Security and Ethics in the Use of Computing Technologies and the Internet

Laercio Cruvinel Júnior[1,2][0000-0002-7672-3243], António Cabeças[1][0000-0001-8496-535X], Adriana Lopes Fernandes[3][0000-0001-7025-9470],

[1] Universidade Autónoma de Lisboa Luís de Camões, 1169-023 Lisboa, Portugal

[2] Autónoma TechLab, 1169-023 Lisboa, Portugal

[3] Escola Superior Náutica Infante Dom Henrique, 2770-058 Paço de Arcos

lcruvinel@autonoma.pt✉, acabecas@autonoma.pt, adrianafernandes@enautica.pt

EXTENDED ABSTRACT

1. Introduction

The rapid advancement of computing technologies and the pervasive use of the Internet have transformed societies, businesses, and educational institutions. However, issues such as data privacy, algorithmic bias, cybersecurity threats, digital burnout, and ethical AI applications have become central to discussions in academia, industry, and policy-making (Stahl et al., 2023; Zostant & Chataut, 2023).

This paper offers a critical synthesis of contemporary ethical and security challenges in computing, arguing that digital well-being and user empowerment must be central to policy reform and technological design. It also identifies best practices for the responsible use of computing technologies, aiming to balance innovation with ethical accountability, data protection, and digital well-being.

2. Ethical Considerations in Computing Technologies

2.1. Privacy, Data Protection, and Digital Well-being

Privacy is one of the most pressing ethical issues in computing technologies (Zostant & Chataut, 2023). The collection, storage, and processing of personal data raise concerns about user autonomy and the right to control one's information. The challenge is to implement transparent policies that ensure user awareness and control over their digital footprint (van Baalen, 2018).

In addition to privacy concerns, digital burnout has emerged as a major ethical issue (Pinto, 2023). Although commonly discussed as separate issues, digital burnout and algorithmic surveillance often co-occur in educational and workplace settings, revealing a broader ethical concern with techno-governance over personal autonomy.

2.2. Algorithmic Bias and Fairness

AI and machine learning algorithms increasingly influence decision-making in critical sectors such as healthcare, finance, and education (Stahl et al., 2023). However, these systems are vulnerable to biases embedded in their training data, which can lead to discriminatory outcomes that disproportionately affect marginalized populations. Addressing these issues demands ethical scrutiny.

From a deontological perspective, systems must be designed to treat all individuals with equal respect, regardless of statistical utility. In contrast, a consequentialist approach might justify certain algorithmic trade-offs if the overall benefit outweighs individual harms, such as increased efficiency or predictive accuracy.

The reasoning above can be ethically fraught when it normalizes systemic inequities under the guise of optimization. Ethical AI development should be grounded in frameworks that emphasize

transparency, **accountability**, and **inclusivity**. Without such safeguards, the deployment of AI risks reinforcing existing social hierarchies rather than promoting equitable outcomes.

2.3. Autonomy, Digital Ethics, and Work-Life Balance

AI-driven recommendations and automated decisions can subtly, or overtly, diminish user influence and discernment—particularly when algorithms operate as "black boxes" with limited transparency or explainability (Knight, 2024). From a Kantian (deontological) perspective, such opacity is ethically problematic: individuals must be treated as ends in themselves, not as means to statistical or institutional efficiency. When users are subjected to decisions they cannot understand, challenge, or opt out of, their moral agency is compromised. In contrast, a utilitarian viewpoint might argue that automation improves outcomes overall, streamlining processes and reducing human error. However, this must be weighed against the psychological and social costs of reduced control and depersonalized interaction. To reconcile these tensions, ethical guidelines should prioritize explainability, informed consent, and design for user empowerment.

Moreover, prolonged engagement with digital systems contributes to digital burnout, a condition linked to stress, fatigue, and a deteriorating work-life balance (Pinto, 2023). Ethical technology design must therefore support human-centered practices, such as workload modulation, screen-time awareness, and proactive disengagement policies that respect the limits of cognitive and emotional labor.

2.4. Cybersecurity, Ethical Hacking, and Digital Exhaustion

Ethical hacking plays a critical role in safeguarding digital systems (Wang, 2023). However, the ethical implications of cybersecurity practices must be carefully examined, particularly as AI-driven surveillance tools become more pervasive.

From a consequentialist view, continuous monitoring may be justified if it prevents harm. Yet, a deontological perspective emphasizes the intrinsic value of individual privacy and autonomy, and AI-powered systems that monitor user behavior to detect threats may unintentionally erode trust and contribute to digital exhaustion (Jawad, 2024).

Ethical cybersecurity should prioritize transparency, proportionality, and user well-being. Systems must be designed to minimize invasiveness while maintaining effectiveness, and users should be made aware of how their data is monitored and protected.

3. Security Threats in Computing Technologies and the Internet

Cybercrime exploits vulnerabilities in digital infrastructures, often targeting individuals, institutions, and critical systems (Shillair et al., 2015). In response, organizations have embraced advanced cybersecurity strategies such as end-to-end encryption, multi-factor authentication, and continuous network monitoring. These measures also introduce complex ethical trade-offs related to privacy, autonomy, and psychological well-being.

