e-ISSN: 3107-619X

NBPA Journal for Arts, Humanities & Social Sciences
A Peer-reviewed Multidisciplinary Quarterly Journal

Cyber Ethics: A Philosophical Exploration from the Perspective of 'Human Rights'

Subhajit Das

PhD Research Scholar, Presidency University, Kolkata
Email: subhajitdas.rs@presiuniv.ac.in

Abstract

This study delves into the philosophical underpinnings and practical significance of cyber ethics within the ever-expanding realm of cyberspace. As cyber technologies reshape human consciousness, interaction, and modes of living, they simultaneously introduce profound ethical challenges and moral dilemmas. The digital domain, though a catalyst for global connectivity and information exchange, has also become a space where acts such as hacking, data manipulation, identity obscuration, and intellectual theft thrive. These emerging forms of immorality demand a reflective and principled approach to digital conduct. At the core of this inquiry lies the necessity of embedding ethical frameworks within the very design of software and digital infrastructure—ensuring that technological development is not divorced from moral responsibility. Cyber ethics thus emerges as an interdisciplinary field that interrogates the boundaries of right and wrong in virtual spaces and assesses the broader social consequences of information technologies. Given the global reach and influence of cyberspace, the responsibility to uphold ethical standards extends beyond governments and institutions to include individuals and communities. The collective cultivation of digital morality—anchored in principles of privacy, transparency, and justice—is imperative. This paper argues for a conscious and cooperative effort to engage with cyber ethics not merely as a regulatory necessity, but as a philosophical commitment to human dignity, responsible innovation, and the ethical stewardship of our shared digital future.

Original Article

Open Access

Received: 27.08.2025
Accepted: 04.12.2025
Publication Date: October-December 2025
Volume: 1
Issue: 3
Doi:
https://doi.org/10.65842/nbpa.v1.i3.002

Published by: North Bengal Philosophers Association
Website: **https://nbpajournal.com/**
https://nbpa.org.in/

Key Words: ***Cyber ethics*** . ***Virtual space*** . ***Privacy*** . ***Transparency*** . ***Justice***

Introduction

Today, the virtual world or cyber world has become an integral part of our daily life. Therefore, it's essential to understand security and sequestration issues, as well as the major negative impact of information technology on cyberspace. Although some technical approaches similar to encryption, digital ID, and firewall systems have been developed to overcome some of the troubles, legal action must also be executed encyclopaedically, which will tackle the increasing number of ethical problems arising out of the harmful impact of Information Technology in the world. In our digital society, safeguarding the population, specifically the young people, from cybercrime has become a serious concern. Actually, it is very urgent to save the spiritual likeness of a person to protect their ethical awareness from cyber-attacks. It's truly challenging for any nation to tackle such threats on its own. In these circumstances, it's essential to strengthen international collaboration, leverage the mechanisms of globalization, and work together to combat cybercrime effectively. So that's why we need to produce a particular law of conduct or behaviour, and that's cyber ethics.

Discussion

As a result of the development of the world today, it appears that we have become dependent on technology to a large extent. So, ethics is no longer limited to a theory, but it has become associated with the virtual world itself. So, ethics associated with the virtual world is called cyber-ethics. Cyber ethics is the philosophical inquiry into the moral dimensions of computing, examining both human conduct in digital environments and the ethical implications of what computers are designed to perform. It explores how these technological interactions influence individuals and shape broader societal structures. So the term "Cyber-ethics" refers to a set of moral rules or codes of behaviour applied to the environment. So cyber-ethics creates a safe environment in cyberspace. Cyber ethics is a term commonly used to describe ethical behavior and principles in cyberspace. Cyber ethics refers to the broad range of applied ethical issues that arise from human activities involving technology.

