Ethical Reflections

Vol. 7, Issue 3, No. 27, Fall 2026, pp. 139-165
Online ISSN: 2717-1159 / Print ISSN: 2676-4810
https://jer.znu.ac.ir

Security and Ethical Challenges in the Internet of Things Ecosystem

Seyedeh Mahshid Miri Balajorshari,[1] Amirreza Mahmoudi,[2] Babak Pourghahramani [3]

Article info

DOI: 10.30470/er.2026.2088584.1528

Review Article

Submission History
Received: 12/05/2026
Revised: 18/07/2026
Accepted: 25/07/2026
Published: 23/09/2026

Authors' Contribution
Mahshid Miri Balajorshari: Data collection, initial and final drafting of the manuscript, revision of the manuscript.
Amirreza Mahmoudi: Conceptualization of the study, final drafting of the manuscript, analysis and critical appraisal, revision of the manuscript, providing suggestions and comments for revision, final review and approval of the manuscript.
Babak Pourghahramani: Analysis and critical appraisal, revision of the manuscript, providing suggestions and comments for revision, final review and approval of the manuscript.

Conflict of Interests
The authors declare no conflict of interest.

Funding/Support
This research has not received any financial support from funding organizations.

Extraction
his article has been extracted from Ph.D thesis in Islamic Azad University of Lahijan, entitled "Criminal Policy of Iran Towards Crimes Related to the Internet of Things in the Light of International Instruments" Ph.D. Student: Seyedeh Mahshid Miri Balajorshari, Supervisor: AmirReza Mahmoudi and Advisor: Babak Pourghahramani.

AI Usage
No artificial intelligence tools were used in the preparation of this article.

Abstract

As one of the modern and advanced technologies, the Internet of Things (IoT) plays a vital role in improving quality of life and facilitating various processes across diverse sectors such as healthcare, transportation, and industry. Nevertheless, the widespread adoption of this technology is accompanied by significant security and ethical challenges and vulnerabilities that require particular attention. The present study aims to elucidate the ethical and security challenges within the IoT ecosystem and to propose effective measures for enhancing security conditions and ensuring compliance with ethical principles in this field. This research is theoretical in nature and employs a descriptive-analytical method. The findings indicate that the principal security issues in the Internet of Things include cyber-attacks, weaknesses in security protocols, and the misuse of users' sensitive data. Ethical concerns are likewise primarily centered on the unauthorized collection and use of personal data and the violation of privacy. The results of this study further demonstrate that the development of ethical artificial intelligence in such systems, regular updating of devices, user education and awareness-raising, transparency in artificial intelligence algorithms, prevention of algorithmic discrimination, long-term device support are among the most effective strategies for strengthening security and ethics in the Internet of Things.

Keywords: Ethics, Security, Ethical Challenges, Security Challenges, Internet of Things.

1. Ph.D. Student in Criminal Law and Criminology, Department of Law, La.C., Islamic Azad University, Lahijan, Iran., s.miribalajorshari@iau.ac.ir

2. **Corresponding author,** Assistant Professor of Law, La.C., Islamic Azad University, Lahijan, Iran, dr.mahmoudi@iau.ac.ir

3. Professor of Criminal Law and Criminology, Mar.C., Islamic Azad University, Maragheh, Iran, pourghahramani@iau.ac.ir

Introduction

The rapid development of digital technologies has fundamentally transformed modern life and social structures. Among emerging technologies, the Internet of Things (IoT) has become one of the most important innovations connecting the physical world to cyberspace through sensors, smart devices, and communication networks. IoT technologies enable continuous collection, processing, and exchange of data, thereby improving efficiency and service quality in various sectors such as healthcare, transportation, industry, agriculture, and smart cities. Despite these significant benefits, the rapid expansion of IoT systems has also created serious ethical, legal, and cybersecurity challenges. Continuous data collection, extensive connectivity, and reliance on intelligent systems expose users and organizations to threats such as cyberattacks, privacy violations, unauthorized surveillance, and misuse of personal information. Accordingly, IoT should be understood not merely as a technological advancement but also as a legal, ethical, and security-related phenomenon requiring responsible governance and effective regulation. This study aims to analyze the major ethical and security challenges within IoT ecosystems and propose practical solutions for establishing secure and ethically responsible IoT systems.

Main Body

The study first examines the conceptual foundations and major applications of IoT technologies. IoT is described as an interconnected ecosystem of smart devices, sensors, communication protocols, and cloud infrastructures capable of collecting and exchanging data with minimal human intervention. The article highlights the broad use of IoT in healthcare systems, smart transportation, industrial manufacturing, energy management, agriculture, and environmental monitoring, emphasizing its role in improving productivity and operational efficiency. The article then analyzes the main ethical challenges associated with IoT systems. One of the most significant concerns involves the collection and misuse of personal and sensitive data. IoT devices continuously gather information such as medical records, behavioral patterns, geolocation data, and financial information, often without users having sufficient awareness of how such data are processed or shared. Unauthorized disclosure of this information may lead to identity theft, financial exploitation, psychological harm, and social discrimination. The study also emphasizes ethical concerns related to children and adolescents as vulnerable users of IoT technologies, highlighting the importance of parental supervision and digital literacy. Another important issue discussed in the article is privacy protection and informed consent. Many IoT systems collect data automatically and continuously, creating environments of constant monitoring and surveillance. In addition, the research addresses the risks of commercial exploitation and algorithmic discrimination arising from the use of artificial intelligence and data-driven decision-making systems. Biased datasets

and unfair algorithms may reinforce social inequalities and discriminatory practices. Alongside ethical concerns, the article examines major cybersecurity threats affecting IoT ecosystems. These include network-based attacks, malware infections, weak encryption systems, impersonation attacks, and data manipulation. Because many IoT devices are designed with insufficient security protections, they are highly vulnerable to cyber intrusions and unauthorized access. The research also highlights the risks resulting from the lack of regular software updates and long-term technical support, which leave many devices exposed to emerging cyber threats. To address these challenges, the article proposes several practical and governance-oriented solutions. These include the development of ethical and transparent artificial intelligence systems, implementation of privacy-by-design principles, and adoption of strong encryption protocols, regular software updates, and long-term security support for IoT devices. The study also emphasizes the importance of public awareness, cybersecurity education, and cooperation among governments, industry actors, and academic institutions in developing comprehensive legal and ethical frameworks for IoT governance.

Conclusion

The Internet of Things has significantly improved connectivity, efficiency, and quality of life across numerous sectors; however, its rapid expansion has simultaneously created complex ethical and cybersecurity challenges. The findings of this study demonstrate that cyberattacks, privacy violations, unauthorized surveillance, misuse of personal data, and algorithmic discrimination represent major threats within IoT ecosystems. Addressing these challenges requires an integrated approach combining legal regulation, ethical principles, cybersecurity measures, technological accountability, and public education. The study concludes that responsible governance of IoT systems depends on achieving a balance between technological innovation and the protection of fundamental human rights, particularly privacy, security, transparency, and fairness. Without such balance, IoT technologies may undermine public trust and become sources of insecurity and social inequality rather than tools for human progress and welfare.

References

Aghdasi, F., & Mohaqeq Damad, M. S. (2021). Legal dimensions of privacy in the Internet of Things. *Interdisciplinary Legal Research Quarterly*, 2(2), 49–67. (In Persian)

Ahmed, A. A., Farhan, K., Jabbar, W. A., Al-Othmani, A., & Abdulrahman, A. G. (2024). IoT Forensics: Current Perspectives and Future Directions. Sensors, 24(10), 1-16.

Almasoud, A., Idowu, J. (2025). Algorithmic fairness in predictive policing. AI and Ethics. 5. 2323-2337.

Bakhtiari, I. (2022). An analysis of the application of the Internet of Things in air defense networks from the perspective of vulnerabilities and threats. *Military Sciences and Techniques Quarterly*, 18(61), 55–82. (In Persian)

Dhinakaran, D., Raja, S., Ramathilagam, A., Vennila, G. (2025). Ethical and legal challenges with IoT in home digital twins, MethodsX. 14.

Farahzadi, A. A., & Naser, M. (2021). The right to exchange private data and solutions to address its challenges within the operational mechanisms of Internet of Things devices. *Commercial Reviews Quarterly*, 18(108), 115–128. (In Persian)

Ghariby, J., Gharaei, H., Farajipour, M. R., & Halili, K. (2024). Presenting a strategic model for Internet of Things data security governance in smart cities. *National Security Quarterly*, 14(53), 143–176. (In Persian)

Ghasempour, A. (2025). Medical big data and its ethical challenges regarding violations of patients' privacy. *Ethics in Science and Technology Quarterly*, 20(2), 9–18. (In Persian)

Hamidi, H. (2015). Ethics and protection of children's online privacy with parental consent. *Ethics in Science and Technology Quarterly*, 10(3), 41–57. (In Persian)

Hosseinzadeh, M., & Rezaei, A. (2023). Cybersecurity in the field of the Internet of Things. *Arman Pardazesh Quarterly*, 4(1), 1–9. (In Persian)

International Telecommunication Union (ITU). (2012). Recommendation ITU-T Y.2060: Overview of the Internet of Things. Geneva: ITU.

Kiankhah, E., & Karimi Ghahroudi, M. R. (2015). The challenging impact of the Internet of Things on the pillars of national security. *National Security Quarterly*, 5(16), 81–106. (In Persian)

Looschelders, D., Schulze, R., & Staudenmayer, D. (2023). *Liability of artificial intelligence and the Internet of Things* (F. Najibzadeh, Trans.). Tehran: Jangal Publications. (In Persian)

Luthfi, A., Minhar, E., (2022). Towards Privacy by Design on the Internet of Things (IoT) Use: A Qualitative Descriptive Study. Journal of Information Systems and Informatics. 4(2). 457-468.

Lyon, D. (2018). The Culture of Surveillance. Cambridge: Polity.

Moeinifar, M., & Vahidizadeh, D. (2022). Requirements for the realization of the right to privacy in the Internet of Things from the perspective of Iranian law. *Journal of New Technologies Law*, 3(6), 61–75. (In Persian)

Najafpour, V., Ghanbari, A., Nazari, D., & Moradi, A. (2018). Examining the role of the Internet of Things in the development of modern technologies at the societal level and its challenges. *Journal of Research in Engineering Science and Technology*, 4(2), 49–64. (In Persian)

Organization for Economic Co-operation and Development (OECD). (2023). Measuring the Internet of Things. OECD Publishing, Paris.

Sadeghi, H., & Naser, M. (2020). Presenting a legal framework for accountability in the operation of Internet of Things tools within e-government: Explaining an effective policymaking model. *Public Policy Quarterly*, 6(3), 81–103. (In Persian)

Sasi, T., Lashkari, A., Lu, R., Xiong. P., Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. Journal of Information and Intelligence. 2. 455-513.

Semantha, F., Azam, S., Yeo, Kh. Shanmugam, B. (2020). A Systematic Literature Review on Privacy by Design in the Healthcare Sector. Electronics. 9(3). 452.

Soni, N. (2024). IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. Computer and Telecommunication Engineering, 2(4).

Thakral, M., Singh, R. R., & Kalghatgi, B. V. (2022). Cybersecurity and ethics for IoT system: A massive analysis. In Internet of Things: Security and Privacy in Cyberspace. Springer Nature Singapore. 209-233.

Tzafestas, S. (2018). Ethics and Law in the Internet of Things World. Smart cities journal, 1(1), 98-120.

Weber, V. (2017). The Synergetic Smart City Framework – From Idea to Reality, Real Estate Issues.

تأملات اخلاقی

دورهٔ هفتم، شمارهٔ سوم (پیاپی ۲۷)، پاییز ۱۴۰۵، صفحات ۱۳۹-۱۶۵

شاپا الکترونیکی: ۱۱۵۹-۲۷۱۷/ شاپا چاپی: ۴۸۱۰-۲۶۷۶

https://jer.znu.ac.ir

چالش‌های امنیتی و اخلاقی در اکوسیستم اینترنت اشیاء

سیده مهشید میری بالاجورشری،[۱] امیررضا محمودی،[۲] بابک پورقهرمانی[۳]

اطلاعات مقاله

DOI:10.30470/er.2026.2088584.1528

مقاله مروری

تاریخ دریافت: ۱۴۰۵/۰۲/۲۲

تاریخ اصلاح: ۱۴۰۵/۰۴/۲۷

تاریخ پذیرش: ۱۴۰۵/۰۵/۰۳

تاریخ انتشار: ۱۴۰۵/۰۷/۰۱

نقش نویسندگان

مهشید میری: جمع آوری داده، نگارش اولیه و نهایی مقاله، انجام اصلاحات.

امیررضا محمودی: ایده‌پرداز اصلی مقاله، نگارش نهایی مقاله، تحلیل و نقادی، انجام اصلاحات، ذکر پیشنهادات و نکات اصلاحی، خوانش و تأیید نهایی مقاله.

بابک پورقهرمانی: تحلیل و نقادی، انجام اصلاحات، ذکر پیشنهادات و نکات اصلاحی، خوانش و تأیید نهایی مقاله.

حمایت مالی و تعارض منافع

مقاله حامی مالی و تعارض منافع ندارد.

استخراج

این مقاله مستخرج از رساله دکتری در دانشگاه آزاد اسلامی واحد لاهیجان با عنوان «سیاست جنایی ایران در قبال جرایم مرتبط با اینترنت اشیاء در پرتو اسناد بین‌المللی» دانشجو: سیده مهشید میری بالاجورشری، استاد راهنما: امیررضا محمودی و استاد مشاور: بابک پورقهرمانی است.

