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 .Kec. Senin, Jakarta 10440.
https://orcid.org/ 0000-0003-0122-4594
Email: halkis@idu.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 caused changes in various fields, including defense. These technologies, including NLP (Natural Language Processing) analysis, machine translation, and speech recognition, are increasingly being used in military applications such as intelligence analysis, communications strategy, and cyber operations (Elder, 2020). The application of technology in the defense context poses complex ethical challenges and requirements that are discussed in depth.

First, an issue that arises from the use of computational linguistics in advocacy is privacy. Technology enables the analysis and storage of large amounts of personal data collected from various sources. According to Hovy and Spruit (2021), the experience of a technological language can significantly impact an individual's personal life, especially when data are used without clear and informed consent (Hovy and Prabhumoye, 2021). In addition, Benotti et al. (2023) highlighted the importance of data transparency to ensure that individual privacy is not violated.

In addition to privacy, data and information control are also of concern. The application of computational linguistics in the defense context often involves collecting data from multiple sources, which can raise issues regarding authority and data control (Benotti *et al.*, 2023). According to Klein et al. (2017), open tools for machine translation can help increase transparency and accountability in the management of language data; however, such tools still require strict regulations to avoid misuse. In the military context, strict information is required to prevent potential data leaks that threaten national security. On the other hand, the defense agencies of countries around the world continue to increase their AI capabilities to maintain superiority (Klein *et al.*, 2017).

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

The implication is that philosophical and computational linguistics in defense also deserves attention. The use of technology raises questions about the relationship between the state and its 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), applying a framework that considers basic human ethical principles to prevent abuse of power is important.

Furthermore, transparency and accountability are essential in ensuring the responsible use of linguistic technology to compute answers. Technology developers should focus on creating easy-to-understand and auditable models to ensure ethical and responsible use of technology. This approach enhances transparency and fosters trust among users and stakeholders by allowing for thorough examination and validation of the technology's processes and outcomes (Saeidnia *et al.*, 2024). Transparency in operational algorithms and accountability for decision-making can help reduce the risk of misuse and increase public trust in the technology.

Many existing regulations do not specifically address the issue of bias in language algorithms. This bias can lead to discrimination based on race, gender, or other factors if not managed properly. Existing regulations focus more on privacy and data security aspects but do not sufficiently consider how bias can undermine fairness and accountability. Regulations such as the GDPR and the AI Act focus on specific regions (e.g., the European Union), but AI and NLP technologies are often used globally. This poses challenges in enforcing regulations in countries outside the jurisdiction of legislators. The lack of global harmonization in AI and language technology regulations can lead to legal ambiguity for companies operating in different countries[6].

A robust regulatory framework is needed to address ethical challenges and ensure fair and responsible use of technology and language in defense contexts. Regulations should include privacy protection, strict data controls, bias mitigation, and enforcement of transparency and accountability. For technology applications to protect society's interests and the principle of security, it is also important to promote constant communication between technology developers, legislators, and society (Darinka Verdonik, 2020).

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. This study provides insights into comprehensive challenges and ethical intersections. It offers recommendations for addressing these issues to ensure that linguistic technologies are used responsibly and ethically in defense applications.

2. Literature Review

The advancement of AI technology also poses new ethical challenges in the military context, especially related to decision-making involving human life. Applying the computational ethics framework in military ethics can help develop AI systems that are efficient and in accordance with moral principles that have long been the basis for military decision-making, thereby strengthening the integrity and legitimacy of military action in the era of advanced technology. The advancement of AI technology also poses new ethical challenges in the military context, especially related to decision-making involving human life. Applying the computational ethics framework in military ethics can help develop AI systems that are efficient and in accordance with moral principles that have long been the basis for military decision-making, thereby strengthening the integrity and legitimacy of military action in the era of advanced technology (Rashid *et al.*, 2023).

