# MULTIDISZCIPLINÁRIS KIHÍVÁSOK
# SOKSZÍNŰ VÁLASZOK

GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT

# MULTIDISCIPLINARY CHALLENGES
# DIVERSE RESPONSES

JOURNAL OF MANAGEMENT
AND BUSINESS ADMINISTRATION

18 57 BGE

2023/2.

**Online folyóirat**

Főszerkesztő: Fenyvesi Éva, PhD

Szerkesztette: Vágány Judit Bernadett, PhD

Borító: FLOW PR

Kiadja: Budapesti Gazdasági Egyetem

Felelős kiadó: Prof. Dr. Heidrich Balázs, rektor

ISSN 2630-886X

2023.

# TOWARDS A SAFE AND SECURE GLOBAL INFORMATION TECHNOLOGY ECOSYSTEM: THE IMPORTANCE OF ETHICAL APPROACHES AND INTERNATIONAL COOPERATION IN ADDRESSING PERSISTENT CHALLENGES

# A BIZTONSÁGOS ÉS VÉDETT GLOBÁLIS INFORMATIKAI ÖKOSZISZTÉMA FELÉ: AZ ETIKAI MEGKÖZELÍTÉSEK ÉS A NEMZETKÖZI EGYÜTTMŰKÖDÉS FONTOSSÁGA A TARTÓS KIHÍVÁSOK KEZELÉSÉBEN

**TOKAT Yasin**

**Keywords:** *Cyberspace, Privacy and Security Challenges, Cybersecurity Ethics, Ethical Leadership, International Cooperation in Cyberspace*
**Kulcsszavak:** *Kibertér, Magánélet és Biztonsági Kihívások, Kibervédelem Etikája, Etikus Vezetés, Nemzetközi Együttműködés a Kibertérben*

**JEL kód:** L86, F51, O33, K42

https://doi.org/10.33565/MKSV.2023.02.09

**ABSTRACT**

*Cyberspace, an expanding and boundless platform created by a vast network of interconnected devices, has caused a fundamental change in communication, work, and information accessibility. The unprecedented potential of this platform, however, also poses major challenges in terms of privacy and security. Due to its multinational nature, cyberspace transcends the sovereignty of any one government and therefore evades exclusive ownership by a nation-state. Although the growth of digitalization has simplified many processes and increased productivity in daily life, this exponential growth has rendered the digital ecosystem more vulnerable to a wide range of cybersecurity threats. The increasing frequency and sophistication of cyberattacks and operations carried out by both state and non-state actors highlight the need for better international cooperation to help protect critical infrastructure from malicious actors. Collective action in response to global cyber threats requires consistency and adherence to ethical principles within the international community. Ethical approaches to leadership and international cooperation can play an important part in resolving global cybersecurity issues by paving the way for the development and adoption of better and more effective cybersecurity policies that can help mitigate the risk more optimally. The purpose of this study is to evaluate the possibilities of bolstering global solidarity via the use of ethical methods to combat the challenges posed by digital technology. The intricate and interconnected nature of cyber issues underscores the cruciality of ethical governance in the identification and implementation of practical solutions. The present study seeks to examine and assess the practicality, applicability, and efficiency of various ethical frameworks in addressing issues pertaining to digital platforms, thereby contributing to a better understanding of the interplay between ethics and cybersecurity. This study would contribute to the development of strategies for inspiring ethical and responsible behavior from public and private sectors regarding cybersecurity, and to the promotion of international solidarity and cooperation in addressing global cyber threats.*

**ABSZTRAKT**

*A kibertér, az összekapcsolt eszközök hatalmas hálózata által létrehozott, egyre bővülő és határtalan platform alapvető változást okozott a kommunikációban, a munkában és az*