استفاده از هوش مصنوعی

در نگارش این مقاله از هوش مصنوعی استفاده نشده است.

چکیده

اینترنت اشیاء به‌عنوان یکی از فناوری‌های نوین و پیشرفته، نقش حیاتی در بهبود کیفیت زندگی و تسهیل فرآیندهای مختلف در حوزه‌های متنوعی چون مراقبت‌های بهداشتی، حمل‌ونقل و صنعت ایفا می‌کند. با این حال، استفاده گسترده از این فناوری با چالش‌ها و آسیب‌پذیری‌های امنیتی و اخلاقی قابل توجهی همراه است که نیازمند توجه ویژه و راهکارهای اجرایی است. هدف این پژوهش تبیین چالش‌های اخلاقی و امنیتی در اکوسیستم اینترنت اشیاء و ارائه راهکارهای مؤثر برای بهبود وضعیت امنیتی و رعایت اصول اخلاقی در این حوزه است. نوع تحقیق در پژوهش حاضر نظری و روش تحقیق توصیفی-تحلیلی است. یافته‌های پژوهش نشان می‌دهد که مشکلات اصلی امنیتی در اینترنت اشیاء شامل حملات سایبری، ضعف در پروتکل‌های امنیتی و سوءاستفاده از داده‌های حساس کاربران است. مسائل اخلاقی نیز عمدتاً حول محور جمع‌آوری و استفاده غیرمجاز از داده‌های شخصی و نقض حریم خصوصی است. نتایج این پژوهش حاکی از آن است که توسعه هوش مصنوعی اخلاقی در این سامانه‌ها، به‌روزرسانی منظم دستگاه‌ها، آموزش و آگاهی‌بخشی به کاربران، شفافیت در الگوریتم‌های هوش مصنوعی، پیشگیری از تبعیض‌های الگوریتمی و پشتیبانی طولانی‌مدت دستگاه‌ها از جمله راهکارهای موثر برای تقویت امنیت و اخلاق در اینترنت اشیاء است.

واژه‌های کلیدی: اینترنت اشیاء، اخلاق، امنیت، چالش‌های اخلاقی، چالش‌های امنیتی.

۱. دانشجو دکتری حقوق کیفری و جرم‌شناسی، گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. s.miribalajorshari@iau.ac.ir

۲ . **نویسنده مسئول:** استادیار گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. dr.mahmoudi@iau.ac.ir

۳. استاد گروه حقوق کیفری و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران. pourghahramani@iau.ac.ir

مقدمه

تحول دیجیتال در دهه‌های اخیر، با گسترش فناوری‌های نوظهور، شیوه زیست فردی و اجتماعی بشر را به‌صورت بنیادین دگرگون ساخته است. در این میان، اینترنت اشیاء به‌عنوان یکی از مهم‌ترین جلوه‌های همگرایی میان جهان فیزیکی و فضای سایبری، زمینه‌ساز شکل‌گیری محیطی هوشمند، داده‌محور و به‌شدت متصل شده است؛ محیطی که در آن اشیاء، دستگاه‌ها و سامانه‌های مختلف با اتکا به حسگرها، نرم‌افزارها و زیرساخت‌های ارتباطی، قادر به جمع‌آوری، پردازش و تبادل مستمر داده‌ها هستند. این فناوری، به‌واسطه ظرفیت بالای خود در بهینه‌سازی فرایندها، افزایش کارآمدی، کاهش هزینه‌ها و ارتقای کیفیت خدمات، در حوزه‌هایی نظیر سلامت، حمل‌ونقل، صنعت، کشاورزی، انرژی و مدیریت شهری جایگاهی روزافزون یافته و به یکی از ارکان اصلی زیست فناورانه معاصر تبدیل شده است. با وجود مزایای گسترده و کارکردهای تحول‌آفرین اینترنت اشیاء، توسعه سریع و گاه شتاب‌زده آن، چالش‌های عمیق و چندلایه‌ای را نیز پدید آورده است. ماهیت فراگیر، نامرئی و دائمی جمع‌آوری داده در این فناوری، از یک سو، مخاطرات متعددی را در حوزه امنیت سایبری به همراه دارد و از سوی دیگر، پرسش‌های مهمی را در قلمرو اخلاق، حقوق و حکمرانی فناوری مطرح می‌سازد. اتصال مداوم دستگاه‌ها به شبکه، ضعف در طراحی امن، فقدان به‌روزرسانی‌های منظم، آسیب‌پذیری پروتکل‌های ارتباطی و امکان دسترسی غیرمجاز به داده‌های حساس، اینترنت اشیاء را به بستری مستعد برای حملات سایبری، نقض حریم خصوصی، سوءاستفاده از اطلاعات شخصی و حتی تهدید زیرساخت‌های حیاتی تبدیل کرده است. در چنین شرایطی، صرف تکیه بر راه‌حل‌های فنی برای مواجهه با این چالش‌ها کافی نیست، بلکه باید ابعاد حقوقی، اخلاقی و اجتماعی این پدیده نیز به‌صورت هم‌زمان و نظام‌مند مورد توجه قرار گیرد. اهمیت این مسئله زمانی دوچندان می‌شود که بدانیم بخش قابل توجهی از داده‌های تولید و پردازش‌شده در اکوسیستم اینترنت اشیاء، ماهیتی شخصی، حساس و گاه حیاتی دارند. داده‌های مربوط به سلامت، موقعیت جغرافیایی، الگوهای رفتاری، سبک زندگی و عادات روزمره افراد، در صورت جمع‌آوری، پردازش یا افشای غیرمجاز، می‌توانند به نقض گسترده حریم خصوصی، تبعیض، نظارت افراطی، استثمار تجاری کاربران و آسیب‌های مادی و معنوی منجر شوند. از این منظر، اینترنت اشیاء تنها یک فناوری کارآمد نیست، بلکه عرصه‌ای نوین برای بازاندیشی در مفاهیم بنیادینی چون رضایت آگاهانه، خودمختاری اطلاعاتی، مسئولیت‌پذیری فناورانه، عدالت الگوریتمی و حمایت از داده‌های شخصی به شمار می‌رود. بر همین اساس، بررسی هم‌زمان چالش‌های امنیتی و آسیب‌پذیری‌های اخلاقی این فناوری، ضرورتی انکارناپذیر برای نظام‌های حقوقی، نهادهای سیاست‌گذار، تولیدکنندگان فناوری و کاربران محسوب می‌شود. در ادبیات موجود، هرچند بخشی از مطالعات به جنبه‌های فنی و امنیتی اینترنت اشیاء پرداخته و برخی دیگر بر مسئله حریم خصوصی و حمایت از داده‌ها تمرکز کرده‌اند، اما نیاز به پژوهش‌هایی احساس می‌شود که با رویکردی میان‌رشته‌ای و تحلیلی، پیوند میان تهدیدات امنیتی و پیامدهای اخلاقی و حقوقی آن را به‌صورت منسجم تبیین نماید. در نتیجه، اهمیت این پژوهش در آن است که با نگاهی تلفیقی و مسئله‌محور، اینترنت اشیاء را نه صرفاً به‌عنوان یک فناوری کارآمد، بلکه به‌مثابه یک پدیده حقوقی، اخلاقی و امنیتی تحلیل می‌کند؛ پدیده‌ای که بهره‌برداری مطلوب از آن، مستلزم توازن میان نوآوری فناورانه و صیانت از حقوق و آزادی‌های بنیادین انسان است. بدون استقرار این توازن، توسعه اینترنت اشیاء می‌تواند به جای آنکه در خدمت رفاه و پیشرفت انسان قرار گیرد، به منشأیی برای تعمیق مخاطرات امنیتی، تضعیف اعتماد عمومی و نقض حقوق اشخاص بدل شود. بر این اساس، مسئله اصلی

پژوهش حاضر آن است که اینترنت اشیاء با وجود کارکردهای گسترده و مزایای غیرقابل انکار، چه چالش‌ها و آسیب‌پذیری‌های امنیتی و اخلاقی ایجاد می‌کند و چه راهکارهایی می‌توان برای کاهش این مخاطرات و استقرار نوعی حکمرانی مسئولانه و اخلاق‌مدار در این حوزه ارائه کرد. در پاسخ به این مسئله، پژوهش حاضر می‌کوشد ضمن شناسایی مهم‌ترین تهدیدات سایبری و مخاطرات اخلاقی در بستر اینترنت اشیاء، نسبت میان امنیت، حریم خصوصی، شفافیت، عدالت و مسئولیت‌پذیری را در این اکوسیستم تحلیل کرده و راهکارهایی اجرایی برای ارتقای سطح امنیت و رعایت ملاحظات اخلاقی ارائه دهد.

بدین‌منظور، ابتدا مفهوم و کاربردهای اینترنت اشیاء تبیین می‌گردد؛ سپس مسائل اخلاقی ناشی از جمع‌آوری و پردازش داده‌ها، افشای اطلاعات، بهره‌برداری تجاری از داده‌ها، تبعیض‌های الگوریتمی و وضعیت گروه‌های آسیب‌پذیر، به‌ویژه کودکان و نوجوانان، تحلیل می‌شود، در ادامه، مهم‌ترین چالش‌ها و آسیب پذیری‌های امنیتی اینترنت اشیاء از جمله تهدیدات سایبری، ضعف حفاظت از داده‌ها، فقدان به‌روزرسانی و سوءاستفاده‌های اجتماعی، مورد بررسی قرار می‌گیرد و در نهایت، راهکارهایی مانند تقویت استانداردهای حقوقی و فنی، طراحی مبتنی بر حریم خصوصی، آموزش کاربران، پشتیبانی بلندمدت از دستگاه‌ها و توسعه هوش مصنوعی اخلاقی ارائه خواهد شد.

پیشینه پژوهش

حسین‌زاده و رضایی (۱۴۰۲) در مقاله‌ای با عنوان «امنیت سایبری در حوزه اینترنت اشیاء» که در فصلنامه آرمان پردازش منتشر شده است، با تمرکز بر ابعاد فناورانه و امنیتی اینترنت اشیاء، به بررسی این موضوع پرداخته‌اند که با افزایش روزافزون دستگاه‌های متصل به اینترنت، موضوع امنیت سایبری به یکی از اصلی‌ترین چالش‌ها و دغدغه‌های جامعه جهانی بدل شده است. مقاله با بررسی تهدیدات امنیتی حوزه اینترنت اشیاء نشان می‌دهد که چنانچه امنیت سایبری به صورت جدی مورد توجه قرار نگیرد، اینترنت اشیاء می‌تواند به بستری برای جرایم سایبری گسترده و حتی تهدیدات علیه امنیت تبدیل شود. یافته‌های مقاله بیانگر آن است که امنیت سایبری یک فرآیند مستمر و پویاست که نیازمند رویکردی چندلایه، تحلیل‌محور و پیشگیرانه است. تفاوت این منبع با مقاله حاضر در این است که نگاه آن صرفاً محدود به سطح فنی و امنیتی بوده و به ابعاد و چالش‌های اخلاقی اینترنت اشیاء توجهی ندارد.

لوسه و همکاران (۱۴۰۲) در کتابی با عنوان «مسئولیت هوش مصنوعی و اینترنت اشیاء» که توسط فاطمه نجیب‌زاده ترجمه شده است، به‌طور خاص به موضوع مسئولیت ناشی از کاربرد هوش مصنوعی و اینترنت اشیاء می‌پردازند. نویسندگان با بررسی مبانی سنتی مسئولیت در حقوق خصوصی، نشان می‌دهند که قواعد کلاسیک مسئولیت مبتنی بر تقصیر به‌تنهایی پاسخگوی چالش‌های ناشی از فناوری‌های خودکار و پیش‌بینی‌ناپذیر نیستند و نیاز به بازنگری و طراحی نظام‌های جدید مسئولیت احساس می‌شود. یافته‌های کتاب حاکی از آن است که برای مدیریت ریسک‌های ناشی از اینترنت اشیاء و هوش مصنوعی باید نظام ترکیبی مسئولیت در نظر گرفته شود و در حوزه‌های پرخطر مانند خودروهای خودران یا ربات‌های پزشکی، مسئولیت سخت‌گیرانه و نوعی اعمال گردد. تفاوت اساسی این کتاب با مقاله حاضر در این است که کتاب بیشتر بر حوزه مسئولیت مدنی و جبران خسارت متمرکز است، در حالی که

پژوهش حاضر به بررسی چالش‌های امنیتی و اخلاقی در اینترنت اشیاء خواهد پرداخت.

رلف و رومانا وبر (۱۳۹۹) در کتابی با عنوان «چشم انداز حقوقی اینترنت اشیاء» که توسط فاطمه اقدسی ترجمه شده است، با رویکردی مرحله به مرحله ابتدا مفهوم اینترنت اشیا را تبیین می‌نمایند و برای فهم حقوقی بعدی، بستر فنی آن را به‌طور نسبتاً عمیق می‌گشایند. نویسندگان توضیح می‌دهند که اینترنت اشیاء یک فناوری فراملی و پیچیده است که از یک‌سو فرصت‌های گسترده‌ای برای رفاه بشر، بهداشت، امنیت غذایی و کاهش شکاف دیجیتال فراهم می‌کند و از سوی دیگر، تهدیدات و آسیب‌پذیری‌های قابل توجهی در حوزه امنیت داده‌ها و مسئولیت حقوقی به همراه دارد. در این کتاب موضوع چارچوب‌های قانون‌گذاری اینترنت اشیا مورد توجه قرار گرفته است و نویسندگان مطرح می‌کنند که اینترنت اشیاء بیشتر متمایل به سمت خود نظام دهی است. در این کتاب نویسندگان به ضرورت هماهنگی قوانین ملی با استانداردهای بین‌المللی و ایجاد یک سازوکار حقوقی جهانی یا حداقل منطقه‌ای برای مقابله با تهدیدات اینترنت اشیاء اشاره دارند. تفاوت اصلی این کتاب با مقاله حاضر در آن است که کتاب بیشتر به کلیات حقوقی و چارچوب‌های حکمرانی اینترنت اشیاء پرداخته است، در حالی که پژوهش حاضر به تحلیل چالش‌های امنیتی و اخلاقی در اینترنت اشیاء و ارائه راهکارها در این راستا می‌پردازد.