Ethical considerations in computational linguistics technology are becoming increasingly important as algorithms are increasingly used to make important decisions for humans. The article "Artificial Intelligence: A Powerful Paradigm for Scientific Research" discusses how advances in AI and the availability of large amounts of human behavioural data have increased the reliance on algorithms for decision-making in various contexts, including access to credit, medical care, and hiring processes. While algorithms can produce more objective decisions than humans, who are prone to bias, conflicts of interest, or fatigue, there are concerns that this process can lead to privacy violations, information asymmetry, opacity, and discrimination. In this context, computational linguistics technology also faces similar challenges, especially in ensuring that the systems developed are fair, accountable, and transparent while respecting privacy. Therefore, the adoption of technical solutions that focus on data ownership, accountability, transparency, and fairness is urgent, especially when these technologies are used in contexts that significantly impact human lives (Lepri, Oliver and Pentland, 2021).

Hovy and Spruit (2016) emphasize the significant social impact of NLP, especially in the military context. This technology can amplify or reduce social biases depending on how the algorithms are developed and implemented (Ferrara, 2024). They highlight the importance of identifying and mitigating biases in datasets and algorithms to ensure fair and accurate results. Ethics in NLP writing and review are essential to ensure that the technology is used responsibly. Transparency in technology development is essential for minimizing the risk of misuse and increasing accountability, especially in the military context (Benotti *et al.*, 2023).

Privacy and data control are two issues frequently discussed in the linguistics literature. Open machine translation tools can help increase transparency and accountability in language data management. However, such tools still require strict regulations to prevent misuse. In the military context, protecting individual privacy is even more important because misusing data for such purposes is unethical. This highlights 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 easier and more accessible models to ensure that technology is used ethically and responsibly.

Accuracy and internal bias in decision-making are critical to the ethics of the linguistic use of technology in defense. Hovy and Spruit (2016) noted that bias in the linguistic experience of technology can have broad societal impacts, including in the military context, where biased decisions can be made, leading to unfair or discriminatory actions. Therefore, bias mitigation is critical in the development and implementation of such technologies. McCrae and Cillessen (2021) found that the use of interoperable lexical data can help mitigate internal bias. This demonstrates the importance of accurate data that is free from internal bias when ensuring fair and informed decisions.

The philosophical implications of using computational linguistics in advocacy are also important to consider. This technology raises questions about the relationship between the state and its citizens and between decision-makers and data subjects. Ethical theories, both deontological and utilitarian, can be applied to evaluate the moral impact of using language technology in advocacy contexts. According to ethical theory, action is ethical if it is carried out based on a predetermined moral obligation with no regard for its consequences. In this context, the use of such technology violates the privacy of language or reinforces social biases. This cannot be ethically justified, even if it may result in strategic military benefits. In contrast, utilitarianism and the ethics of judgment are based on the outcomes or consequences of actions. Applying computational linguistic technology means using technology that optimizes safety and security while minimizing negative impacts on individuals and society, which can be considered ethical.

Transparency and accountability are important aspects of the use of linguistic technologies, including language gestures. Technology developers should develop understandable and auditable models to ensure that technology is used ethically and responsibly. Transparency in algorithm operation and accountability in decision-making can help reduce the risk of misuse and increase public trust in technology. Benotti et al. (2023) emphasized the importance of transparency in technology development to minimize the risk of misuse and increase accountability. In the military context, transparency is especially important because decisions made based on analysis of language data can have far-reaching consequences.

To address ethical challenges, a solid regulatory framework is needed to ensure fair and responsible use of technology and language in the context of national defense. Regulations should include privacy protections, strict data controls, bias mitigation, and transparency and accountability for law enforcement. In addition, it is important to foster ongoing dialogs between technology developers, policymakers, and the public to ensure that application technologies adhere to important security principles. Benotti et al. (2023) suggested that active participation from multiple stakeholders can help to create a more comprehensive and responsive framework for developing technology.

3. Methodology

This study aims to identify and analyze the main ethical issues arising from the use of computational linguistics. in defense applications and its philosophical implications for security and human rights. The methodology used in this study involves a qualitative approach with three main steps: literature review, concept analysis, and case study. Each step in the data collection and analysis process was designed to ensure that the results of this study could be replicated with high accuracy while still taking into account strict research ethics principles, including data protection and confidentiality of the analyzed information.