People face various opinions that possess ethical confines in the cyberworld. So it's essential to frame what moral theoretical perspective & ethical persuasions trigger respectable and inferior ethical judgment. Moral theory enables Individuals to take a stand either in support of or against a specific ethical issue related to cyberspace. Various ethical doctrines, such as – Teleology, Kantian ethics, and virtue ethics, are the most applicable to the cyber world. Teleology holds that the ethical proposition is that the consequence of particular conduct is the Foundation for making a legitimate moral assessment of an action, or provides a framework

for such evaluation. Kantian ethics focuses on the duties and moral obligations of individuals, emphasizing what one ought to do regardless of the outcomes their actions may produce. Virtue ethics emphasizes the criteria having to do with Personal growth in character or the moral and ethical development of individuals and the acquisition of good character, particularly. So, it employs these three prominent ethical propositions to prognosticate and explain the ethical judgment of individuals in the cyber world. Therefore, the presence of cyber ethics is essential within the domain of cyberspace.

Cyber ethics, as a philosophical exercise, seeks to explore the moral aspect of human-computer interaction—both the actions of users and programmed intentions of machines, and how these influence individuals and society. As digital technology becomes more and more pervasive in everyday life, especially through the internet and social media use by children, the ethical ramifications become more and more significant. Governments have reacted with regulatory models, and organizations have attempted to establish ethical limits through company policies. However, the moral dilemma still persists, particularly when engaging with youth, who are likely to reject prescriptive concepts of right and wrong. The resistance is an indicator of a more profound philosophical conflict between autonomy and moral direction in the online age. To negotiate this changing landscape, institutions need to develop ethical awareness. Organisations can start with the development of codes of conduct, building an ethical culture of thought, and setting out explicit guidelines for ethical use of information and communication technologies. Simultaneously, professional associations have a similar duty: to revitalize ethical principles, guide young professionals, and maintain critical discussion of the ethical issues brought by information and communication technologies. Finally, the question is not merely how we govern behaviour online, but how we form the moral character of those who live there, leading them to a more reflective, responsible, and compassionate virtual life.

Cyber ethics, through a philosophical lens, constitutes the critical examination of moral conduct within digital realms. It probes the ethical obligations of individuals in cyberspace, considers the consequences of virtual actions on others, and seeks foundational principles to govern human behaviour where the line between virtual existence and physical reality becomes increasingly indistinct.

As stewards of intellectual and moral development, academic institutions bear a foundational responsibility to cultivate ethical awareness in the minds of the young. This entails integrating ethical inquiry and moral reasoning into both education and research agendas. Students must

be awakened to the ethical dimensions of their disciplines and guided in the art of discerning moral dilemmas and exercising principled judgment. Embedding such ethical reflection within the curriculum affirms the university's role not merely as a transmitter of knowledge but as a formative space for nurturing responsible, critically engaged individuals capable of navigating the moral complexities of contemporary life.

The scientific grasp of the challenges posed by virtual reality—particularly the evolving nature of internet-mediated communication—remains in its nascent stages. As with any emergent and transformative phenomenon, cyberspace provokes a spectrum of responses, from irrational anxieties to overly idealized expectations, each accompanied by ethically ambiguous judgments. In light of this conceptual uncertainty, the imperative to establish *cyber ethics* as a domain of applied ethics becomes evident. Its purpose must be to offer sustained moral and philosophical inquiry into the nature of virtual interaction, providing ethical frameworks through which the complexities of digital communication can be critically assessed and responsibly navigated.

Conversely, social networking sites and messaging applications are great resources that can be used to bring children closer to others worldwide. They also provide an entry to cyberbullying. To prevent this, get into the habit of using these sites along with your child and let them understand what online text message communication is. Highlight that the words and things they write and send to a friend mean as close as actual words said out loud. Yet, that word will sting and damage their friendship as badly as an actual fight world, if they say a bad word to a friend. Kids often do not have the foresight to grasp online language, and teaching them about it is a significant component of cyber ethics education.