۱. چارچوب مفهومی و نظری پژوهش

تحلیل منسجم چالش‌های اخلاقی و امنیتی اینترنت اشیاء، پیش از هر چیز، مستلزم تبیین دقیق موضوع و تعیین مبانی نظری ارزیابی آن است. ازاین‌رو، در این بخش ابتدا مفهوم و مهم‌ترین کاربردهای اینترنت اشیاء بررسی می‌شود و سپس چارچوب نظری پژوهش بر پایه اخلاق فناوری و اخلاق کاربردی ارائه می‌گردد تا مبنای هنجاری لازم برای تحلیل مباحث بعدی فراهم شود.

۱-۱. مفهوم و کاربردهای اینترنت اشیاء

برای واژه اینترنت اشیاء[1] تعاریف مختلفی وجود دارد. کوین اشتون[2] در سال ۱۹۹۹ میلادی برای نخستین بار واژه اینترنت اشیاء را به کار برد تا مفهومی نوین در پیوند میان فضای مجازی و جهان فیزیکی را تبیین نماید. وی این اصطلاح را برای توصیف سامانه‌ای مطرح ساخت که با استفاده از حس‌گرها امکان برقراری ارتباط مستقیم میان اشیاء و شبکه اینترنت را فراهم می‌سازد. در چشم‌انداز ترسیم شده توسط او، اشیای بی‌جان واجد هویتی دیجیتال خواهند بود و از این طریق، قابلیت سازمان‌دهی، شناسایی و مدیریت توسط رایانه‌ها را پیدا می‌کنند (بختیاری، ۱۴۰۱، ص ۵۸).

براساس تعریف اتحادیه بین المللی مخابرات[3]، اینترنت اشیاء زیر ساختی برای راه اندازی یک شبکه جهانی پویا، همراه با قابلیت خود پیکربندی و مبتنی بر پروتکل‌های ارتباطی استاندارد و سازگار با سایر بخش‌های شبکه است. در این زیرساخت، اشیاء فیزیکی

1. Internet of Things (IoT)
2. Kevin Ashton
3. International Telecommunication Union (ITU)

و مجازی دارای هویت مستقل، ویژگی‌های فیزیکی مشخص و شخصیت مجازی هستند و از طریق واسطهای هوشمند، با شبکه اطلاعاتی یکپارچه شده‌اند؛ به عبارت دیگر اینترنت اشیاء زیرساختی جهانی برای جامعه اطلاعاتی است که با بهره‌گیری از تعامل و ارتباط میان اشیاء فیزیکی و مجازی، امکان ارائه خدمات نوین و پیشرفته را فراهم می‌سازد (ITU-T Y2060, 2012). در این تعریف، اینترنت اشیاء به‌عنوان بستری پویا و در حال تکامل معرفی می‌شود که قادر است از ظرفیت‌های موجود در فناوری‌های اطلاعاتی و ارتباطی برای ایجاد ارتباطات هوشمند میان افراد، اشیاء و سامانه‌ها استفاده کند.

از سوی دیگر، سازمان همکاری و توسعه اقتصادی[1] در تعریفی، اینترنت اشیاء را مجموعه‌ای از دستگاه‌ها و اشیائی معرفی می‌کند که وضعیت یا حالت آن‌ها می‌تواند از طریق شبکه اینترنت، با یا بدون دخالت مستقیم انسان، تغییر کند (OECD, 2023). این تعریف بر جنبه کارکردی اینترنت اشیاء تمرکز دارد و نشان می‌دهد که هدف اصلی آن، هوشمندسازی اشیای روزمره و یکپارچه‌سازی آن‌ها در بستر داده محور جهانی است. می‌توان گفت عناصر تشکیل دهنده اینترنت اشیاء عبارت است از: شیء فیزیکی، کنترل کننده‌ها، حسگرها، عملگرها و اینترنت که در کنار هم نوعی هوشمندی سایبری را برای اشیاء فیزیکی به ارمغان می‌آورند. (کیان‌خواه و کریمی قهرودی، ۱۳۹۴، ص ۸۷) بنابراین بر اساس منابع مختلف، اینترنت اشیاء را می‌توان شبکه‌ای یکپارچه و سامانه‌ای گسترده از دستگاه‌های متصل به یکدیگر دانست که هر یک دارای شناسه منحصربه‌فرد و آدرس اختصاصی برای اتصال به اینترنت بوده و قابلیت برقراری ارتباط با خود و سایر دستگاه‌ها را دارند. این تجهیزات قادرند داده‌ها و اطلاعات را جمع‌آوری، تبادل، سنجش، پردازش و به اشتراک بگذارند. افزون بر این، آن‌ها می‌توانند بر اساس نتایج به‌دست‌آمده از سایر دستگاه‌ها یا دستورات انسانی، با حداقل یا حتی بدون مداخله انسان، اقدام به اجرای وظایف گوناگون کرده و تصمیم‌های هوشمندانه اتخاذ نمایند. در واقع، اینترنت اشیا بستری را فراهم می‌آورد که به‌واسطه آن، انسان می‌تواند اشیای مورد استفاده روزمره را که به حسگرها و نرم‌افزارهای الکترونیکی مجهز شده‌اند، به اینترنت متصل سازد و از ظرفیت‌های هوشمند آن‌ها بهره‌مند شود.

اینترنت اشیاء در زندگی افراد و جوامع کاربردهای فراوانی دارد و در زمینه‌های مختلفی می‌تواند تحولات شگرفی ایجاد کند. از جمله مهم‌ترین کاربردهای این فناوری در حوزه‌های سلامت، حمل‌ونقل، صنعت، انرژی، کشاورزی، و محیط‌زیست می‌توان اشاره کرد. در حوزه سلامت و تجهیزات پزشکی، اینترنت اشیاء به تجهیز ابزارهای پزشکی به حسگرهای هوشمند کمک می‌کند تا امکان پایش مستمر وضعیت بیماران، تنظیم خودکار دارو و نظارت از راه دور توسط پزشکان فراهم شود. تجهیزاتی مانند ربات‌های جراحی، پمپ‌های انسولین هوشمند، ضربان‌سازهای متصل و دستبندهای سلامت، از نمونه‌های بارز این کاربرد هستند که نقش مهمی در ارتقای کیفیت خدمات درمانی ایفا می‌کنند. با استفاده از این فناوری، پزشکان قادر خواهند بود به‌صورت لحظه‌ای وضعیت بیماران را تحت نظر قرار دهند و در صورت بروز هرگونه تغییر در وضعیت بیمار، اقدامات فوری و مؤثری انجام دهند. در بخش حمل‌ونقل و صنعت خودرو، اینترنت اشیاء بستر لازم برای توسعه خودروهای متصل و خودران را فراهم کرده است. این فناوری به بهینه‌سازی الگوهای ترافیکی، کاهش تصادفات، و مدیریت هوشمند مصرف سوخت کمک می‌کند. همچنین سامانه‌های حمل‌ونقل عمومی

1. Organization for Economic Co-operation and Development (OECD)

هوشمند، سیستم‌های مترو و قطارهای هوشمند، و پهپادها و هواپیماهای بدون سرنشین از دیگر جلوه‌های این کاربرد محسوب می‌شوند. این فناوری‌ها در تلاش برای ایجاد حمل‌ونقل پایدار و ایمن‌تر هستند و می‌توانند نقش مهمی در بهبود کیفیت زندگی شهری ایفا کنند. در عرصه صنعت و تولید، اینترنت اشیاء با شکل‌دهی به کارخانه‌های هوشمند به کنترل و پایش فرآیندهای تولید، بهینه‌سازی مصرف انرژی، مدیریت زنجیره تأمین، پیش‌بینی خرابی تجهیزات و افزایش بهره‌وری کمک می‌کند. در این زمینه، حسگرهای متصل به ماشین‌آلات و تجهیزات قادر به جمع‌آوری داده‌ها در زمان واقعی هستند و این اطلاعات می‌تواند برای بهینه‌سازی فرآیندها و کاهش هزینه‌ها مورد استفاده قرار گیرد. با استفاده از اینترنت اشیاء، فرآیندهای تولید به‌طور هوشمند و بهینه مدیریت می‌شوند که موجب افزایش سرعت تولید و کاهش هدررفت منابع می‌شود (معینی‌فر و وحیدزاده، ۱۴۰۱، ص ۶۹-۷۰).

در حوزه انرژی و برق، شبکه‌های هوشمند توزیع که بر پایه فناوری اینترنت اشیاء بنا شده‌اند، امکان مدیریت لحظه‌ای مصرف، کاهش تلفات انرژی و بهبود پایداری شبکه را فراهم می‌آورند. این شبکه‌ها با استفاده از حسگرهای متصل به تجهیزات شبکه برق، داده‌های مربوط به مصرف و تولید انرژی را در زمان واقعی جمع‌آوری و تحلیل می‌کنند و از این اطلاعات برای بهینه‌سازی مصرف انرژی و کاهش هزینه‌ها استفاده می‌شود. در بخش کشاورزی هوشمند، اینترنت اشیاء با استفاده از حسگرهای متصل برای سنجش رطوبت خاک، کنترل مصرف آب، تحلیل داده‌های اقلیمی و پایش سلامت محصولات، منجر به افزایش بهره‌وری و کاهش اتلاف منابع طبیعی می‌شود. با استفاده از این فناوری، کشاورزان قادر خواهند بود تا در زمان واقعی وضعیت مزارع خود را تحت نظر قرار دهند و از این طریق مصرف منابع طبیعی مانند آب را بهینه کنند. در حوزه محیط‌زیست، اینترنت اشیاء می‌تواند در مدیریت منابع طبیعی و پایش آلودگی‌ها نقش کلیدی ایفا کند. از طریق حسگرهای محیطی متصل به اینترنت، می‌توان داده‌هایی از قبیل کیفیت هوا، میزان آلودگی آب و شرایط محیطی مختلف را جمع‌آوری کرده و در زمان واقعی به مسئولین و سازمان‌ها گزارش داد تا اقدامات لازم برای حفاظت از محیط‌زیست انجام گیرد. این قابلیت‌ها می‌توانند به شفاف‌سازی اطلاعات زیست‌محیطی و اتخاذ سیاست‌های مناسب برای مقابله با چالش‌های زیست‌محیطی کمک کنند (نجف‌پور و همکاران، ۱۳۹۷، ص ۵۰).

اینترنت اشیاء با داشتن پتانسیل‌های فراوان، می‌تواند به‌عنوان یک نیروی محرکه در دنیای امروز به تحولات اساسی در صنایع مختلف منجر شود. با این حال، این فناوری نیازمند مدیریت و پیاده‌سازی دقیق و مؤثر است تا از بروز مشکلات امنیتی، اخلاقی و اجتماعی جلوگیری شده و از ظرفیت‌های آن به بهترین نحو استفاده شود.

۲-۱. چارچوب نظری اخلاق فناوری و اخلاق کاربردی در اینترنت اشیاء

اخلاق فناوری شاخه‌ای از اخلاق کاربردی است که مشروعیت اخلاقی طراحی، تولید، استقرار و آثار اجتماعی فناوری را ارزیابی می‌کند. در این رویکرد، فناوری ابزار خنثی تلقی نمی‌شود؛ زیرا معماری فنی، تنظیمات پیش‌فرض، مدل کسب‌وکار و قواعد دسترسی به داده‌ها می‌توانند ارزش‌هایی مانند حریم خصوصی، آزادی انتخاب، عدالت یا نظارت را در خود تثبیت کنند (بوالهری و همکاران، ۱۴۰۱، ص ۳۱). بنابراین، ارزیابی اخلاقی اینترنت اشیاء نباید به قصد ذهنی تولیدکننده یا رضایت ظاهری کاربر محدود شود، بلکه

باید ساختار فنی سامانه، روابط قدرت میان بازیگران، پیامدهای مستقیم و غیرمستقیم و توزیع منافع و مخاطرات را نیز دربرگیرد.

در سطح نظریه‌های هنجاری، پژوهش حاضر از دو چارچوب وظیفه‌گرایی و پیامدگرایی بهره می‌گیرد. بر مبنای اخلاق وظیفه‌گرا، اشخاص نباید صرفاً وسیله‌ای برای استخراج داده، تبلیغات یا بهینه‌سازی تجاری تلقی شوند و احترام به کرامت، حق انتخاب و خودمختاری اطلاعاتی آنان، مستقل از سود اقتصادی یا کارآمدی سامانه، یک الزام اخلاقی است. در مقابل، پیامدگرایی اخلاقی بر سنجش مجموع منافع و زیان‌های فناوری تأکید دارد و ایجاب می‌کند منافع حاصل از خدمات هوشمند با احتمال و شدت آسیب‌هایی مانند افشای داده، سرقت هویت، تبعیض، تهدید سلامت یا اختلال در زیرساخت‌های حیاتی مقایسه شود (Mill, 2001, p. 32). ترکیب این دو دیدگاه مانع از آن می‌شود که منفعت عمومی به توجیه نقض حقوق بنیادین تبدیل شود یا، برعکس، آثار واقعی و اجتماعی تصمیم‌های فناورانه نادیده گرفته شود.