*információk elérhetőségében. E platform soha nem látott lehetőségei azonban komoly kihívásokat is jelentenek a magánélet és a biztonság szempontjából. A kibertér multinacionális jellegéből adódóan túllép bármely kormány szuverenitásán, és ezért elkerülhetővé teszi a nemzetállamok kizárólagos tulajdonjogát. Bár a digitalizáció növekedése számos folyamatot egyszerűsített és növelte a termelékenységet a mindennapi életben, ez az exponenciális növekedés a digitális ökoszisztémát a kiberbiztonsági fenyegetések széles körével szemben sebezhetőbbé tette. Az állami és nem állami szereplők által végrehajtott kibertámadások és műveletek növekvő gyakorisága és kifinomultsága rávilágít arra, hogy a kritikus infrastruktúrák rosszindulatú szereplőkkel szembeni védelme érdekében jobb nemzetközi együttműködésre van szükség. A globális kiberfenyegetésekre adott kollektív fellépés a nemzetközi közösségen belül következetességet és az etikai elvek betartását igényli. A vezetés és a nemzetközi együttműködés etikai megközelítései fontos szerepet játszhatnak a globális kiberbiztonsági problémák megoldásában, mivel előkészítik az utat a jobb és hatékonyabb kiberbiztonsági politikák kidolgozásához és elfogadásához, amelyek hozzájárulhatnak a kockázatok optimálisabb csökkentéséhez. E tanulmány célja, hogy értékelje a globális szolidaritás megerősítésének lehetőségeit a digitális technológia által támasztott kihívások leküzdésére szolgáló etikai módszerek alkalmazásával. A kiberproblémák bonyolult és összekapcsolódó jellege kiemeli az etikus kormányzás döntő fontosságát a gyakorlati megoldások meghatározásában és végrehajtásában. Jelen tanulmány célja, hogy megvizsgálja és értékelje a különböző etikai keretek gyakorlatiasságát, alkalmazhatóságát és hatékonyságát a digitális platformokkal kapcsolatos kérdések kezelésében, és ezáltal hozzájáruljon az etika és a kiberbiztonság közötti kölcsönhatás jobb megértéséhez. Ez a tanulmány hozzájárulna olyan stratégiák kidolgozásához, amelyek a kiberbiztonsággal kapcsolatos etikus és felelős magatartásra ösztönzik a köz- és a magánszektort, valamint a nemzetközi szolidaritás és együttműködés előmozdításához a globális kiberfenyegetések kezelésében.*

## INTRODUCTION

The internet has become a vital medium for the dissemination of information, the conduct of business, and the facilitation of communication as a result of technological progress. However, as people become more reliant on digital resources, cybersecurity has emerged as a major issue. Cybersecurity challenges range from personal social media accounts with personal information to some of the most critical national security issues of the information age. In the face of these challenging situations, a unique and adaptable leadership approach, coupled with a clearly defined code of ethics and principles, becomes imperative to assure the security of information communication technologies. Adopting an ethical approach aid in upholding cyber hygiene and maintaining vigilance towards emerging issues, thus mitigating potential consequences. These essential components are vital for effectively addressing and mitigating serious cybersecurity threats. It is also crucial to remember that, as increasingly more people get connected to networks with various devices, cybersecurity has become less about technology and more about people, their behaviors, and their habits. Hence, besides the technical knowledge, skills, and expertise, there is a growing need for a human-centered focus on cybersecurity and leadership. Given that users and individuals serve as both sources of vulnerabilities and defenders, the adoption of ethical approaches holds promise for enhancing cybersecurity by binding security to norms, values, and principles. Moreover, the implementation of an ethical approach needs the right leadership and organizational culture. By cultivating a culture rooted in trust and accountability, organizations can effectively nurture a heightened sense of responsibility among employees, encouraging them to protect sensitive information and effectively counter cyber threats. As a result, organizations can provide a more safe and sturdy digital infrastructure.