In light of advancing computational technologies, it becomes imperative to engage deeply with the ethical considerations surrounding cybersecurity, the protection of information confidentiality, and the profound adverse effects wrought by information and communication technologies. Such reflection is essential to navigate the moral landscape shaped by these powerful tools. A structured approach or framework needs to be established to address the increasing range of global ethical issues arising from the negative consequences of information technology within cyberspace and the broader digital society.

Information technology occupies a foundational role across the domains of commerce, governance, healthcare, education, entertainment, and the broader social fabric. Its economic and societal contributions are both profound and self-evident. Yet, as with all technologies, IT

is not morally neutral—it carries with it a set of complex ethical implications. While it empowers and connects, it also disrupts, challenges norms, and raises pressing moral questions. At the heart of these concerns lie three principal ethical dimensions: the preservation of individual privacy, the just and equitable access to digital resources, and the mitigation of harmful or destructive behaviour within technological environments.

In the realm of personal privacy, information technology facilitates the vast and instantaneous exchange of data across global boundaries, transcending time and space. This unprecedented connectivity amplifies the risk of unauthorized disclosure and infringements upon the privacy rights of individuals and communities, as sensitive information circulates widely and uncontrollably. Thus, it becomes a profound ethical obligation and collective challenge to safeguard the sanctity and integrity of personal data, honouring the dignity and autonomy of those it represents.

The second critical dimension of ethical concern in computing pertains to access rights. With the rapid expansion of global digital commerce, issues surrounding computer security and equitable access have shifted from peripheral considerations to urgent ethical imperatives for both corporations and governmental institutions. Incidents of unauthorized intrusions, such as those targeting prominent entities like Los Alamos National Laboratories and NASA, underscore the vulnerability inherent in digital infrastructures. Repeated violations of governmental and military systems by hackers highlight the ethical necessity of safeguarding these networks. Without robust security frameworks and principled regulatory measures, the integrity of digital communication and data remains precarious. Hence, the establishment of clear and enforceable codes of conduct is essential to uphold justice, trust, and responsibility within the interconnected digital sphere.

So, there are 3 main types of issues with ethical implications in cyberspace.

- Personal privacy
- Right to access
- Harmful actions

In the contemporary digital age, individuals possess the unprecedented ability to exchange information instantaneously and across vast distances, transcending traditional boundaries. Yet, the preservation of personal privacy within this expansive network depends heavily on the skill

and intent of those who seek to protect or violate it. Within the realm of cyberspace, the right to privacy is inseparable from the ethical responsibility to honour the privacy of others. This digital domain offers unique opportunities for human connection—linking individuals who might otherwise remain strangers—thereby expanding the social fabric. However, the phenomenon of hacking exemplifies a profound ethical challenge, where technical expertise is sometimes wielded not as a means of constructive knowledge but as an instrument of exploitation and harm. Such misuse constitutes a grave moral failing, for possessing knowledge does not grant license to violate the dignity or rights of others. The impersonal nature of the cyber environment risks eroding empathy, mutual respect, and recognition of intrinsic human worth, exposing a critical need for an ethics rooted in the care and respect of "the other," akin to ethical neighborliness in the tangible world. Whether communicating through emails or social media platforms—be it between spouses, educators and students, friends, colleagues, or leaders and subordinates—one must cultivate a disposition of respect, civility, and attentiveness to the dignity and privacy of others. Ethical behaviour in digital interaction demands a conscious recognition of responsibility, restraint, and the interconnectedness that binds individuals across virtual spaces. While physical interactions are often regulated by social norms and shared visibility, the anonymity and confidentiality inherent in cyberspace may weaken these moral constraints. Therefore, individuals must exercise heightened vigilance and unwavering ethical integrity, whether acting publicly or in the solitude of their digital engagements with family, friends, or colleagues, thus sustaining the fabric of trust and respect fundamental to a secure and humane cyber society.