در این راستا برای عملیاتی‌کردن اخلاق کاربردی در اینترنت اشیاء، اصولی همچون عدالت، سودرسانی، پرهیز از آسیب، باید مورد توجه قرار گیرد. اصل عدالت، بر توزیع منصفانه منافع، جلوگیری از سوگیری الگوریتمی و حمایت مضاعف از کودکان، سالمندان، بیماران و سایر گروه‌های آسیب‌پذیر دلالت دارد؛ اصل سودرسانی، طراحان را به توسعه سامانه‌هایی متعهد می‌کند که فایده واقعی و قابل اثبات برای کاربران داشته باشند؛ اصل پرهیز از آسیب، پیشگیری از نقض امنیت، افشا، دستکاری و استفاده ثانویه زیان‌بار از داده‌ها را ایجاب می‌کند (Beauchamp & Childress, 2019, p. 143). این اصول مطلق و منفک از یکدیگر نیستند، بلکه در هر کاربرد باید با توجه به شدت خطر، نوع داده، موقعیت کاربر و هدف پردازش تفسیر و موازنه شوند.

در سطح طراحی و حکمرانی اینترنت اشیاء، اخلاق باید به‌عنوان جزء درونی فرایند توسعه فناوری مورد توجه قرار گیرد، نه صرفاً به‌عنوان واکنشی پس از وقوع آسیب. در این راستا رویکرد طراحی ارزش‌محور بر این مبنا استوار است که ارزش‌هایی مانند حریم خصوصی، خودمختاری، امنیت، عدالت، شفافیت و مسئولیت‌پذیری از همان مراحل اولیه طراحی شناسایی و در ساختار فنی سامانه وارد شوند. بر اساس این رویکرد، لازم است ذی‌نفعان و حقوق و منافع آنان به‌صورت مفهومی شناسایی، تجربه‌ها و نگرانی‌های کاربران به‌صورت تجربی بررسی و تأثیر ویژگی‌های فنی دستگاه بر تحقق یا تضعیف ارزش‌های اخلاقی ارزیابی شود (Friedman et al. 2017, p. 78). در کنار آن، چارچوب نوآوری مسئولانه با تأکید بر پیش‌نگری پیامدهای اخلاقی، بازاندیشی انتقادی درباره اهداف و منافع طراحان، مشارکت کاربران و سایر ذی‌نفعان و پاسخ‌گویی در برابر آثار پیش‌بینی‌نشده، مسئولیت اخلاقی تولیدکنندگان را به تمام چرخه حیات دستگاه گسترش می‌دهد (Stilgoe et al. 2013, p. 1571). بر این اساس، رعایت اخلاق در اینترنت اشیاء باید به تعهداتی قابل ارزیابی در مراحل طراحی، آزمون، عرضه، بهره‌برداری، به‌روزرسانی، پشتیبانی و پایان عمر دستگاه تبدیل شود.

بر پایه این مبانی، تحلیل بخش‌های بعدی با معیارهایی چون رضایت آگاهانه، تناسب منفعت مورد انتظار با احتمال و شدت آسیب، انطباق جریان داده با هدف و زمینه مشروع جمع‌آوری، توزیع عادلانه منافع و میزان پیش‌بینی‌پذیری، شفافیت، پاسخ‌گویی و امکان اصلاح در سراسر چرخه حیات فناوری انجام می‌شود. بدین‌ترتیب، مسائل اخلاقی اینترنت اشیاء در این پژوهش صرفاً بر اساس نامطلوب بودن نتایج یا مخالفت اجتماعی تحلیل نمی‌شوند، بلکه با معیارهای هنجاری مشخصی سنجیده خواهند شد که

امکان پیوند میان ملاحظات اخلاقی، الزامات حقوقی و تصمیم‌های فنی را فراهم می‌سازند.

۲. چالش‌های اخلاقی در اکوسیستم اینترنت اشیاء

امنیت در اینترنت اشیاء نه تنها یک مسئله فنی است بلکه به شدت با مسائل اخلاقی و اجتماعی در ارتباط است. جمع‌آوری داده‌ها، حفظ حریم خصوصی کاربران، و استفاده مسئولانه از اطلاعات شخصی از جمله چالش‌های اخلاقی جدی در اینترنت اشیاء به شمار می‌روند. با گسترش روزافزون دستگاه‌های اینترنت اشیاء و تأثیرات آن‌ها در زندگی روزمره، رعایت اصول اخلاقی در نحوه جمع‌آوری، پردازش و استفاده از داده‌ها ضروری است. در این بخش، به بررسی مهم‌ترین مسائل اخلاقی در امنیت اینترنت اشیاء پرداخته می‌شود.

۲-۱. مخاطرات اخلاقی ناشی از سوءاستفاده از داده‌ها و افشای اطلاعات

دستگاه‌های اینترنت اشیاء به‌طور مداوم داده‌های حساس از کاربران جمع‌آوری می‌کنند و در بسیاری از موارد این داده‌ها در فضای ابری ذخیره می‌شوند. استفاده نادرست یا افشای غیرمجاز این داده‌ها می‌تواند عواقب جدی داشته باشد، نه تنها از نظر امنیتی بلکه از نظر اخلاقی نیز بسیار نگران‌کننده است.

در خصوص دستگاه‌های اینترنت اشیاء درحوزه پزشکی و بهداشتی بایستی بیان کرد که داده‌های مربوط به وضعیت سلامتی افراد از حساس‌ترین انواع داده‌ها است. افشای این داده‌ها یا استفاده نادرست از این داده‌ها می‌تواند منجر به عواقب جبران‌ناپذیر شود. به‌عنوان مثال، اطلاعات مربوط به بیماری‌های مزمن، داروهای مصرفی و تاریخچه پزشکی افراد می‌تواند برای سوءاستفاده‌هایی چون اخاذی، تهدیدات اجتماعی یا حتی سیاه‌نمایی مورد استفاده قرار گیرد. در این زمینه، رعایت اصول اخلاقی جمع‌آوری و حفاظت از داده‌ها از اهمیت ویژه‌ای برخوردار است (قاسم‌پور، ۱۴۰۴، ص ۱۱).

در برخی موارد، افشای داده‌های بهداشتی ممکن است عواقب روانی برای فرد به همراه داشته باشد. برای مثال، اگر اطلاعاتی در مورد بیماری یا شرایط جسمانی یک فرد به‌طور غیرمجاز به بیرون درز کند، ممکن است موجب استرس، اضطراب و حتی افسردگی فرد شود. در موارد شدید، این افشاگری‌ها می‌توانند به تهدید به خودکشی یا اختلالات روانی دیگر منجر شوند. یکی دیگر از چالش‌ها در این زمینه سرقت هویت و سوءاستفاده‌های مالی است. داده‌هایی مانند نام، آدرس، اطلاعات بانکی و شماره‌های شناسایی از مهم‌ترین اطلاعاتی هستند که در اینترنت اشیاء جمع‌آوری می‌شوند. اگر این داده‌ها به‌طور نادرست مدیریت شوند، می‌توانند به سرقت هویت منجر شوند. مهاجمان می‌توانند از این داده‌ها برای دسترسی به حساب‌های بانکی، خریدهای آنلاین غیرمجاز یا حتی ایجاد بدهی‌های کاذب به نام افراد استفاده کنند. علاوه بر این، در صورتی که اطلاعات پزشکی یا بهداشتی افراد به‌طور نادرست منتشر شود، ممکن است از آن‌ها برای اخاذی یا سوءاستفاده‌های مالی استفاده شود. یکی از مسائل اخلاقی دیگر، استفاده غیرمجاز از داده‌های جمع‌آوری‌شده برای نظارت اجتماعی است. به‌عنوان مثال، می‌توان از داده‌های موقعیت جغرافیایی یا عادات روزانه افراد برای پیش‌بینی و شبیه‌سازی رفتارهای آن‌ها استفاده کرد (اقدسی و محقق داماد، ۱۴۰۰، ص ۵۳-۵۴). این پیش‌بینی‌ها می‌تواند منجر به ایجاد

پروفایل‌های دقیق اجتماعی و حتی رفتارهای دست‌کاری‌شده شود. علاوه بر این، این داده‌ها می‌توانند برای تبلیغات هدفمند و حتی سوءاستفاده‌های سیاسی استفاده شوند.

۲-۲. مسائل اخلاقی ناظر بر کودکان و جوانان در فضای اینترنت اشیاء

کودکان و نوجوانان به عنوان یکی از گروه‌های آسیب‌پذیر در استفاده از اینترنت اشیاء، با چالش‌های ویژه‌ای در زمینه حریم خصوصی و امنیت روبرو هستند. این گروه‌ها ممکن است آگاهی کمی از خطرات استفاده از این دستگاه‌ها داشته باشند و در نتیجه، در معرض تهدیدات امنیتی و اخلاقی قرار گیرند. بسیاری از کودکان و نوجوانان بدون درک کامل از خطرات، از دستگاه‌های اینترنت اشیاء استفاده می‌کنند. آن‌ها ممکن است مجوزهایی برای دسترسی به داده‌های شخصی خود به اپلیکیشن‌های مختلف بدهند که ممکن است از آن‌ها برای اهداف تجاری یا حتی شبیه‌سازی رفتارهایشان استفاده شود. در این زمینه، والدین باید نظارت بیشتری بر دستگاه‌های هوشمند کودکان خود داشته باشند تا از سوءاستفاده‌های احتمالی جلوگیری کنند (حمیدی، ۱۳۹۴، ص ۵۴).

۲-۳. ملاحظات اخلاقی مرتبط با گردآوری داده‌ها و حریم خصوصی

یکی از مسائل اصلی اخلاقی در اینترنت اشیاء، گردآوری داده‌های شخصی و حریم خصوصی کاربران است. بسیاری از دستگاه‌های اینترنت اشیاء برای کارکرد صحیح خود نیاز دارند که داده‌های مختلفی را از کاربران و محیط اطراف جمع‌آوری کنند. این داده‌ها می‌توانند شامل اطلاعات حساس مانند موقعیت جغرافیایی، وضعیت سلامتی، عادات روزانه و اطلاعات خانوادگی باشند. از آنجا که این دستگاه‌ها به‌طور مستمر و در زمان واقعی داده‌ها را جمع‌آوری می‌کنند، این نگرانی وجود دارد که داده‌ها بدون رضایت یا آگاهی کامل از سوی کاربران، جمع‌آوری و به‌طور غیرقانونی استفاده شوند. از مسائل اخلاقی مهم در جمع‌آوری داده‌ها، نیاز به رضایت آگاهانه کاربران است. بسیاری از دستگاه‌های اینترنت اشیاء از کاربران می‌خواهند که به جمع‌آوری و استفاده از داده‌هایشان رضایت دهند، اما این رضایت معمولاً بدون ارائه اطلاعات کافی در مورد نحوه استفاده و ذخیره‌سازی داده‌ها گرفته می‌شود. این امر باعث می‌شود که کاربران از نحوه استفاده از داده‌های خود آگاه نباشند و ممکن است با استفاده‌های غیرمجاز یا ناخواسته از داده‌هایشان روبرو شوند (Tzafestas, 2018, p. 104).

دستگاه‌های اینترنت اشیاء، به‌ویژه در خانه‌های هوشمند، می‌توانند نظارت دائمی بر رفتارهای کاربران داشته باشند. این امر می‌تواند منجر به نقض حریم خصوصی و احساس نارضایتی کاربران شود. به‌طور مثال، دوربین‌های نظارتی یا دستیارهای صوتی ممکن است همواره فعال باشند و اطلاعات مربوط به فعالیت‌های روزانه کاربران را جمع‌آوری کنند. این داده‌ها می‌توانند به‌طور غیرمجاز در اختیار شرکت‌ها یا اشخاص ثالث قرار گیرند، که ممکن است از آن‌ها برای مقاصد تبلیغاتی یا حتی فعالیت‌های جاسوسی استفاده کنند (Weber, 2017, p. 96).

۲-٤. بهره‌برداری تجاری و تبعیض‌آمیز از داده‌ها

در بسیاری از موارد، دستگاه‌های اینترنت اشیاء داده‌ها را جمع‌آوری کرده و از آن‌ها برای مقاصد تجاری استفاده می‌کنند. این داده‌ها می‌توانند برای بهبود خدمات، ارائه تبلیغات هدفمند یا پیش‌بینی رفتار مشتریان استفاده شوند. این استفاده از داده‌ها باید با رعایت کامل اصول اخلاقی صورت گیرد. در غیر این صورت، استفاده نادرست از داده‌ها می‌تواند به تبعیض و رفتارهای ناعادلانه منجر شود. بسیاری از شرکت‌ها از داده‌های جمع‌آوری‌شده برای طراحی تبلیغات هدفمند استفاده می‌کنند. این تبلیغات ممکن است به‌طور خودکار برای کاربران ارسال شوند و ممکن است حاوی اطلاعات شخصی و حساس باشند که بر تصمیمات خرید و انتخاب‌های شخصی افراد تأثیر بگذارند. این امر می‌تواند منجر به نادیده گرفتن نیازهای واقعی و ترجیحات کاربران و به‌وجود آمدن احساسات استثماری در آن‌ها شود.