Machine learning algorithms can detect anomalies, predict vulnerabilities, and automate threat response mechanisms at a scale unmanageable by human analysts (Wang, 2023). Yet, the use of AI introduces its own risks—most notably, adversarial AI attacks and limited transparency, raising concerns about accountability and user agency.

From a consequentialist perspective, the use of AI in cybersecurity can be justified by the greater good it achieves: preventing data breaches, protecting infrastructure, and maintaining public safety. But this rationale becomes ethically precarious when it fails to address the deontological obligation to respect user rights. For instance, pervasive surveillance technologies can infringe on privacy, chill free expression, and foster distrust among users (van Baalen, 2018). The normalization of such practices undermines the foundational democratic value of privacy as a prerequisite for free thought and expression. Legal frameworks alone are insufficient unless paired with institutional ethics that prioritize human dignity alongside data protection (Zostant & Chataut, 2023).

Ultimately, effective cybersecurity must be both technically robust and ethically grounded, also ensuring that the tools designed to protect do not become mechanisms of control.

4. Proposed Solutions and Best Practices

4.1. Ethical AI Development

AI developers should adopt ethical AI principles, including:

- Transparency: Clear documentation of AI decision-making processes.
- Accountability: Mechanisms to identify and rectify biases in AI models.
- Inclusivity: Diverse and representative datasets for training AI systems.
- Human-Centered Design: AI applications that prioritize human well-being and reduce digital exhaustion.

4.2. Strengthening Cybersecurity Measures

Organizations and individuals should implement robust cybersecurity practices, such as:

- Encryption and Secure Authentication: Protecting sensitive data with strong encryption methods.
- Regular Security Audits: Conducting periodic vulnerability assessments.
- User Awareness Programs: Educating users about phishing attacks, online threats, and the impact of digital exhaustion (Shillair et al., 2015).

4.3. Regulatory and Policy Frameworks

Essential measures by governments and regulatory bodies should include:

- Data Protection Laws: Ensuring compliance with global standards.
- AI Ethics Guidelines: Establishing clear ethical standards for AI deployment.
- Consumer Rights Protection: Enforcing transparency in data collection and user consent policies.

4.4. Digital Literacy and User Responsibility

Digital literacy programs should focus on:

- Privacy Awareness: Teaching users how to safeguard their personal data.
- Critical Thinking: Encouraging skepticism towards misinformation and online manipulation.

While the proposed solutions aim to foster ethical and secure digital practices, their implementation is not without challenges, to be discussed in the full version of this article.

5. Conclusion

By considering transparency, fairness, and accountability in AI development, strengthening cybersecurity measures, enforcing regulatory frameworks, and promoting digital well-being, we can create a digital environment that upholds ethical standards and protects user rights. The future of computing technologies depends on responsible innovation that aligns with societal values, ensuring a secure, ethical, and mentally sustainable digital landscape for all. By prioritizing ethical reflexivity in

design and regulation, institutions can not only enhance security but also restore public trust in digital systems—a crucial factor for democratic resilience in the information age.

KEYWORDS: Cybersecurity, Ethical AI, Data Privacy, Algorithmic Bias, Digital Ethics, Regulatory Frameworks

REFERENCES

Jawad, L. A. (2024). Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies. *Abhigyan*, *42*(1), 23–31. https://doi.org/10.1177/09702385241233073

Knight, T. D. (2024). Genealogical Ethics in the United States and the Popularization of Genealogical Research in the Digital Age. *Genealogy (2313-5778)*, *8*(3), 78. https://doi.org/10.3390/genealogy8030078

Pinto, M. I. F. (2023). Devem as instituições de ensino superior estar preocupadas com o digital burnout? Uma perspetiva sobre a satisfação no trabalho. Master thesis, http://hdl.handle.net/10400.5/30117

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *COMPUTERS IN HUMAN BEHAVIOR*, *48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Stahl B. C. Timmermans J. Mittelstadt B. D. (2016). The Ethics of Computing: A Survey of the Computing-Oriented Literature. *ACM Computing Surveys*, 48(4), 1–38. 10.1145/2871196

van Baalen, S. (2018). 'Google wants to know your location': The ethical challenges of fieldwork in the digital age. *Research Ethics*, *14*(4), 1–17. https://doi.org/10.1177/1747016117750312

Wang, R. (2023). AI Use in Enhancing Cybersecurity for Safeguarding Digital Information. *2023 International Conference on Applied Physics and Computing (ICAPC), Applied Physics and Computing (ICAPC), 2023 International Conference on, ICAPC*, 412–419. https://doi.org/10.1109/ICAPC61546.2023.00082

Zostant, M., & Chataut, R. (2023). Privacy in computer ethics: Navigating the digital age. *Computer Science and Information Technologies; Vol 4, No 2: July 2023; 183-190 ; 2722-3221 ; 2722-323X ; 10.11591/Csit.V4i2*. https://doi.org/10.11591/csit.v4i2.p183-190