The first step in this research is a comprehensive literature review. Overview: this section covers relevant ethical technology, computational linguistics, and defense application literature. The sources 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 Reference Review focuses on identifying recognized ethical challenges in the use of technological language in a military context and the solutions proposed by previous researchers. At this stage, it Is important to understand the social impact of natural language processing (NLP) and how technological bias can influence outcomes and decisions. They highlight the need for transparency and accountability when developing NLP algorithms. Additionally, Benotti et al. (2023) emphasized 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, in which ethical theories, deontological and utilitarian, are applied. Computational linguistic technology can be used to evaluate or assess the moral consequences it causes [16]. The deontological ethical theory proposed by Immanuel Kant emphasizes the importance of acting appropriately with moral obligations without considering consequences. In this context, violating an individual's technological privacy or reinforcing social biases is considered unethical even though it may provide a strategic advantage to 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 the use of technological language in the defense context and provides a basis for a more ethical evaluation.

Example: The most prominent case in 2013 was when Edward Snowden, a former contractor for the United States National Security Agency (NSA), revealed a secret surveillance program known as PRISM. This program allowed the NSA to access data from major technology companies, such as Google, Facebook, and Microsoft, including emails, text messages, and other digital communications. Computational linguistics technology was used in this study to analyze large amounts of data and detect potential threats to national security, such as terrorist plots and other illegal activities. However, this disclosure raised a major controversy over privacy, as many citizens and international figures felt that the surveillance violated human rights and was carried out without their consent or knowledge. The case highlights an ethical dilemma between maintaining national security and protecting individual rights. It has sparked a global debate about the limits of government surveillance in the digital age (Kilroy, 2016).

The third step is to study cases to illustrate the application of computational linguistics technology in the defense context and to challenge the ethical implications. A case study is selected based on its relevance and the availability of sufficient data for analysis. This includes data analysis from operations involving the military that use technology—language for intelligence, surveillance, and strategic communication (Doshi-Velez and Kim, 2017).

Each case study was analyzed to identify specific ethical challenges, such as privacy, data control, accuracy, bias, transparency, and accountability. For example, machine translation tools demonstrate the importance of regulating the misuse of language data during military operations (Klein *et al.*, 2017). The analysis also evaluates how technology affects the relationship between states and citizens and between decision makers and data subjects.

The internal data collection process involved literature from various sources. Academic databases were used to access journals, books, and study reports[21]. In addition, 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. After collection, the data were qualitatively analyzed to identify key thematic patterns relevant to the study questions. This analysis included content analysis and thematic analysis techniques to effectively evaluate the data and provide comprehensive, in-depth, and productive insights into the issues and ethics discussed.

Data triangulation is essential for ensuring the validity and reliability of findings. Data triangulation involves the use of multiple data sources and analysis methods to ensure consistency and accuracy (Tang and Surdeanu, 2023). Academic literature data are compared with non-academic sources to validate results and identify potential inconsistencies.

4. Research Results and Discussion

This study identified and analyzed the main ethical issues arising from the use of computational linguistics in application advocacy. The following research results are discussed in depth based on the main findings:

4.1 Privacy

One of the major ethical issues identified in this study is the right to privacy. Computational linguistics technologies used in national defense often involve the collection and analysis of language data from various sources, including personal communication and intelligence data. The experience of language processing can significantly impact individuals because of the technology's ability to access and analyze personal data without the individual's explicit consent (Hovy and Spruit, 2016). The unauthorized use of data can raise serious concerns about how the data are collected, stored, and used, and who has access to it.

In addition, it emphasizes the importance of transparency in data collection and analysis to protect individual rights. Transparency in the use of technology is essential for building trust between users and service providers. Without adequate transparency, users may feel that their data are being misused or used as they wish.

In the military, privacy breaches can occur when data are used for unethical purposes or without adequate oversight. Where strict regulations are in place, the use of technological, linguistic, and computational surveillance can violate citizens' privacy. Excessive surveillance can result in unnecessary data collection and harmful misuse of information. Therefore, it is important to implement policies and regulations that protect individuals and ensure that data are used transparently and ethically.

For example, the use of computational linguistics technology in intelligence analysis requires data collection from various sources, including private and public communication data. With proper oversight, these data can be used for unethical purposes and with the consent of the individual. The use of machine translation tools can increase transparency and accountability in the management of language data and even broaden semantic understanding (Kraska-Szlenk, Iwona; Wójtowicz, 2023); however, these tools still require strict regulations to avoid misuse.