Those who violate the sanctity of privacy, security, and intellectual property within cyberspace fundamentally breach ethical norms. Acts such as hacking, spamming, extortion, and the dissemination of unsolicited communications demand rigorous moral scrutiny and robust regulatory frameworks to uphold order in the virtual realm. The profound disruptive impact of information and communication technologies compels a renewed philosophical inquiry into the nature of "right" and "wrong." While children can often discern moral distinctions clearly in the physical world, the complexity and novelty of digital environments obscure these judgments, complicating ethical evaluation. Emerging technologies necessitate not only the reinterpretation of enduring moral principles but also the formulation of novel ethical codes to address unprecedented actions—such as the mass distribution of unsolicited commercial messages or the manipulation and unchecked dissemination of digital pornography, phenomena impossible before the advent of the internet. Moreover, the virtual realm challenges traditional

safeguards, as minors face far fewer barriers to accessing inappropriate content than before. This situation calls for conscientious efforts from educators, guardians, and institutions to establish protective boundaries without infringing upon the freedom and potential of digital engagement. A critical reason cyber ethics warrants focused attention lies in the human tendency to diminish the moral gravity of actions performed in the intangible digital sphere compared to those in the physical world. Few would consider physically stealing software from a store, yet many underestimate the ethical implications of digital theft or misconduct online. Hence, educators bear the vital responsibility to cultivate students' capacity for ethical discernment, encouraging them to construct well-reasoned value judgments, engage with opposing perspectives, and refine their moral reasoning. Given that many students' ethical reflections remain superficial—often limited to unchallenged assertions—educators must design intentional learning experiences that deepen conceptual understanding and foster critical engagement with technology's ethical dimensions. In doing so, the educational enterprise contributes not only to knowledge acquisition but also to the moral formation necessary for responsible digital citizenship.

Media plays a vital role in ethical dilemmas; movies as well as books and television programs, often make questionable ethical actions such as breaking into the secure computer system seen as heroic on at least sympathetic. As these actions are not questioned ethically but approached as an outcome of intelligence. So, the use of information technologies spreads throughout society and its importance to our national economy and individual concern, everyone will need to make good ethical decisions when using computers. That's why cyberethics is very important in our cyberspace.

In today's event, with concerns of security, eavesdropping, hacking, and so on, whereby no government is in charge of the internet, an international body has to rely on the accord. This organization ought to work on the digital moral code or rules of conduct that would arguably be suitable for regulating people groups' behaviour on the internet. Some matters where cyber ethics can contribute significantly to -

- Fraud and deception represent morally corrosive practices arising from the direct or indirect exploitation of personal information. As the misuse of data becomes increasingly prevalent, the erosion of individual privacy, anonymity, and autonomy deepens. In this context, ethical business conduct is not merely a matter of compliance but a moral imperative—one that safeguards the dignity and trust of individuals by protecting the confidentiality of their personal

data. Upholding such values reflects a deeper commitment to justice, responsibility, and respect for the person in the digital age.

- The digital sphere has given rise to a multitude of ethically irresponsible behaviours, ranging from the exploitation of individuals' financial vulnerability to the propagation of hate speech and discriminatory expressions based on gender, race, culture, and other morally sensitive dimensions. The internet, while enabling unprecedented freedom of expression and interaction, also becomes a space where ethical boundaries are frequently blurred or transgressed. This calls for deeper moral reflection on the nature of respect, human dignity, and the responsible exercise of freedom in virtual environments.
- While technology enables unprecedented access and distribution, much of the shared content includes copyrighted material, particularly music, the unauthorized transfer of which raises serious legal and ethical concerns. Whether the act of sharing such protected media is morally justifiable remains an open and complex question, inviting deeper reflection on ownership, intellectual property, and the ethical use of digital freedom.
- Issues of accessibility, surveillance, and control present complex ethical dilemmas that lie at the heart of cyber ethics. These concerns give rise to ongoing questions that challenge our understanding of privacy, security, and our place within the digital public sphere. In pursuit of protection and order, societies have developed tools of monitoring and regulation—yet these same instruments often manifest as forms of censorship and digital segregation, restricting access to information and shaping the flow of knowledge. Such practices call for a critical moral examination of the balance between collective security and individual freedom in the age of information.