Ethical approaches play a vital role in international cybersecurity, directly influencing the achievement of two paramount goals: safeguarding individuals

and institutions against cyber threats and cultivating a secure digital environment. Cybersecurity is an ever-evolving sector that calls for both technological know-how and a human-centered approach to leadership and governance. The paradigm of ethical leadership places a priority on ethical decision-making and places emphasis on the welfare of individuals as well as society as a whole. It is essential that leaders concentrate on user behavior and the ethical aspects of security decisions considering the prevalence of network-connected devices and the growing significance of personal and sensitive information available on the internet. Abuse of power, such as the sale of personal information and data to third parties, can emerge from ethical failures, highlighting the importance of upholding ethical standards in the digital ecosystem. Otherwise, if ethical elements are missing, the borderless, anonymous internet, with its great revenue opportunities, might tempt both senior executives and state officials to act for self-benefit while abusing the positions they have within an organization. The emergence of recent scandals involving the illicit sale of user data, the propagation of false news, the manipulation of information, and increasing cyber frauds underscores the inadequacy of relying solely on technical proficiency within the domain of cybersecurity. Cyberspace constitutes a highly dynamic environment characterized by the continual evolution of devices, users, technologies, and networks. Furthermore, there is a need for collaboration among technical experts and non-technical stakeholders in order to effectively address the complexities of cybersecurity challenges. Morals, principles, and values serve as powerful unifying forces, enabling the effective convergence of diverging interests and viewpoints among all those diverging stakeholders and the public at large.

In the realm of cybersecurity, safeguarding information requires a constant commitment to adaptability and innovation, ensuring the capacity for responding to emerging and evolving security events effectively. The extensive degree of innovation, adaptability, and tolerance for change inherent in the realm of cybersecurity necessitates the establishment of a foundational framework rooted

in organizational culture. Ultimately, ethical leadership assumes a central role in cultivating a culture characterized by creativity, trust, and awareness, thus enabling the cultivation of innovation and adaptation. Since innovative concepts emerge and develop in environments that are reliable and safe, ethics and values are essential to ensure the innovative culture is upheld without compromising the rights, freedoms, and security needs. An organization that consistently upholds a well-defined code of ethics and principles plays a pivotal role in facilitating the achievement of desired outcomes and guiding others in their pursuit of goals.

Ethical behavior as an organizational culture, whether in the private or public sector, can establish a benchmark for moral conduct with a sense of personal and public commitment to benevolence and transparency. Such commitment can also play an important part in the process of establishing the guiding principles and values that the members of the organization are expected to adhere to, contributing to the development of a culture of trust and integrity within the establishment. Furthermore, ethical leaders can help shield their organizations from the financial and reputational damage that might result from non-compliance. As the dynamic digital world necessitates the presence of leadership characterized by qualities of creativity and flexibility, ethical approaches ought to be present for the cultivation of a culture that fosters innovation, trust, and awareness to keep up with the rapid pace of the IT sector. By maintaining constant adaptive and innovative aspects, organizations can cultivate a more favorable cybersecurity stance and facilitate enhanced international collaboration within the cyberspace domain. In this respect, ethical leadership is not limited to simply adhering to a set of ethics; rather, it is about understanding the needs and motivations of individuals and assisting them in their aspirations.

Failures to uphold ethical standards in the technology industry can have far-reaching repercussions, both financially and socially. The long-term effects of a tarnished reputation can be far more detrimental to a company's fortunes than the immediate financial repercussions. Additionally, ethical managers have an

important function in establishing a model of virtue for others to follow. Due to the complexity and sensitivity of cybersecurity, it is of the uttermost importance that individuals entrusted with technology development and policymaking adhere to the highest ethical standards. When cybersecurity issues are present, ethical leadership is also necessary for the preservation of people's fundamental rights. Respect for privacy, protection from online harm, and the prevention of children's exposure to inappropriate content are all components of this initiative. Given the importance of ethical leadership in the field of international cyber security, this study aims to look at the viability of ethical approaches in addressing issues of mistrust and rising tensions between nation-states in cyberspace. The purpose of the study is to investigate the impact of ethical leadership on organizations and its role in promoting a safe and secure digital environment for its users. The study will examine the connection between ethical leadership and the development of a culture of trust and integrity within organizations. The impact of ethics and values on organizational innovation and adaptability in the face of an ever-changing and dynamic business environment will be investigated. In addition, the research will examine the extent to which ethical approaches can limit potential security vulnerabilities and their capacity to mitigate the risks in cyberspace.

## LITERATURE REVIEW

In recent years, the growing significance of ethical leadership in the domain of cybersecurity has garnered considerable attention, yet the literature on this subject remains scant. