Yang, Y., Carbonell, J., Salakhutdinov, R., & Le, Q. V. (2019). XLNet: Generalized Autoregressive Pretraining for Language Understanding. Advances in Neural Information Processing Systems, pp. 32, 5753–5763.

[22] Lan, Z., Chen, M., Goodman, S., Gimpel, K., Sharma, P., & Soricut, R. (2020). ALBERT: A Lite BERT for Self-supervised Learning of Language Representations. International Conference on Learning Representations.

[23] Clark, K., Kandelia, U., Levy, O., & Manning, C. D. (2019). What does BERT observe? Analysis of BERT's Attention. Proceedings of the 2019 ACL Workshop BlackboxNLP: Analyzing and Interpreting Neural Networks for NLP, pp. 276–286. doi:10.18653/v1/W19-4828

[24] Peters, M. E., Neumann, M., Iyyer, M., Gardner, M., Clark, C., Lee, K., & Zettlemoyer, L. (2018). Deep contextualized word representations. Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers), pp. 2227–2237. doi:10.18653/v1/N18-1202

[25] Liu, Q., Chen, P., Ji, Y., Li, X., & Shi, S. (2020). You Impress Me: Dialog Generation via Mutual Persona Perception. Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP), pp. 2927–2937. doi:10.18653/v1/2020.emnlp-main.237

[26] Doshi-Velez, F., and Kim, B. (2017). To develop a rigorous science of interpretable machine learning. arXiv preprint arXiv:1702.08608.

[27] Lipton, Z. C. (2018). The myth of model interpretability. Communications of the ACM, 61 (10), 36-43. doi:10.1145/3233231

[28] Rajpurkar , P., Jia, R. and Liang, P. (2018). Know What You Don't Know: Unanswerable Questions for SQuAD.,Proceedings of the 56th Annual Meeting of the Association

[29] Saif, M. (2022). Ethics Sheet for Automatic Emotion Recognition and Sentiment Analysis. Computational Linguistics, 48 (2), 239–278. doi:10.1162/coli_a_00433.

[30] S. M. Mohammad, “Ethics Sheet for Automatic Emotion Recognition and Sentiment Analysis,” Comput. Linguist., vol. 48, no. 2, pp. 239–278, 2022, doi: 10.1162/coli_a_00433