  In the cyber world, such journals assume no responsibilities, because they claim they do not publish anything independently; they publish links, which are followed if readers are interested in the material. This seems straightforward enough, but what if a site that is not very popular or a personal weblog publishes a scandalous piece of news which is not true. The news is read hundred of thousand of times because of the link and produces a huge impact. The source site has to pull out the news, but this is not evidenced in the link dump or does not earn points to visit there, so the retraction is pointless.

  Even way back, pre-internet, technology's influence on social interaction was something that had been under extended study (Russel 1931; Kierkegaard 1967). Indeed, the development and entrenchment of online social networks have further heightened the prescience of his research and reinforced the necessity to complete it. For Bertrand Russel (1931), the assimilation of new

technology equates with the shift from contemplation of nature to its manipulation. Kierkegaard (1967) extends the argument, postulating that technology changes not only the nature of immediate, human relationships but also deposits traces—masks—behind which people hide from each other. It is fear, in the opinion of Kierkegaard, which eventually encourages humans towards certain technologies that give humans the opportunity to avoid or hide from those areas of human relations they dread the most.

Kierkegaard (1967), Dreyfus (1999), and Szalvitz (1999) also stress that the new communication technology can work to conceal or sustain some anonymous features of the being (which would also reinforce the ethical imperative in the important world). But we believe this dissimulation effect must only be collateral, and hide nothing from the importance to be afforded to the other kind of consequences, which affect business social networking is judged to be much more pertinent, for the creation and emancipation of virtual communities, appearing to be full of vitality. However, from a moral perspective, it is considered relevant to note the thinking of the cited authors since the very nature of the virtual world as intangible could promote a gaze of seriousness and soften the feeling of responsibility and genuineness essential to the shaping of a healthy and transparent social & economic structure

The true driving force behind any technological advance is economic convenience, not an esoteric psychological determinism founded on Fear of humanization. We hold that the deficiency of trust, implanted in the social fabric while working with new technology, results from the as yet primitive level of relationship experienced in the essential world, where interactivity has not arrived at the realism attained in face-to-face relationships. This counsel is to carry out an ethical consideration and take steps that enable the minimization of uncertainty and insecurity among the users and enhance faith in business practices on social networking.

The most widely adopted online applications are likely to be those that effectively serve large virtual communities by offering practical utility, ease of access, and user-friendly design. However, this broad participation significantly amplifies the ethical responsibility surrounding their use. Such platforms must be governed by guiding principles and regulations that uphold fairness—ensuring equal access to information, clearly defined user privileges, and the protection of individual privacy preferences. Furthermore, these systems should empower users to verify the accuracy of shared content, promoting transparency and accountability. Equally important is the safeguarding of intellectual property, preventing misuse or unauthorized

appropriation within the digital community. In essence, ethical frameworks must evolve alongside these technologies to support equity, integrity, and trust in virtual environments.

conversely, the liability of software masterminds for the safety and trustworthiness of their work was an issue only while designing critical control systems for sensitive industrial, military, profitable, or medical environments. Now, the proliferation of ubiquitous computing with increasing independence is rendering the issue of software trustability and safety more stringent. Additionally, as debated, new types of ethical issues emerge regarding the impact of creating such types of artifacts in a range of environments. The issue is therefore how software geniuses should approach these ethical issues..

1. After identifying the ethical implications of a design, how can software engineers modify or shape the artifact to prevent these issues?
2. By what means can designers ascertain that the functions embodied in a technological artifact align with and fulfill the ethical principles it is intended to uphold?
3. In what ways can software engineers assess the ethical implications of the artifacts they create?

So that's why cyber ethics is very much important for our cyberspace.