یکی دیگر از خطرات استفاده غیرمجاز از داده‌ها، تبعیض و رفتارهای ناعادلانه است. برای مثال، اگر از داده‌های مربوط به نژاد، جنسیت یا وضعیت اقتصادی افراد سوءاستفاده شود، ممکن است منجر به تفکیک اجتماعی یا حتی محرومیت‌های اقتصادی برای گروه‌هایی از جامعه شود. این مسائل می‌توانند تبعات اخلاقی و اجتماعی بزرگی را برای جوامع به همراه داشته باشند. از آنجا که اشیای هوشمند بر مبنای داده‌ها و الگوریتم‌ها عمل می‌کنند، کیفیت این داده‌ها و نحوه طراحی الگوریتم‌ها می‌تواند تعیین‌کننده نحوه رفتار آن‌ها با افراد باشد. بنابراین، اگر داده‌های آموزشی یا الگوریتم‌ها سوگیری داشته باشند، این سوگیری‌ها به‌صورت خودکار در عملکرد اشیای هوشمند بازتاب خواهد یافت و ممکن است منجر به تبعیض ساختاری گسترده شود (Lyon, 2018, p. 97). این ویژگی، اینترنت اشیاء را مستعد آن می‌سازد که به‌جای حذف تبعیض‌ها، به ابزار بازتولید انواع جدیدی از برچسب‌گذاری، تمایزگذاری و طرد اجتماعی تبدیل شود.

۳. چالش‌های امنیتی در اکوسیستم اینترنت اشیاء

اینترنت اشیاء به‌طور گسترده‌ای در زمینه‌های مختلفی مانند خانه‌های هوشمند، مراقبت‌های بهداشتی، صنعت و حمل‌ونقل به کار گرفته می‌شود. با این حال، استفاده از این تکنولوژی با چالش‌ها و آسیب‌پذیری‌های امنیتی سایبری فراوانی همراه است که می‌تواند تهدیدی جدی برای حریم خصوصی و امنیت داده‌ها باشد. این چالش‌ها و آسیب‌پذیری‌ها نه تنها دستگاه‌های فردی بلکه شبکه‌های وسیعی از دستگاه‌ها و حتی زیرساخت‌های حیاتی را تحت تأثیر قرار می‌دهند. در این بخش به بررسی مهم‌ترین چالش‌ها و آسیب‌پذیری‌های امنیتی سایبری در اینترنت اشیاء پرداخته می‌شود.

۳-۱. چالش‌های ناظر بر حریم خصوصی و حفاظت از داده‌های حساس

جمع‌آوری و ذخیره‌سازی داده‌های حساس از کاربران یکی از چالش‌های اصلی اینترنت اشیاء است. این داده‌ها می‌توانند شامل اطلاعات شخصی، موقعیت جغرافیایی، رفتارهای روزانه، اطلاعات سلامت و بسیاری از داده‌های حساس دیگر باشند. عدم رعایت اصول حریم خصوصی در این سیستم‌ها می‌تواند منجر به مشکلات جدی برای کاربران شود.

یکی از این چالش‌ها افشای اطلاعات شخصی است. بسیاری از دستگاه‌های اینترنت اشیاء داده‌هایی مانند موقعیت مکانی

کاربران، فعالیت‌های روزانه و حتی اطلاعات شخصی مانند: نام، سن و وضعیت سلامتی را جمع‌آوری می‌کنند. اگر این داده‌ها به‌درستی محافظت نشوند، می‌توانند به راحتی افشا شوند و برای اهداف مخرب، مانند سرقت هویت یا سوءاستفاده‌های مالی مورد استفاده قرار گیرند. چالش دیگر عدم شفافیت در جمع‌آوری داده‌ها است. درواقع یکی از مسائل اخلاقی در اینترنت اشیاء این است که بسیاری از کاربران از نحوه جمع‌آوری، استفاده و اشتراک‌گذاری داده‌هایشان اطلاعی ندارند. این موضوع می‌تواند منجر به نقض حریم خصوصی افراد شود، زیرا آن‌ها ممکن است بدون اطلاع از نحوه استفاده از داده‌های خود، موافقت به اشتراک‌گذاری آن‌ها را بدهند (لوسه و همکاران، ۱۴۰۲، ص ۱۸۶).

مسئله دیگر مشکلات ذخیره‌سازی داده در فضای ابری است. بسیاری از سیستم‌های اینترنت اشیاء از فضای ابری برای ذخیره‌سازی داده‌ها استفاده می‌کنند. اگر فضای ابری به‌درستی ایمن‌سازی نشود، این داده‌ها می‌توانند مورد دسترسی غیرمجاز قرار گیرند و به سرقت بروند. همچنین، برخی از سرویس‌دهندگان ابری ممکن است از روش‌های امنیتی ضعیف استفاده کنند که منجر به افشای داده‌ها شود (Soni, 2024, p. 18-20).

۳-۲. مخاطرات ناشی از سوءاستفاده‌های اجتماعی در بستر اینترنت اشیاء

با رشد و گسترش سریع فناوری اینترنت اشیاء و تأثیر آن در زندگی روزمره انسان‌ها، این سیستم‌ها می‌توانند به ابزاری برای سوءاستفاده‌های اجتماعی و تهدیدات مرتبط با حریم خصوصی تبدیل شوند. دستگاه‌های اینترنت اشیاء که به‌طور مداوم داده‌های حساس از افراد جمع‌آوری می‌کنند، ممکن است در صورت عدم نظارت مناسب به ابزاری برای نقض حریم خصوصی، نظارت بیش‌ازحد و سوءاستفاده‌های تجاری تبدیل شوند. این سوءاستفاده‌ها به‌ویژه زمانی مشهودتر می‌شوند که دستگاه‌های اینترنت اشیاء در فضای خصوصی کاربران، مانند خانه‌ها یا محل‌های کار، به‌طور دائمی حضور داشته و داده‌های شخصی کاربران را جمع‌آوری می‌کنند. یکی از بزرگ‌ترین خطرات در این زمینه، استفاده نادرست از دستگاه‌های اینترنت اشیاء برای نظارت دائمی بر کاربران است. دستگاه‌هایی مانند دوربین‌های نظارتی، دستیارهای صوتی و سیستم‌های خانه هوشمند ممکن است از افراد در محیط‌های خصوصی نظارت کرده و داده‌های حساس از جمله فعالیت‌های روزانه، مکالمات و موقعیت جغرافیایی آن‌ها را ذخیره و ارسال کنند. در صورتی که این داده‌ها به‌درستی محافظت نشوند یا در اختیار اشخاص ثالث قرار گیرند، نقض حریم خصوصی و سوءاستفاده از این اطلاعات می‌تواند به شدت بر زندگی شخصی افراد تأثیر بگذارد. داده‌های جمع‌آوری‌شده از دستگاه‌های اینترنت اشیاء می‌توانند برای ایجاد پروفایل‌های دقیق از کاربران استفاده شوند و به‌صورت هدفمند برای تبلیغات تجاری، شبیه‌سازی رفتار مصرفی و حتی تغییر رفتارهای خرید افراد به‌کار روند. این نوع سوءاستفاده از داده‌ها می‌تواند به فشارهای اجتماعی و اقتصادی بر افراد منجر شود و از جنبه‌های اخلاقی قابل قبول نیست (Weber, 2017, p. 95). دسترسی غیرمجاز به داده‌های شخصی، به‌ویژه داده‌های مربوط به سلامت یا رفتارهای روزانه افراد، می‌تواند به آسیب‌های روانی جبران‌ناپذیری منجر شود. برای مثال، در صورت افشای اطلاعات بهداشتی یا رفتارهای فردی، فرد ممکن است با استرس، اضطراب یا حتی افسردگی روبه‌رو شود. به‌ویژه در گروه‌های آسیب‌پذیر مانند کودکان،

این آسیب‌ها می‌تواند تأثیرات روانی عمیق‌تری به‌دنبال داشته باشد.

۳-۳. تهدیدات سایبری و آسیب‌پذیری‌های امنیتی

یکی از بزرگ‌ترین مشکلات امنیتی اینترنت اشیاء، آسیب‌پذیری‌های موجود در ارتباطات میان دستگاه‌ها و شبکه‌ها است. دستگاه‌های اینترنت اشیاء به‌طور معمول از پروتکل‌های ارتباطی مختلفی برای تبادل داده‌ها استفاده می‌کنند. این پروتکل‌ها و کانال‌های ارتباطی می‌توانند به راحتی مورد حملات سایبری قرار گیرند. برخی از آسیب‌پذیری‌های اصلی که اینترنت اشیاء با آن‌ها روبرو است عبارتند از:

۱) **حملات سایبری مبتنی بر شبکه**: دستگاه‌های اینترنت اشیاء برای ارتباط با یکدیگر به شبکه‌های بی‌سیم و اینترنتی متکی هستند. این شبکه‌ها ممکن است با ضعف‌هایی در پروتکل‌های امنیتی مواجه باشند که امکان نفوذ به سیستم‌ها و سرقت داده‌ها را فراهم می‌کند (آل‌بویه و آل‌بویه، ۱۴۰۰، ص ۵۲). برای مثال، اگر یک پروتکل امنیتی به‌طور صحیح پیاده‌سازی نشود، مهاجمین می‌توانند اطلاعات حساس مانند داده‌های شخصی یا اطلاعات مربوط به موقعیت جغرافیایی دستگاه‌ها را دستکاری کرده و از آن‌ها سوءاستفاده کنند.

۲) **حملات مبتنی بر داده**: بسیاری از دستگاه‌های اینترنت اشیاء داده‌های شخصی و حساس مانند: اطلاعات مربوط به سلامت، رفتارهای روزانه و موقعیت جغرافیایی افراد را جمع‌آوری می‌کنند. اگر این داده‌ها به‌درستی ذخیره و رمزنگاری نشوند، مهاجمان می‌توانند به آن‌ها دسترسی پیدا کنند و برای اهداف مخرب خود مانند فروش داده‌ها در بازار سیاه یا سوءاستفاده از آن‌ها استفاده کنند.

۳) **حملات مبتنی بر بدافزار**: بسیاری از دستگاه‌های اینترنت اشیاء با استفاده از سیستم‌عامل‌های ساده و بدون محافظت مناسب طراحی شده‌اند. این دستگاه‌ها می‌توانند به‌راحتی آلوده به بدافزار شوند که پس از نفوذ به دستگاه، می‌تواند به سایر دستگاه‌ها در شبکه گسترش یابد و عملکرد دستگاه‌ها را مختل کند. در برخی موارد، این بدافزارها می‌توانند برای ارسال اسپم، دستکاری دوربین‌های نظارتی یا کنترل سیستم‌های حیاتی استفاده شوند.

۴) **حملات شبیه‌سازی**[1]: یکی دیگر از تهدیدات رایج در اینترنت اشیاء، حملات شبیه‌سازی است. در این نوع حملات، مهاجمان از اطلاعات سرقتی یا ضعفی در پروتکل‌ها استفاده می‌کنند تا خود را به‌عنوان یک دستگاه معتبر در شبکه معرفی کنند و دسترسی غیرمجاز به سیستم‌ها و داده‌ها پیدا کنند. این نوع حملات می‌تواند منجر به نفوذ به سیستم‌های حساس مانند سیستم‌های پزشکی یا حمل‌ونقل هوشمند شود (Sasi, 2024, p. 475).

۵) **حملات مبتنی بر رمزنگاری ضعیف**: بسیاری از دستگاه‌های اینترنت اشیاء به دلیل محدودیت‌های سخت‌افزاری، از رمزنگاری ضعیف یا هیچ رمزنگاری استفاده نمی‌کنند. این مسئله باعث می‌شود که داده‌ها در طول انتقال در شبکه، به‌راحتی قابل شنود و دستکاری باشند. به‌عنوان مثال، در برخی از سیستم‌ها، از رمزگذاری‌های ساده‌ای مانند رمزنگاری به روش‌های مبتنی بر کلیدهای عمومی و خصوصی ضعیف استفاده می‌شود که به راحتی قابل شکستن توسط مهاجمان هستند.

1. Impersonation Attacks

۶) **حملات تشخیص و تغییر داده**[1]: در برخی از سیستم‌ها، داده‌ها پس از انتقال ممکن است توسط مهاجمین تغییر داده شوند. این تغییرات می‌توانند تأثیرات جدی بر عملکرد دستگاه‌ها داشته باشند، به‌ویژه در سیستم‌هایی که به اطلاعات دقیق نیاز دارند، مانند سیستم‌های پزشکی یا سیستم‌های نظارتی. تغییر داده‌ها می‌تواند باعث بروز مشکلات جدی برای کاربران و حتی تهدیدات جانی شود (Dhinakaran et al. 2025, p. 5-6).

بر مبنای اخلاق فناوری، تأمین امنیت دستگاه‌های اینترنت اشیاء صرفاً یک مزیت فنی یا تجاری نیست، بلکه تکلیفی اخلاقی است. هنگامی که تولیدکننده از قابل پیش‌بینی بودن حملات، ضعف رمزنگاری یا احتمال دستکاری داده‌ها آگاه است، عرضه یا ادامه بهره‌برداری از دستگاه بدون تدابیر متناسب می‌تواند نقض وظیفه مراقبت تلقی شود. بنابراین، تناسب سطح امنیت با ماهیت داده‌ها، کارکرد دستگاه و شدت زیان احتمالی، یکی از معیارهای اصلی ارزیابی اخلاقی است.