Therefore, it is important to implement policies and regulations that protect individual privacy and ensure that data use is conducted transparently and ethically. Benotti et al. (2023) also showed that data collection and analysis transparency can help reduce the risk of misuse and increase public trust in technology. Transparency can be achieved through transparent reporting on how data are collected, stored, and used and who has access to the data. In this way, users can feel safer and more confident that their data will not be hacked.

Technological linguistics in a military context also poses challenges related to data monitoring and control. Understanding the importance of applications and vulnerabilities is crucial for policymakers, military professionals, and technology enthusiasts (Dogra, 2025).Data collected for objective defense is often sensitive, sophisticated and contain valuable information. Therefore, it is important to ensure that these data are managed carefully and used only for legitimate purposes. Strict regulations are required to ensure that data are not misused and that individual privacy is protected(Saeidnia *et al.*, 2024).

In addition, it is important to consider the ethical implications of data collection and use in a military context. Data for surveillance or objective intelligence must be used with individual privacy in mind and ensure that they are used responsibly. For example, collecting data from private communications without consent is considered a serious violation of privacy and should be avoided. Benotti et al. (2023) emphasized that technology developers must ensure that data collection and analysis are transparent and ethical.

Privacy breaches can also occur when data are used for unauthorized purposes or without adequate oversight. For example, the use of computational linguistics technology to monitor communications may result in data misuse and breach of personal privacy. Therefore, it is important to ensure that data are used transparently and ethically and that strict regulations are in place to protect individual privacy.

Overall, privacy is an ethical issue when using linguistic technology in the military context. Protective policies and regulations must be implemented to protect individual privacy and ensure transparent and ethical data use. Technology can improve safety and effectiveness during military operations without compromising individual privacy.

4.2 Data Control

Control of the data collected and analyzed using linguistic technologies is also an ethically significant issue. Open machine translation tools can help increase transparency and accountability in the management of language data; however, strict regulations are required to prevent misuse. In defense of the application, strict data controls are needed to ensure that the data collected is only used for legitimate purposes and is not misused for the benefit of others(Malgieri and Pasquale, 2024).

The use of technology in the military often involves collecting data from multiple sources, including personal and public data. The emotional state of the public must also be understood more deeply. This poses the challenge of ensuring that data are managed ethically and responsibly. Strict regulation and strict oversight are necessary to ensure that data are not misused and that individuals have control over their personal data.

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

For example, in a military context, data collected for intelligence analysis must be managed very carefully to prevent misuse of the available information and compromise individual privacy. Strict oversight is required to ensure that the data are only used for legitimate purposes and to protect authorized individuals. According to Hovy and Spruit (2016), the language experience of technology can significantly affect individuals. Therefore, strict data controls are required to prevent misuse.

In addition, regulations are needed to ensure that the collected data are used responsibly. Klein et al. (2017) emphasize that strict regulation is necessary to prevent data misuse and ensure that data are managed transparently and accountable. This rule should have robust supervision measures to prevent data misuse and empower individuals with control over their own data.

Strict regulation policies must also be implemented to protect individual privacy and ensure that data are only used for legitimate purposes. Transparency in data collection and analysis is essential to ensure that individual rights are protected and that data are used ethically(Benotti *et al.*, 2023). Stringent regulation is necessary to prevent data misuse and empower individuals with control over their data.

To address these challenges, a multifaceted approach is needed to develop 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 the risk of misuse and increase public trust in technology.

Data control is an ethically significant issue in the use of computational linguistics technology in the context of National Defense. Strict policies and regulations must be implemented to protect individual privacy and ensure that data are used transparently and ethically. Strict oversight and regulation are required to ensure that data are 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 algorithmic bias another ethical issue was found in this study when making decisions. Hovy and Spruit (2016) noted that bias in technological linguistic experiences can have far-reaching implications, including in military contexts where biased decisions can be made, leading to unfair or discriminatory actions(Hovy and Spruit, 2016). Technological Linguistics is often developed based on the possibility that data sets contain inherent biases that can be amplified by algorithms. Therefore, bias mitigation is an important step in developing and implementing computational linguistics to ensure fair and accurate decision-making based on data analysis.