A genuine evaluation of a person's ethical stranding is carried out through ethical reasoning that cannot be reduced to a conduct code. Ethics is a separate discipline, with its own conceptual toolkits and specialization. It does not appear probable that software engineers can readily or should even be made into ethicists. Yet, it is plausible to imagine an integrated team of engineers and ethicists collaborating towards a common purpose.
Interdisciplinary team ethicists would be in the best position to provide a solution to the problem of reaching the nature of the ethical effect generated by the artifact to be designed. The engineers, on the other hand, would also need to resolve the problem of determining how a design could be formalized and verified with such knowledge in mind.
The main philosophical research question based on this discussion is:

"How can moral principles and ethical frameworks be applied to guide human behaviour and decision-making within cyberspace to ensure responsible use of technology and safeguard societal values?"

<u>Relation between Cyber ethics and Human rights:-</u>

The relationship between cyber ethics and human rights is increasingly significant as technology evolves and intersects with social issues. Several studies shed light on how ethical

considerations in cyberspace impact individual rights and public interests, highlighting critical areas such as privacy, free speech, and the implications of information technology.

Cyber ethics embodies the moral framework that governs the conduct of individuals and institutions within the digital realm. It calls for the conscientious and principled application of technology, underscoring the importance of respecting privacy, eschewing illicit activities, fostering equity, and safeguarding security in virtual spaces. Human rights, by contrast, represent the intrinsic and inalienable freedoms and entitlements of every individual—such as the right to privacy, freedom of expression, equality, and access to knowledge—which transcend both the physical and digital spheres. At the intersection of these domains lies the imperative to honour the sanctity of personal privacy; cyber ethics insists upon the ethical stewardship of personal data, affirming the human right to privacy by resisting unauthorized surveillance or exploitation. While human rights enshrine freedom of expression as a cornerstone of human dignity, cyber ethics tempers this freedom by advocating for responsible speech that does not incite harm through hate, falsehood, or harassment. Furthermore, cyber ethics endeavors to forestall violations such as hacking, identity theft, and digital harassment—acts that infringe upon human rights by compromising individual security and dignity. In the vast expanse of cyberspace, where personal information is perpetually collected and disseminated, the ethical imperative is to protect this data from misuse, thereby upholding the right to privacy. The philosophical essence of human rights extends to ensuring equitable access to information and technological resources; cyber ethics responds by challenging digital exclusion and advocating for inclusivity of marginalized populations in the digital discourse. Ultimately, honouring human rights in the digital realm demands a shared moral responsibility—where individuals, corporations, and governments alike are held to account—so that justice is not merely an ideal, but a guiding force in confronting ethical failures.

In the absence of a human rights foundation, cyber ethics risks dissolving into relativism—its principles susceptible to the shifting tides of cultural norms, political ideologies, or corporate agendas. What one group deems "ethical" may, without a universal moral compass, justify the suppression of freedoms or the exploitation of the vulnerable. Detached from the universality of human rights, cyber ethics becomes a collection of soft, unenforceable norms—well-intentioned, but ultimately hollow**.** By contrast, when anchored in the enduring principles of human dignity, autonomy, and justice, cyber ethics gains coherence and moral force. Human rights infuse cyber ethics with a shared moral grammar, one that transcends borders and ideologies, offering a global vision of what it means to act responsibly and respectfully in the

digital realm. Moreover, human rights compel cyber ethics to confront its deepest ethical responsibility: the protection of the vulnerable. In a digital world where surveillance, exclusion, and exploitation disproportionately affect children, minorities, and the marginalized, cyber ethics must be more than technical fairness or corporate compliance—it must be an expression of moral solidarity. To be truly ethical, cyber behaviour must echo the fundamental truth that every human being, even in virtual space, possesses inviolable worth.