۳-٤. پیامدهای ناشی از فقدان به‌روزرسانی و پشتیبانی فنی دستگاه‌ها

یکی دیگر از مشکلات اساسی در دنیای اینترنت اشیاء، عدم به‌روزرسانی منظم دستگاه‌ها و پروتکل‌های امنیتی است. دستگاه‌های اینترنت اشیاء اغلب از نرم‌افزارها و سیستم‌عامل‌هایی بهره می‌برند که به‌طور مرتب به‌روزرسانی نمی‌شوند. این مشکل در بسیاری از مواقع ناشی از عدم توجه به اهمیت به‌روزرسانی‌های امنیتی از سوی تولیدکنندگان و کاربران است. به‌ویژه، در بسیاری از موارد، دستگاه‌های اینترنت اشیاء در معرض آسیب‌پذیری‌های امنیتی قرار دارند که می‌توانند از طریق حملات سایبری مورد سوءاستفاده قرار گیرند. یکی از جنبه‌های مهم این مسئله این است که دستگاه‌ها معمولاً در شبکه‌های وسیع و به‌هم‌پیوسته‌ای که شامل دستگاه‌های متعددی است، عمل می‌کنند و هنگامی که یک دستگاه در این شبکه‌ها دچار نقص امنیتی شود، ممکن است دیگر دستگاه‌ها را نیز در معرض خطر قرار دهد. عدم به‌روزرسانی نرم‌افزارها و پروتکل‌های امنیتی در دستگاه‌های اینترنت اشیاء می‌تواند منجر به آسیب‌پذیری‌های جدی امنیتی شود. به‌ویژه در سیستم‌هایی که به‌طور مستقیم با داده‌های حساس و حیاتی ارتباط دارند، مانند دستگاه‌های پزشکی، خانه‌های هوشمند یا سیستم‌های حمل‌ونقل هوشمند، نقص‌های امنیتی می‌تواند در نهایت به سرقت داده‌ها، نفوذ به شبکه‌ها و سوءاستفاده‌های مالی و شخصی منجر شود. این دستگاه‌ها معمولاً از پروتکل‌های قدیمی و آسیب‌پذیر برای انتقال داده‌ها استفاده می‌کنند و این مسئله می‌تواند یک دروازه مناسب برای حملات سایبری باشد. یکی دیگر از پیامدهای عدم به‌روزرسانی منظم، افزایش خطرات ناشی از دسترسی غیرمجاز است. بسیاری از دستگاه‌های اینترنت اشیاء که به شبکه‌های حساس متصل هستند، در صورت عدم به‌روزرسانی، به‌راحتی می‌توانند به‌وسیله مهاجمان و هکرها مورد سوءاستفاده قرار گیرند. برای مثال، دستگاه‌های اینترنت اشیاء که از الگوریتم‌های رمزنگاری ضعیف یا حتی بدون رمزنگاری استفاده می‌کنند، می‌توانند اطلاعات حساس مانند تاریخچه پزشکی بیماران یا اطلاعات شخصی افراد را در معرض تهدید قرار دهند. این دسترسی‌های غیرمجاز به‌راحتی می‌توانند منجر به حملات گسترده‌ای در سطح شبکه‌ها و حتی آسیب به زیرساخت‌های حیاتی شوند (غریبی و همکاران، ۱۴۰۳، ص ۱۷۰-

1. Data Tampering and Detection Attacks

۱۷۱). عدم به‌روزرسانی دستگاه‌ها و نرم‌افزارهای آن‌ها باعث می‌شود که بسیاری از این دستگاه‌ها از استانداردهای جدید امنیتی بی‌بهره بمانند و در نتیجه، به‌طور بالقوه در معرض حملات سایبری جدید و پیچیده‌تری قرار گیرند.

قطع پشتیبانی امنیتی از دستگاهی که همچنان در چرخه استفاده قرار دارد، از منظر اخلاق فناوری به معنای انتقال یک‌جانبه ریسک از تولیدکننده به کاربر است. کاربران غالباً از توان فنی لازم برای شناسایی یا رفع آسیب‌پذیری‌ها برخوردار نیستند و هنگام خرید نیز نمی‌توانند مدت واقعی پشتیبانی محصول را پیش‌بینی کنند. اصل عدالت و وظیفه پیشگیری از آسیب اقتضا می‌کنند که تولیدکنندگان مدت پشتیبانی امنیتی را پیشاپیش و به‌صورت شفاف اعلام کرده، به‌روزرسانی‌های ضروری را برای دوره‌ای متناسب ارائه دهند و در پایان عمر محصول، امکان حذف ایمن داده‌ها و غیرفعال‌سازی اتصال آن را فراهم کنند.

٤. راهکارهای اخلاق‌مدار در مواجهه با چالش‌های اینترنت اشیاء

در بخش‌های پیشین، به چالش‌ها و آسیب‌پذیری‌های امنیتی و مسائل اخلاقی در اینترنت اشیاء پرداخته شد. اکنون، در این بخش، راهکارهایی برای بهبود وضعیت امنیت و رعایت اصول اخلاقی در اینترنت اشیاء مطرح خواهد شد. این راهکارها به‌ویژه بر لزوم همکاری میان تولیدکنندگان، دولت‌ها، کاربران و محققان برای ایجاد یک محیط امن و اخلاقی در زمینه اینترنت اشیاء تأکید دارند.

٤-١. توسعه هوش مصنوعی اخلاق‌مدار در اینترنت اشیاء

با توجه به بهره‌گیری روزافزون سامانه‌های اینترنت اشیاء از الگوریتم‌های هوش مصنوعی در تحلیل داده‌ها و اتخاذ تصمیم، توسعه و استقرار اخلاق‌مدار این الگوریتم‌ها یکی از راهکارهای اساسی برای کاهش مخاطرات اخلاقی این اکوسیستم به شمار می‌رود. مقصود از این راهکار، توسعه بیشتر هوش مصنوعی بدون توجه به آثار آن نیست؛ بلکه طراحی، آموزش، ارزیابی و نظارت بر سامانه‌های هوشمند بر پایه اصولی مانند شفافیت، عدالت، حفظ حریم خصوصی، پرهیز از آسیب و پاسخ‌گویی است. در واقع، استفاده فاقد ضابطه از هوش مصنوعی ممکن است به تصمیم‌های غیرشفاف، تبعیض‌آمیز و ناقض حقوق کاربران منجر شود، اما رویکرد اخلاق‌مدار می‌کوشد همین مخاطرات را از طریق پیش‌بینی و کنترل سوگیری‌ها، حفاظت از داده‌های شخصی، فراهم کردن امکان نظارت انسانی و تعیین مسئولیت تصمیم‌های الگوریتمی کاهش دهد. این ضرورت به‌ویژه در سامانه‌های حساس اینترنت اشیاء، مانند تجهیزات پزشکی هوشمند، خودروهای خودران و زیرساخت‌های حمل‌ونقل، اهمیت بیشتری دارد؛ زیرا تصمیم‌های الگوریتمی در این حوزه‌ها می‌توانند مستقیماً بر سلامت، امنیت و حقوق اشخاص اثر بگذارند. بر این اساس، شفافیت و توضیح‌پذیری متناسب با نوع سامانه و مخاطب، یکی از الزامات توسعه اخلاق‌مدار هوش مصنوعی در اینترنت اشیاء است و باید امکان شناخت منطق کلی تصمیم، عوامل مؤثر بر آن و اعتراض به نتایج زیان‌بار را برای کاربران و نهادهای ناظر فراهم سازد (Ahmed et al. 2024, p. 6).

یکی دیگر از الزامات توسعه و استقرار اخلاق‌مدار هوش مصنوعی در اینترنت اشیاء، پیشگیری از تبعیض الگوریتمی است. بسیاری از الگوریتم‌های هوش مصنوعی، به‌ویژه در سیستم‌های یادگیری ماشین، به داده‌هایی که برای آموزش این الگوریتم‌ها استفاده می‌شوند، وابسته هستند. اگر داده‌های آموزشی که برای این الگوریتم‌ها استفاده می‌شوند، شامل تبعیض‌های نژادی، جنسیتی یا

اجتماعی باشند، ممکن است الگوریتم‌های هوش مصنوعی نیز همان تبعیض‌ها را بازتاب دهند و در نهایت منجر به تصمیمات ناعادلانه و تبعیض‌آمیز شوند. برای مثال، در سیستم‌های هوش مصنوعی مورد استفاده در فرآیندهای استخدام یا ارزیابی عملکرد کارکنان، اگر الگوریتم‌ها بر اساس داده‌های قبلی که حاوی تبعیض‌های اجتماعی هستند، برنامه‌ریزی شده باشند، ممکن است این الگوریتم‌ها به‌طور ناعادلانه برخی افراد را نسبت به دیگران اولویت دهند. برای جلوگیری از این نوع تبعیض‌ها، باید در طراحی و آموزش الگوریتم‌های هوش مصنوعی دقت فراوانی صورت گیرد. به‌ویژه، باید از داده‌های آموزشی بی‌طرفانه استفاده شود که شامل نمایندگانی از تمام گروه‌های اجتماعی، نژادی و جنسیتی باشد. علاوه بر این، توسعه‌دهندگان باید از ابزارهای خاصی برای شناسایی و حذف سوگیری‌ها از داده‌ها استفاده کنند. استفاده از روش‌های یادگیری ماشین منصفانه[1] می‌تواند کمک کند که الگوریتم‌ها به‌گونه‌ای طراحی شوند که بر اساس معیارهای بی‌طرفانه و عادلانه تصمیم‌گیری کنند و از ایجاد نابرابری‌ها جلوگیری کنند (Almasoud & Idowu, 2025, p. 2335).

در کنار شفافیت و پیشگیری از تبعیض‌های الگوریتمی، یکی از جنبه‌های مهم دیگر در توسعه هوش مصنوعی اخلاقی در سیستم‌های اینترنت اشیاء، حفاظت از حقوق فردی کاربران است. در این زمینه، باید اطمینان حاصل شود که تصمیمات هوش مصنوعی هیچ‌گونه نقض حریم خصوصی یا سوءاستفاده از این داده‌ها به همراه نداشته باشد. حفاظت از حقوق فردی کاربران در تصمیمات هوش مصنوعی به‌ویژه در سیستم‌هایی که با داده‌های شخصی سروکار دارند، نظیر سیستم‌های بهداشتی، مالی و حمل‌ونقل، از اهمیت زیادی برخوردار است. در این راستا، استفاده از تکنیک‌های پیشرفته رمزنگاری و اطمینان از رضایت آگاهانه کاربران برای جمع‌آوری داده‌ها و استفاده از آن‌ها یکی از الزامات اساسی است (قاسم‌پور، ۱۴۰۴، ص ۱۵). علاوه بر این، باید از سیستم‌های نظارتی و قابل‌اعتماد برای نظارت بر تصمیمات هوش مصنوعی استفاده شود تا اطمینان حاصل شود که این تصمیمات مطابق با قوانین و مقررات حریم خصوصی و اخلاقی اتخاذ می‌شوند.

٤-٢. آموزش و آگاهی‌بخشی به کاربران

یکی از مهم‌ترین جنبه‌های امنیت و اخلاق در اینترنت اشیاء، آموزش و آگاهی‌بخشی به کاربران است. بسیاری از مشکلات امنیتی و اخلاقی ناشی از ناآگاهی کاربران از خطرات امنیتی و نحوه حفاظت از دستگاه‌های اینترنت اشیاء خود است. به‌همین‌دلیل، آموزش‌های لازم در خصوص امنیت و حریم خصوصی دستگاه‌های اینترنت اشیاء باید به کاربران ارائه شود تا آن‌ها بتوانند از داده‌ها و اطلاعات شخصی خود محافظت کنند و به‌درستی از دستگاه‌های خود استفاده کنند. این آموزش‌ها باید شامل نکات اساسی در زمینه امنیت سایبری، تهدیدات اینترنتی و روش‌های مقابله با آن‌ها باشد.

اولین بخش از این آموزش‌ها باید مربوط به آگاه‌سازی کاربران از خطرات و تهدیدات احتمالی ناشی از استفاده از دستگاه‌های اینترنت اشیاء باشد. کاربران باید از تهدیداتی مانند سرقت داده‌ها، حملات سایبری، نقض حریم خصوصی و سوءاستفاده‌های

1. Fair Machine Learning

احتمالی آگاه شوند. برای مثال، آگاهی از حملات رایج مانند حملات فیشینگ، دسترسی غیرمجاز به داده‌ها و تغییرات غیرمجاز در دستگاه‌ها به‌ویژه در سیستم‌های حساس می‌تواند به کاهش ریسک‌ها کمک کند. این آموزش‌ها باید از طریق منابع معتبر، وب‌سایت‌ها و اپلیکیشن‌های موبایل به‌طور مداوم به کاربران ارائه شود و از آن‌ها خواسته شود که برای ایمن‌سازی دستگاه‌های خود اقدامات لازم را انجام دهند. دومین بخش از این آموزش‌ها، آگاهی‌بخشی در خصوص تنظیمات امنیتی دستگاه‌ها است. یکی از دلایل اصلی وقوع حملات سایبری به دستگاه‌های اینترنت اشیاء، استفاده از تنظیمات امنیتی پیش‌فرض و ضعیف است که بسیاری از کاربران از آن‌ها غافل هستند. این تنظیمات می‌توانند شامل رمز عبور پیش‌فرض یا عدم فعال‌سازی ویژگی‌های امنیتی ضروری باشند. آموزش نحوه تغییر رمز عبور پیش‌فرض، فعال‌سازی احراز هویت دو مرحله‌ای و به‌روزرسانی منظم نرم‌افزار دستگاه‌ها می‌تواند از وقوع بسیاری از حملات سایبری جلوگیری کند. کاربران باید آگاه شوند که بسیاری از تهدیدات می‌توانند با تنظیمات ساده امنیتی قابل پیشگیری باشند و هرگونه غفلت در این زمینه می‌تواند عواقب جدی برای امنیت دستگاه‌ها و داده‌ها به دنبال داشته باشد. در نهایت، اطلاع‌رسانی به کاربران در خصوص حقوق و مسئولیت‌های آن‌ها در قبال حریم خصوصی و امنیت داده‌ها از اهمیت ویژه‌ای برخوردار است. کاربران باید از حقوق خود در قبال حریم خصوصی و امنیت داده‌ها مطلع باشند. همچنین، باید آگاه شوند که مسئولیت حفاظت از داده‌های خود در برابر حملات سایبری و سوءاستفاده‌های احتمالی بر عهده خود آن‌هاست (فرحزادی و ناصر، ۱۴۰۰، ص ۱۲۶).