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 language-related decisions. Interoperable lexical data can be a more holistic and accurate analysis tool, which, in turn, helps identify and reduce internal bias in decision making. This demonstrates the importance of accurate data that are free from internal bias to ensure fair and informed decisions(McCrae and Cillessen, 2021).

Implementing audited and more transparent algorithms is also an important step toward reducing algorithmic bias and improving decision-making accuracy. Transparency in algorithms means that third parties can examine and verify the decision-making process, which helps identify and correct potential bias(Alamillo *et al.*, 2023). According to Benotti et al. (2023), transparency in developing and implementing NLP technology is essential to ensure that the technology is used responsibly and minimizes the risk of internal bias when making decisions.

Additionally, there is a holistic and multifaceted approach to building technology. Computational Linguistics can help identify and mitigate bias. Highlighting the importance of this approach, including engineering bias mitigation and explanatory AI, to ensure fair and accurate data-driven decision-making.

In the 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 are accurate and free from bias and that the algorithms used to make decisions are transparent and auditable. Hovy and Spruit (2016) emphasized that bias in the language experience of technology can have far-reaching impacts, including in the military context, where biased decisions can be made, leading to unfair or discriminatory actions(Hovy and Spruit, 2016).

In addition to reducing bias, improving decision accuracy is also important when using linguistic technology. Applying more transparent and capable audit algorithms can help improve decision-making accuracy with the possibility of verification and validation by third parties. Transparency between the algorithms and data allows for more accurate and reliable decision-making. 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, thus improving decision-making accuracy (McCrae and Cillessen, 2021).

Thus, accuracy and bias in decision-making are ethically significant issues when using linguistic technology in the military context. Reducing bias and increasing accuracy are essential steps to ensure fair and accurate decisions based on data analysis. Transparency in the algorithms and data used and a holistic approach to developing the technology will help reduce bias and increase the accuracy of decision-making. Ensure that the data used are accurate and free from 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

Using computational linguistics in the defense of applications has implications for deep philosophical relationships between the state and citizens and between decision-makers and data subjects. According to ethical theory, action is considered ethical if it is carried out in accordance with a predetermined moral obligation without regard to its consequences. Using technology that violates an individual's linguistic privacy or reinforces social biases is considered unethical, even though it may produce strategic benefits for the military(Benotti *et al.*, 2023).

In contrast, Utilitarian ethics in ethics of judgment is based on the results or consequences of actions. When applying computational linguistic technology, using a technology that optimizes national defense and security while minimizing negative impacts on individuals and society can be considered ethical. This analysis helps in understanding the implications of the use of language technology in defense contexts and provides a basis for deeper ethical evaluation.

The philosophical implications involve issues of power and control. 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 national defense and security. In this case, implementing a technological language that does not respect individual privacy and freedom is considered unethical (Klein *et al.*, 2017).

On the other hand, from a utilitarian perspective, action can be considered ethical if its consequences outweigh the safety and security of society as a whole. However, careful evaluation is required to determine how the collective benefits offset the negative impacts on individuals. Utilitarian theory demands that the overall benefits outweigh individual harms for action to be considered ethical (McCrae and Cillessen, 2021).

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

Other philosophical implications include the consideration of the balance between security and liberty. In the 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 should take priority, while utilitarian theories emphasize the importance of outcomes that benefit safety and security.

Computational Linguistics Technology in the Context of Defense and national security requires clear policies and strict regulations to ensure that ethical principles are respected. Such policies should include privacy protections, data use oversight, and mechanisms to reduce bias and increase accuracy when making decisions (Hovy and Spruit, 2016).

Thus, the philosophical implications of computational linguistics technology in its application in defense are complex and require a careful and responsible approach. Ethical theories, both deontological and utilitarian, offer a useful framework for evaluating the moral impact and consequences of technology use. Only by considering the ethical and philosophical aspects of computational linguistics 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. because it ensures that AI systems operate according to ethical and legal standards and are accountable to the public.(Novelli, Taddeo and Floridi, 2024) emphasize that technology developers should develop more understandable and auditable models to ensure that technology is used ethically and responsibly. Transparency in algorithm operation and accountability for decision-making can help reduce the risk of misuse and increase public trust in technology.