Cyber ethics gains force and legitimacy when backed by enforceable human rights law. Human rights provide a shared ethical language across nations. This allows cyber ethics to be coherent and consistent across borders, rather than fragmented by local interests or ideologies. A human rights-based cyber ethic demands that we design and govern technology with compassion, fairness, and justice at its core. Human rights are grounded in the idea that every person possesses inherent dignity, regardless of nationality, culture, or circumstance. Cyber ethics, which deals with behaviour in the digital realm, must be guided by these universal standards to avoid becoming culturally biased or morally inconsistent.

So, finally, we can say that:

Cyber ethics offers a structure for guiding behaviour in the digital sphere, but it is human rights that give it moral substance and direction. While ethics shapes conduct, human rights articulate the deeper, non-negotiable values—freedom, dignity, justice—that must be preserved amidst technological advancement. Together, they serve not merely to regulate cyberspace but to humanize it. Human rights are not peripheral to cyber ethics; they are its ethical foundation. They ensure that the pursuit of digital innovation does not eclipse our responsibility to protect the individual, affirm their worth, and hold the powerful to account. Cyber ethics divorced from human rights is like an instrument unmoored from its tuning—present, but dissonant and uncertain. It is the human rights framework that anchors cyber ethics, acting as a moral compass that prevents our digital evolution from becoming ethically adrift. In a world where technology holds the power to both liberate and dominate, only human rights can keep our ethical compass aligned with the intrinsic values of our shared humanity.

So, based on this entire discussion, the fundamental research question will arise:

How can ethical principles grounded in human rights be effectively integrated into the design, governance, and behavior within cyberspace to promote responsible and equitable digital interactions?

Conclusion

In the unfolding landscape of the digital age, cyber ethics emerges not merely as a set of guidelines, but as a philosophical imperative—an anchor for moral reasoning in an increasingly virtual world. It calls for the infusion of ethical consciousness into the very fabric of technological development and use, demanding that human dignity, privacy, justice, and transparency be upheld as sacred principles. The pursuit of a just digital order is not the responsibility of one actor alone, but a collective moral endeavor—uniting individuals, corporations, and governments in the shared task of cultivating digital virtue. In this light, ethical engagement with technology becomes more than a choice; it is a moral vocation. It is through such deliberate and principled action that we safeguard the soul of our digital society, ensuring that technological progress remains a servant to humanity rather than its master. As the digital realm grows ever more complex, so too must our commitment to moral clarity, lest we lose ourselves in the machinery we create.

References

1. Bailey, D. (2008). *Cyber Ethics*. The Rosen Publishing Group, Inc.
2. Blackburn, A., Chen, I. L., & Pfeffer, R. (Eds.). (2018). Emerging trends in cyber ethics and education.
3. Denning, D. E. (2008). The ethics of cyber conflict. *The handbook of information and computer ethics*, 407-428.
4. Dudley, A., Braman, J., & Vincenti, G. (Eds.). (2011). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: Issues, Impacts and Practices*. IGI Global.
5. Liaropoulos, A. N. (2016). Reconceptualising cyber security: Safeguarding human rights in the era of cyber surveillance. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *6*(2), 32-40.
6. Mihr, A. (2017). *Cyber justice: Human rights and good governance for the internet*. Cham, Switzerland: Springer.
7. Sarikakis, K., Korbiel, I., & Piassaroli Mantovaneli, W. (2018). Social control and the institutionalization of human rights as an ethical framework for media and ICT corporations. *Journal of Information, Communication and Ethics in Society*, *16*(3), 275-289.
8. Shackelford, S. J. (2021). Should cybersecurity be a human right?*: Exploring the "shared responsibility" of cyber peace. In *Music, Business and Peacebuilding* (pp. 174-197). Routledge.
9. Spinello, R. A. (2010). *Cyberethics: Morality and Law in Cyberspace*. Jones & Bartlett Publishers.
10. Spinello, R. A. (2010). *Cyberethics: Morality and Law in Cyberspace*. Jones & Bartlett Publishers.
11. Yaokumah, W. (2020). Predicting and explaining cyber ethics with ethical theories. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *10*(2), 46-63.