بنابراین، آگاهی‌بخشی و آموزش کاربران در خصوص امنیت و حریم خصوصی دستگاه‌های اینترنت اشیاء یکی از ارکان اساسی برای مقابله با تهدیدات امنیتی و اخلاقی است. افزایش آگاهی در این زمینه می‌تواند به‌طور قابل توجهی از آسیب‌پذیری‌های امنیتی بکاهد و موجب استفاده مسئولانه و ایمن از دستگاه‌های اینترنت اشیاء شود.

٤-٣. طراحی امن و حریم خصوصی محور از مرحله آغازین

یکی از مهم‌ترین اصول اخلاقی در امنیت اینترنت اشیاء، رویکرد حریم خصوصی در طراحی[1] و به‌صورت پیش‌فرض است. این بدان معناست که امنیت و حریم خصوصی باید از مرحله طراحی و توسعه دستگاه‌ها و سیستم‌های اینترنت اشیاء در نظر گرفته شوند و نه به‌عنوان یک موضوع ثانویه یا بعد از راه‌اندازی.

سامانه‌های مبتنی بر اینترنت اشیاء، به‌طور ذاتی داده‌محور، خودکار و فراگیر هستند و اغلب بدون مداخله مستقیم کاربر فعالیت می‌کنند. در چنین سامانه‌هایی، اگر الزامات حریم خصوصی در مرحله طراحی لحاظ نشود، امکان اعمال کنترل مؤثر بر داده‌ها در مراحل بعدی به‌شدت محدود خواهد شد. از این رو، رویکرد حریم خصوصی در طراحی می‌کوشد با پیش‌بینی ریسک‌ها و ادغام ملاحظات حقوقی در تصمیمات فنی، از بروز نقض‌های گسترده حریم خصوصی جلوگیری کند. رویکرد حریم خصوصی در طراحی بر مجموعه‌ای از اصول بنیادین استوار است که هدف آن‌ها تضمین حمایت مؤثر از داده‌های شخصی در کل چرخه حیات سیستم‌ها است. این اصول شامل پیشگیری به‌جای واکنش، حریم خصوصی به‌عنوان وضعیت پیش‌فرض، ادغام حریم خصوصی در طراحی،

1. Privacy by Design

امنیت سرتاسری داده‌ها، شفافیت و قابلیت نظارت، و احترام به حقوق و منافع کاربران است. بر اساس این اصول، سامانه‌ها باید به‌گونه‌ای طراحی شوند که حتی در صورت عدم اقدام فعال کاربر، بیشترین سطح حفاظت از حریم خصوصی به‌طور خودکار اعمال شود. این امر، به‌ویژه در اینترنت اشیاء که کاربران غالباً از جزئیات پردازش داده‌ها آگاه نیستند، اهمیت اساسی دارد (Luthfi & Minhar, 2022, p. 461). از منظر حقوقی، رویکرد حریم خصوصی در طراحی نشان‌دهنده تغییری پارادایمی در نحوه مواجهه با مسئله حمایت از داده‌ها است. در این رویکرد، مسئولیت حمایت از حریم خصوصی صرفاً بر عهده کاربران یا نهادهای نظارتی قرار نمی‌گیرد، بلکه به‌طور مستقیم متوجه طراحان، توسعه‌دهندگان و بهره‌برداران سامانه‌های فناورانه می‌شود. به عبارت دیگر، حقوق حریم خصوصی از سطح تعهدات انتزاعی و پسینی فراتر رفته و به الزامات عینی و پیشینی در فرآیند طراحی فناوری تبدیل می‌شود. بر اساس این رویکرد، کنترل‌کنندگان داده موظف‌اند در تعیین ابزارها و شیوه‌های پردازش داده‌ها، تدابیر فنی و سازمانی مناسب را به‌گونه‌ای اتخاذ کنند که اصول بنیادین حمایت از داده‌ها، از جمله حداقل‌سازی داده‌ها، هدف‌مندی پردازش و امنیت اطلاعات، به‌طور مؤثر رعایت شود. بدین ترتیب، حریم خصوصی دیگر صرفاً یک ارزش اخلاقی یا توصیه سیاستی نیست، بلکه به یک الزام حقوقی صریح تبدیل می‌شود (معینی‌فر و وحیدزاده، ۱۴۰۱، ص ۶۸).

از آنجا که بسیاری از دستگاه‌های اینترنت اشیاء به جمع‌آوری داده‌ها از کاربران پرداخته و این داده‌ها ممکن است حاوی اطلاعات شخصی و حساس باشند، برای رعایت اخلاق در جمع‌آوری داده‌ها باید از تکنیک‌های حداقل‌سازی داده[1] استفاده شود. این به این معنی است که تنها داده‌های ضروری برای عملکرد سیستم جمع‌آوری شوند و داده‌های اضافی یا غیرضروری حذف شوند. به‌طور مثال، در سیستم‌های پزشکی، اطلاعاتی که برای تشخیص یا درمان بیمار ضروری هستند باید جمع‌آوری شوند و اطلاعات اضافی مانند عادات شخصی باید از سیستم حذف گردند (صادقی و ناصر، ۱۳۹۹، ص ۹۶).

علاوه بر آن، داده‌های جمع‌آوری‌شده در سیستم‌های اینترنت اشیاء باید به‌گونه‌ای پنهان یا رمزگذاری شوند که هویت کاربران قابل شناسایی نباشد. این کار می‌تواند با استفاده از تکنیک‌هایی مانند پنهان‌سازی داده‌ها[2] انجام شود. به‌طور مثال، در سیستم‌های پزشکی، اطلاعات مربوط به وضعیت سلامت بیماران باید به‌صورت ناشناس ذخیره شوند تا در صورت سرقت یا افشای این داده‌ها، هویت فرد به خطر نیافتد و از سوءاستفاده‌های احتمالی جلوگیری شود. علاوه بر این، از آنجا که دستگاه‌های اینترنت اشیاء معمولاً از شبکه‌های بی‌سیم و اینترنت برای برقراری ارتباط با یکدیگر استفاده می‌کنند، پروتکل‌های ارتباطی این دستگاه‌ها باید از الگوریتم‌های رمزنگاری قوی بهره‌برداری کنند تا امنیت داده‌ها حفظ شود. این پروتکل‌ها باید به‌گونه‌ای طراحی شوند که از حملات سایبری مانند حملات مرد در میانه[3]، سرقت داده‌ها و دستکاری اطلاعات جلوگیری کنند. استفاده از الگوریتم‌های پیشرفته رمزنگاری مانند رمزنگاری منحنی بیضوی (ECC) و پروتکل‌های امنیتی مانند SSL/TLS می‌تواند به تقویت امنیت سیستم‌های اینترنت اشیاء و حفظ اطلاعات حساس کاربران کمک کند

1. Data Minimization
2. Data Anonymization
3. Man-in-the-Middle (MTM)

.(Semantha, et al. 2020, p. 5)

٤-٤. هم‌افزایی دولت، جامعه علمی و صنعت در تدوین قوانین و استانداردها

یکی از اولین و ضروری‌ترین گام‌ها برای اطمینان از رعایت اخلاق در امنیت اینترنت اشیاء، همکاری نزدیک بین صنعت، دولت‌ها، جامعه علمی و کاربران است. این همکاری باید منجر به تدوین قوانین و استانداردهایی شود که نه تنها امنیت داده‌ها و حریم خصوصی را تأمین کند، بلکه استفاده مسئولانه از فناوری اینترنت اشیاء را نیز تضمین نماید. در این راستا، یکی از مواردی که بایستی در نظر گرفته شود تدوین قوانین شفاف و جامع است. قوانین باید به‌طور واضح و دقیق نحوه جمع‌آوری، ذخیره‌سازی و استفاده از داده‌های کاربران در دستگاه‌های اینترنت اشیاء را تعیین نمایند. برای مثال، به‌کارگیری مفاهیمی مانند رضایت آگاهانه و حق حذف داده‌ها باید جزء اصول پایه‌ای قوانین باشد. از طرفی، پروتکل‌ها و استانداردهای امنیتی باید به‌طور دقیق تعریف شوند تا دستگاه‌ها و شبکه‌های اینترنت اشیاء از حداکثر حفاظت برخوردار شوند. یکی از چالش‌های اصلی در زمینه اینترنت اشیاء، نگرانی‌ها در خصوص نقض حریم خصوصی کاربران است. مقررات باید الزاماتی را در خصوص نحوه جمع‌آوری و استفاده از داده‌ها، به‌ویژه داده‌های حساس مانند اطلاعات بهداشتی و موقعیت جغرافیایی، تعیین کنند. این مقررات باید تضمین نمایند که داده‌ها تنها برای اهداف معین و با رضایت کامل کاربران جمع‌آوری و استفاده شوند (Tzafestas, 2018, p. 105). علاوه برآن، برای اطمینان از رعایت اصول اخلاقی در امنیت اینترنت اشیاء، بایستی استانداردهای امنیتی- اخلاقی در این راستا تدوین گردد و بر رعایت این استانداردها نظارت مؤثر صورت پذیرد.

٤-٥. به‌روزرسانی مستمر و پشتیبانی طولانی مدت دستگاه‌ها

یکی دیگر از راهکارها برای بهبود امنیت و رعایت اخلاق در اینترنت اشیاء، به‌روزرسانی مستمر دستگاه‌ها و سیستم‌ها است. بسیاری از دستگاه‌های اینترنت اشیاء به دلیل عدم به‌روزرسانی نرم‌افزارها و سیستم‌عامل‌ها، در معرض حملات سایبری قرار دارند. برای جلوگیری از این مشکل، دستگاه‌ها باید به‌طور مرتب به‌روزرسانی شوند و پشتیبانی طولانی‌مدت برای آن‌ها فراهم گردد. بسیاری از دستگاه‌های اینترنت اشیاء پس از گذشت مدت زمانی مشخص و پایان عمر مفید خود دیگر پشتیبانی نمی‌شوند. این موضوع می‌تواند به‌طور جدی امنیت این دستگاه‌ها را تهدید کند، زیرا تولیدکنندگان معمولاً به‌روزرسانی‌های امنیتی را برای این دستگاه‌ها قطع می‌کنند و این موضوع موجب می‌شود که دستگاه‌ها در معرض آسیب‌پذیری‌ها و تهدیدات جدید قرار گیرند. با افزایش استفاده از دستگاه‌های اینترنت اشیاء در حوزه‌های حساس مانند بهداشت و درمان، امنیت اطلاعات مالی و حتی زیرساخت‌های حیاتی شهری، پشتیبانی طولانی‌مدت از دستگاه‌ها از اهمیت ویژه‌ای برخوردار است. اگر تولیدکنندگان از دستگاه‌های قدیمی خود پشتیبانی نکنند و به‌روزرسانی‌های امنیتی برای آن‌ها ارائه ندهند، این دستگاه‌ها می‌توانند به نقطه آسیب‌پذیری برای شبکه‌های متصل تبدیل شوند و حملات سایبری می‌توانند از طریق آن‌ها انجام شوند (حسین‌زاده و رضایی، ۱۴۰۲، ص ۵). برای جلوگیری از این مشکل، تولیدکنندگان باید پشتیبانی از دستگاه‌های خود را برای مدت زمان بیشتری ادامه دهند و به‌روزرسانی‌های امنیتی برای دستگاه‌های

قدیمی نیز ارائه دهند. این پشتیبانی طولانی‌مدت می‌تواند از طریق به‌روزرسانی‌های امنیتی و رفع آسیب‌پذیری‌ها در نسخه‌های نرم‌افزاری قدیمی انجام شود.

در کنار پشتیبانی طولانی‌مدت، لازم است تولیدکنندگان برنامه‌های مشخصی برای مدیریت پایان عمر دستگاه‌های اینترنت اشیاء خود داشته باشند. به‌ویژه در دستگاه‌هایی که در سیستم‌های حیاتی یا بخش‌های حساس مانند بیمارستان‌ها، مراکز مالی و حمل‌ونقل هوشمند استفاده می‌شوند، باید فرآیندهای دقیقی برای مدیریت پایان عمر دستگاه‌ها پیش‌بینی شود. این برنامه‌ها باید شامل مراحل حذف داده‌ها، غیرفعال‌سازی دستگاه‌ها و انجام اقدامات امنیتی برای جلوگیری از سوءاستفاده‌های احتمالی از دستگاه‌های قدیمی باشد. دستگاه‌هایی که پس از پایان عمر مفید خود دیگر مورد استفاده قرار نمی‌گیرند، باید به‌طور کامل از سیستم‌های ذخیره‌سازی و شبکه‌ها حذف شوند تا از دسترسی غیرمجاز به داده‌های حساس جلوگیری شود (Thakral et al., 2022, p. 226). حذف داده‌ها باید به‌طور کامل و مطابق با اصول حفاظت از داده‌ها صورت گیرد، به‌ویژه در دستگاه‌هایی که اطلاعات حساس کاربران یا اطلاعات پزشکی ذخیره می‌کنند. علاوه بر این، غیرفعال‌سازی دستگاه‌ها باید به‌گونه‌ای باشد که دستگاه‌های قدیمی دیگر نتوانند به شبکه‌ها یا سیستم‌ها متصل شوند و از آن‌ها برای حملات سایبری استفاده نشود.