Benotti et al. (2023) emphasized the importance of transparency in the technology development process to minimize the risk of misuse and increase accountability. In the military context, transparency is important because decisions based on language data analysis can have far-reaching consequences. The absence of transparent decisions can lead to mistrust and potential abuse of power, which can negatively impact the relationship between the military and society.

Transparency in algorithm operation means that third parties can audit and verify the decision-making process.(Balasubramaniam *et al.*, 2023). This allows independent oversight to ensure fair and ethical use of algorithms. Accountability in decision-making ensures that those responsible answer questions about the use of technology (Rajpurkar, Jia and Liang, 2018). This can be identified and questioned if misuse occurs.

Research has revealed that the use of linguistic technology in defense and national security poses several complex ethical challenges. These challenges include data control, accuracy, bias, transparency, and accountability. The theoretical approaches to ethics, deontology, and utilitarianism offer practical frameworks for evaluating technology use's moral impact and consequences. The deontological ethical theory emphasizes the importance of acting based on moral obligation without considering the consequences, and utilitarian ethical theory judges ethics based on the outcomes or consequences of actions (Hovy and Spruit, 2016).

Fair and responsible use of language technology requires a robust regulatory framework and ongoing dialog between technology developers, policymakers, and the public. Strong regulation will ensure that individual privacy is protected, strict data controls will be implemented, and mitigation can be implemented effectively. In addition, transparency and accountability in decision making will increase public trust in technology and ensure that such technology is used ethically and responsibly.

In the military context, it is important to implement clear policies and strict regulations to ensure that ethical principles are respected. These policies should include privacy protections, data use oversight, and mechanisms to reduce bias and increase decision-making accuracy. With the answer to this comprehensive and responsible approach, technological linguistics can be used to enhance national defense and effectiveness in military operations without compromising individual privacy (McCrae and Cillessen, 2021).

5. Conclusion

This study examines ethics in computational linguistics for national defense use through philosophical language and security analysis. The results of this study indicate that the potential of computational linguistics technology not only increases the effectiveness of military operations but also raises many significant ethical challenges and needs that can be addressed comprehensively. These challenges include privacy, data control, accuracy, bias, transparency, and accountability, and they require specific and appropriate regulations.

Privacy is a key issue when using linguistic technology in national security and defense. Technologies that enable the collection and analysis of personal data on a large scale can violate individual privacy if not properly regulated. In addition, strict data controls are required to ensure that the collected data are only used for legitimate purposes and are not misused for the benefit of others. The use of technology often involves the collection of data from multiple sources, which poses challenges in ensuring that data are managed ethically and responsibly. Mitigating bias and increasing decision-making accuracy are also important to ensure that technology is used fairly and responsibly.

The implications are philosophical, and the use of technology should be considered. The use of computational linguistics in national defense raises questions about the relationship between the state and its citizens, decision-makers and data owners. Ethical theories, whether deontological or utilitarian, provide useful frameworks for evaluating technology's moral impact and consequences. Deontological ethical theories emphasize that violating an individual's privacy or reinforcing social biases is not ethically justifiable, even if it may yield strategic military advantages. In contrast, utilitarian ethics assumes that technology is optimized for the benefit of safety and security. National law is ethical as long as its negative impacts on individuals and society are minimized.

Addressing ethical challenges requires a solid regulatory framework that ensures fair and responsible use of technology and language in the context of national defense. Regulations should include privacy protections, strict data controls, bias mitigation, and transparency and accountability for law enforcement. In addition, it is essential to foster ongoing dialog between technology developers, policymakers, and the public to ensure that application technologies comply with fundamental human rights and security. Overall, research has shown that despite the computational nature of technological linguistics, its potential is significant in terms of enhancing capabilities in field operations and national defense. However, the application of such technology must be accompanied by deep ethical considerations and strict regulation to avoid impacts on individuals and society.

References

(1) Alamillo, A.R. *et al.* (2023) 'The Analysis of Synonymy and Antonymy in Discourse Relations: An Interpretable Modeling Approach', *Computational Linguistics*, 49(2), pp. 429–464. Available at: https://doi.org/10.1162/coli_a_00477.

(2) Balasubramaniam, N. *et al.* (2023) 'Transparency and explainability of AI systems: From ethical guidelines to requirements', *Information and Software Technology*, 159, p. 107197. Available at: https://doi.org/https://doi.org/10.1016/j.infsof.2023.107197.

(3) Benotti, L. *et al.* (2023) 'Understanding Ethics in NLP Authoring and Reviewing', *EACL 2023 - 17th Conference of the European Chapter of the Association for Computational Linguistics, Proceedings of Tutorial Abstracts*, pp. 19–24. Available at: https://doi.org/10.18653/v1/2023.eacl-tutorials.4.

(4) Collins, C. *et al.* (2021) 'Artificial intelligence in information systems research: A systematic literature review and research agenda', *International Journal of Information Management*, 60, p. 102383. Available at: https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2021.102383.

(5) Darinka Verdonik (2020) 'Annotating dialogue acts in speech data Problematic issues and basic dialogue act categories', *International Journal of Corpus Linguistics*, 28(2). Available at: https://doi.org/https://doi.org/10.1075/ijcl.20165.ver.

(6) Devlin, J. *et al.* (2019) 'BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding', *Proceedings ofNAACL-HLT 2019*, (Mlm), pp. 4171–4186. Available at: https://aclanthology.org/N19-1423.pdf.

(7) Dogra, A. (2025) 'Metaverse in Military Defense Applications BT - Understanding the Metaverse: Applications, Challenges, and the Future', in G. Chhabra and K. Kaushik (eds). Singapore: Springer Nature Singapore, pp. 187–213. Available at: https://doi.org/10.1007/978-981-97-2278-5_9.

(8) Doshi-Velez, F. and Kim, B. (2017) *Towards A Rigorous Science of Interpretable Machine Learning*.

Available at: http://arxiv.org/abs/1702.08608.

(9) Elder, R.J. (2020) ‘Cyberwarfare as Realized Conflict BT - The Palgrave Handbook of International Cybercrime and Cyberdeviance’, in T.J. Holt and A.M. Bossler (eds). Cham: Springer International Publishing, pp. 1437–1469. Available at: https://doi.org/10.1007/978-3-319-78440-3_64.

(10) Ferrara, E. (2024) ‘Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies’, *Sci*, 6(1). Available at: https://doi.org/10.3390/sci6010003.

(11) Hovy, D. and Prabhumoye, S. (2021) ‘Five sources of bias in natural language processing’, *Language and Linguistics Compass*, 15(8), pp. 1–19. Available at: https://doi.org/10.1111/lnc3.12432.

(12) Hovy, D. and Spruit, S.L. (2016) ‘The social impact of natural language processing’, *54th Annual Meeting of the Association for Computational Linguistics, ACL 2016 - Short Papers*, pp. 591–598. Available at: https://doi.org/10.18653/v1/p16-2096.

(13) Kilroy, R. (2016) ‘No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. By Glenn Greenwald, New York, NY: Metropolitan Books, 2014.’, *Journal of Strategic Security*, 9(3), pp. 99–102. Available at: https://doi.org/10.5038/1944-0472.9.3.1552.

(14) Klein, G. *et al.* (2017) ‘OpenNMT: Open-source toolkit for neural machine translation’, *20th Annual Conference of the European Association for Machine Translation, EAMT 2017*, p. 22.

(15) Kraska-Szlenk, Iwona; 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). Available at: https://doi.org/https://doi.org/10.1075/ijcl.20074.kra.

(16) Lepri, B., Oliver, N. and Pentland, A. (2021) ‘Ethical machines: The human-centric use of artificial intelligence’, *iScience*, 24(3), p. 102249. Available at: https://doi.org/https://doi.org/10.1016/j.isci.2021.102249.

(17) Liu, Q. *et al.* (2020) ‘You impress me: Dialogue generation via mutual persona perception’, *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics*, pp. 1417–1427. Available at: https://doi.org/10.18653/v1/2020.acl-main.131.

(18) Liu, Y. *et al.* (2019) ‘RoBERTa: A Robustly Optimized BERT Pretraining Approach’, *Computation and Language* [Preprint]. Available at: https://doi.org/https://doi.org/10.48550/arXiv.1907.11692.

(19) Malgieri, G. and Pasquale, F. (2024) ‘Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology’, *Computer Law & Security Review*, 52, p. 105899. Available at: https://doi.org/https://doi.org/10.1016/j.clsr.2023.105899.