نتیجه‌گیری

اینترنت اشیاء به‌عنوان یکی از فناوری‌های پیشرفته و نوآورانه، به‌طور قابل توجهی بر بسیاری از جنبه‌های زندگی روزمره و صنایع مختلف تأثیر گذاشته است. از آنجایی که این فناوری با اتصال دستگاه‌های فیزیکی به اینترنت و یکدیگر، توانایی جمع‌آوری، پردازش و تبادل داده‌ها را فراهم می‌آورد، کاربردهای فراوانی در زمینه‌هایی چون خانه‌های هوشمند، مراقبت‌های بهداشتی، حمل‌ونقل، کشاورزی و صنعت دارد. در حالی که این پیشرفت‌ها به‌طور کلی به بهبود کارایی، بهره‌وری و کیفیت زندگی انسان‌ها کمک کرده‌اند، به‌ویژه در حوزه‌هایی که با داده‌های حساس و حیاتی سروکار دارند، تهدیدات و چالش‌های امنیتی و اخلاقی نیز به‌طور همزمان ظهور کرده‌اند. مسائل امنیتی مانند حملات سایبری، دسترسی غیرمجاز به داده‌ها و سرقت اطلاعات، از جمله چالش‌های عمده‌ای هستند که می‌توانند به تهدیداتی جدی برای حریم خصوصی کاربران، اعتبار سازمان‌ها و سلامت سیستم‌های اینترنت اشیاء تبدیل شوند. علاوه بر این، مسائل اخلاقی مرتبط با اینترنت اشیاء، نظیر سوءاستفاده از داده‌های شخصی، تبعیض‌های الگوریتمی و نقض حریم خصوصی، باعث بروز نگرانی‌هایی در میان کاربران و جامعه شده است. این مسائل، به‌ویژه در حوزه‌هایی که فناوری‌های نوین در آن‌ها پیاده‌سازی شده‌اند، مانند مراقبت‌های بهداشتی، حمل‌ونقل هوشمند و مدیریت زیرساخت‌ها، نیازمند دقت و حساسیت ویژه‌ای هستند. با توجه به این چالش‌ها، این تحقیق به‌طور دقیق به تحلیل مسائل امنیتی و اخلاقی موجود در اینترنت اشیاء پرداخته است. یافته‌های پژوهش نشان می‌دهند که برای مقابله با تهدیدات امنیتی و رعایت اصول اخلاقی در سیستم‌های اینترنت اشیاء، نیاز به راهکارهایی جامع و منسجم وجود دارد. از جمله این راهکارها می‌توان به به‌روزرسانی منظم دستگاه‌ها، استفاده از پروتکل‌های امنیتی پیشرفته، افزایش شفافیت در الگوریتم‌های هوش مصنوعی، جلوگیری از تبعیض‌های الگوریتمی و ارتقای آگاهی عمومی اشاره کرد.

به‌ویژه، توسعه هوش مصنوعی اخلاقی در سیستم‌های اینترنت اشیاء به‌عنوان یک راه‌حل کلیدی برای کاهش تبعیض‌های الگوریتمی و ارتقای شفافیت در فرآیندهای تصمیم‌گیری هوشمند در این سیستم‌ها مطرح می‌شود. علاوه بر این، به‌روزرسانی منظم دستگاه‌ها و نرم‌افزارها از اهمیت ویژه‌ای برخوردار است، چرا که به‌روزرسانی‌های امنیتی به‌طور مستمر دستگاه‌ها را از آسیب‌پذیری‌های جدید محافظت می‌کند و امکان اجرای پروتکل‌های امنیتی پیشرفته را فراهم می‌آورد. همچنین، شفافیت در عملکرد دستگاه‌های هوش مصنوعی و الگوریتم‌های آن‌ها می‌تواند اعتماد کاربران را جلب کرده و از بروز مشکلات اخلاقی جلوگیری کند. یکی دیگر از عوامل کلیدی در بهبود امنیت و اخلاق در اینترنت اشیاء، آموزش و آگاهی‌بخشی به کاربران است. ناآگاهی کاربران از خطرات امنیتی و نحوه حفاظت از داده‌های خود می‌تواند به تهدیدات جدی منجر شود. بنابراین، لازم است که سازمان‌ها و تولیدکنندگان دستگاه‌های اینترنت اشیاء، به‌طور مستمر به آموزش و آگاهی‌بخشی در خصوص تهدیدات امنیتی و روش‌های محافظت از داده‌ها و حریم خصوصی بپردازند. همچنین بایستی بیان کرد که با ایجاد همکاری‌های مؤثر میان تولیدکنندگان، کاربران و مقامات نظارتی، می‌توان امنیت و اصول اخلاقی را در سیستم‌های اینترنت اشیاء تقویت نمود. به‌ویژه، برای کاهش آسیب‌پذیری‌های امنیتی و حفظ حریم خصوصی کاربران، باید چارچوب‌های قانونی، فنی و اخلاقی به‌طور همزمان مورد توجه قرار گیرند. در مجموع، این تحقیق به‌وضوح نشان می‌دهد که اینترنت اشیاء، با وجود تمامی مزایای آن در بهبود کیفیت زندگی و ارتقای کارایی در بسیاری از حوزه‌ها، نیازمند مدیریت و نظارت دقیق‌تری است تا تهدیدات امنیتی و مسائل اخلاقی مرتبط با آن به‌طور مؤثر برطرف شوند. به‌روزرسانی منظم دستگاه‌ها، استفاده از الگوریتم‌های هوش مصنوعی اخلاقی، افزایش شفافیت و آگاهی‌بخشی به کاربران، از جمله اقداماتی هستند که می‌توانند به کاهش تهدیدات امنیتی و اخلاقی موجود در این زمینه کمک نمایند.

منابع

اقدسی، فاطمه، محقق داماد، مریم سادات. (۱۴۰۰). «ابعاد حقوقی حریم خصوصی در اینترنت اشیا». *فصلنامه پژوهش‌های حقوقی میان رشته‌ای*. تابستان. دوره ۲، شماره ۲، صص ۴۹-۶۷.

آل‌بویه، زینب، آل‌بویه، علیرضا. (۱۴۰۰). «کاربرد نظریهٔ جنگ عادلانه در جنگ سایبری و راهکارهای اخلاقی استفاده از سلاح‌های سایبری». *فصلنامه تأملات اخلاقی*. پاییز. دوره ۲، شماره ۳، صص ۴۹-۷۶.

بختیاری، ایرج. (۱۴۰۱). «تحلیلی بر کاربرد اینترنت اشیاء در شبکه پدافند هوایی از منظر آسیب‌ها و تهدیدها». *فصلنامه علوم و فنون نظامی*. پاییز. دوره ۱۸، شماره ۶۱، صص ۵۵-۸۲.

بوالهری، علیرضا، رادفر، رضا، البرزی، محمود، پورابراهیمی، علیرضا، دهقانی، محمود. (۱۴۰۱). «تبیین تصمیم‌گیری اخلاقی در بستر مدیریت فناوری اطلاعات». *فصلنامه تأملات اخلاقی*. تابستان. دوره ۳، شماره ۲، ۲۹-۴۶.

حسین‌زاده، مرضیه، رضایی، علیرضا. (۱۴۰۲). «امنیت سایبری در حوزه اینترنت اشیاء». *فصلنامه آرمان پردازش*. بهار. دوره ۴، شماره ۱، صص ۱-۹.

حمیدی، حجت‌اله. (۱۳۹۴). «اخلاق و حفاظت از حریم خصوصی آنلاین کودکان با رضایت والدین». *فصلنامه اخلاق در علوم و فناوری*. دوره ۱۰، شماره ۳، صص ۴۱-۵۷.

صادقی، حسین، ناصر، مهدی. (۱۳۹۹). «ارائه چارچوب حقوقی مسئولیت پذیری در عملکرد ابزارهای اینترنت اشیا در بستر دولت الکترونیک؛ تبیین الگوی سیاستگذاری موثر». *فصلنامه سیاست‌گذاری عمومی*. پاییز. دوره ۶، شماره ۳، صص ۸۱-۱۰۳.

غریبی، جواد، قرایی، حسین، فرجی‌پور، محمدرضا، هلیلی، خداداد. (۱۴۰۳). «ارائه طرح راهبردی حاکمیت امنیت داده اینترنت اشیا در شهر هوشمند». *فصلنامه امنیت ملی*. پاییز. دوره ۱۴، شماره ۵۳، صص ۱۴۳-۱۷۶.

فرحزادی، علی‌اکبر، ناصر، مهدی. (۱۴۰۰). «حق بر تبادل داده‌های خصوصی و راهکارهای رفع چالش‌های آن در سازوکار عملکرد ابزارهای اینترنت اشیاء». *بررسی‌های بازرگانی*. پاییز. دوره ۱۸، شماره ۱۰۸، صص ۱۱۵-۱۲۸.

قاسم‌پور، امین. (۱۴۰۴). «کلان داده‌های پزشکی و الش‌های اخلاقی آن از حیث نقض حریم خصوصی بیماران». *فصلنامه اخلاق در علوم و فناوری*. دوره ۲۰، شماره ۲، صص ۹-۱۸.

کیانخواه، احسان، کریمی قهرودی، محمدرضا. (۱۳۹۴). «چالش آفرینی اینترنت اشیاء بر ارکان امنیت ملی کشور». *فصلنامه امنیت ملی*. تابستان. دوره ۵، شماره ۱۶، صص ۸۱-۱۰۶.

لوسه، سباستین، شولتسه، راینر، اشتاودنمایر، دیرک. (۱۴۰۲). *مسئولیت هوش مصنوعی و اینترنت اشیا*. ترجمه: فاطمه نجیب‌زاده، تهران: انتشارات جنگل.

معینی‌فر، محدثه، وحیدزاده، دل‌آرام. (۱۴۰۱). «الزامات استیفای حق بر حریم خصوصی در بستر اینترنت اشیاء از منظر حقوق ایران». *دوفصلنامه حقوق فناوری‌های نوین*. پاییز و زمستان. دوره ۳، شماره ۶، صص ۶۱-۷۵.

نجف پور، وحید، قنبری، علیرضا، نظری، داود، مرادی، عالیه. (۱۳۹۷). «بررسی نقش اینترنت اشیاء در توسعه فناوری‌های نوین در سطح اجتماع و چالش‌ها در آن». *فصلنامه پژوهش در علوم مهندسی و فناوری*. دوره ۴، شماره ۲، صص ۴۹-۶۴.

Ahmed, A. A., Farhan, K., Jabbar, W. A., Al-Othmani, A., & Abdulrahman, A. G. (2024). IoT Forensics: Current Perspectives and Future Directions. Sensors, 24(10), 1-16.

Almasoud, A., Idowu, J. (2025). Algorithmic fairness in predictive policing. AI and Ethics. 5. 2323-2337.

Beauchamp, T. L., & Childress, J. F. (2019). Principles of Biomedical Ethics (8th ed.). Oxford University Press.

Dhinakaran, D., Raja, S., Ramathilagam, A., Vennila, G. (2025). Ethical and legal challenges with IoT in home digital twins, MethodsX. 14.

Friedman, B., Hendry, D. G., & Borning, A. (2017). A survey of value sensitive design methods. Foundations and Trends in Human–Computer Interaction, 11(2), 63–125.

International Telecommunication Union (ITU). (2012). Recommendation ITU-T Y.2060: Overview of the Internet of Things. Geneva: ITU.

Luthfi, A., Minhar, E., (2022). Towards Privacy by Design on the Internet of Things (IoT) Use: A Qualitative Descriptive Study. Journal of Information Systems and Informatics. 4(2). 457-468.

Lyon, D. (2018). The Culture of Surveillance. Cambridge: Polity.

Mill, J. S. (2001). Utilitarianism (2nd ed., G. Sher, Ed.). Hackett Publishing.

Organization for Economic Co-operation and Development (OECD). (2023). Measuring the Internet of Things. OECD Publishing, Paris.

Sasi, T., Lashkari, A., Lu, R., Xiong. P., Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. Journal of Information and Intelligence. 2. 455-513.

Semantha, F., Azam, S., Yeo, Kh. Shanmugam, B. (2020). A Systematic Literature Review on Privacy by Design in the Healthcare Sector. Electronics. 9(3). 452.

Soni, N. (2024). IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. Computer and Telecommunication Engineering, 2(4).

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. Research Policy, 42(9), 1568–1580.

Thakral, M., Singh, R. R., & Kalghatgi, B. V. (2022). Cybersecurity and ethics for IoT system: A massive analysis. In Internet of Things: Security and Privacy in Cyberspace. Springer Nature Singapore. 209-233.

Tzafestas, S. (2018). Ethics and Law in the Internet of Things World. Smart cities journal, 1(1), 98-120.

Weber, V. (2017). The Synergetic Smart City Framework – From Idea to Reality, Real Estate Issues.