(20) McCrae, J.P. and Cillessen, D. (2021) ‘Towards a linking between WordNet and Wikidata’, *GWC 2021 - Proceedings of the 11th Global Wordnet Conference*, pp. 252–257.

(21) McThomas, M. (2016) ‘Theories of Ethics BT - Global Encyclopedia of Public Administration, Public Policy, and Governance’, in A. Farazmand (ed.). Cham: Springer International Publishing, pp. 1–5. Available at: https://doi.org/10.1007/978-3-319-31816-5_931-1.

(22) Novelli, C., Taddeo, M. and Floridi, L. (2024) ‘Accountability in artificial intelligence: what it is and how it works’, *AI & SOCIETY*, 39(4), pp. 1871–1882. Available at: https://doi.org/10.1007/s00146-023-01635-y.

(23) Omrani, N. *et al.* (2022) ‘To trust or not to trust? An assessment of trust in AI-based systems: Concerns, ethics and contexts’, *Technological Forecasting and Social Change*, 181, p. 121763. Available at: https://doi.org/https://doi.org/10.1016/j.techfore.2022.121763.

(24) Rafiq, F. *et al.* (2022) ‘Privacy Prevention of Big Data Applications: A Systematic Literature Review’, *Sage Open*, 12(2), p. 21582440221096444. Available at: https://doi.org/10.1177/21582440221096445.

(25) Rajpurkar, P., Jia, R. and Liang, P. (2018) ‘Know what you don’t know: Unanswerable questions for SQuAD’, *ACL 2018 - 56th Annual Meeting of the Association for Computational Linguistics, Proceedings of the Conference (Long Papers)*, 2, pp. 784–789. Available at: https://doi.org/10.18653/v1/p18-2124.

(26) Rashid, A. Bin *et al.* (2023) ‘Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges’, *International Journal of Intelligent Systems*, 2023. Available at: https://doi.org/10.1155/2023/8676366.

(27) Saeidnia, H.R. *et al.* (2024) ‘Ethical Considerations in Artificial Intelligence Interventions for Mental Health and Well-Being: Ensuring Responsible Implementation and Impact’, *Social Sciences*, 13(7). Available at: https://doi.org/10.3390/socsci13070381.

(28) Taddeo, M. *et al.* (2021) ‘Ethical Principles for Artificial Intelligence in National Defence’, *Philosophy*

and Technology, 34(4), pp. 1707–1729. Available at: https://doi.org/10.1007/s13347-021-00482-3.

(29) Tang, Z. and Surdeanu, M. (2023) 'It Takes Two Flints to Make a Fire: Multitask Learning of Neural Relation and Explanation Classifiers', *Computational Linguistics*, 49(1), pp. 117–156. Available at: https://doi.org/10.1162/coli_a_00463.

(30) Tyagi, N. and Bhushan, B. (2023) 'Demystifying the Role of Natural Language Processing (NLP) in Smart City Applications: Background, Motivation, Recent Advances, and Future Research Directions', *Wireless Personal Communications*, 130(2), pp. 857–908. Available at: https://doi.org/10.1007/s11277-023-10312-8.

(31) Vaccino-Salvadore, S. (2023) 'Exploring the Ethical Dimensions of Using ChatGPT in Language Learning and Beyond', *Languages*, 8(3), pp. 4–9. Available at: https://doi.org/10.3390/languages8030191.

(32) Vitale, G. (2023) 'Research Methodology BT - Understanding Supply Chain Digitalization Through Actor-Network Theory: The Interplay Between Blockchain, Accounting and Management Control', in G. Vitale (ed.). Cham: Springer Nature Switzerland, pp. 47–69. Available at: https://doi.org/10.1007/978-3-031-30988-5_3.

(33) Wulf, A.J. and Seizov, O. (2024) '"Please understand we cannot provide further information": evaluating content and transparency of GDPR-mandated AI disclosures', *AI and Society*, 39(1), pp. 235–256. Available at: https://doi.org/10.1007/s00146-022-01424-z.

(34) Yang, Z. *et al.* (2019) 'XLNet: Generalized autoregressive pretraining for language understanding', *Advances in Neural Information Processing Systems*, 32(NeurIPS), pp. 1–11.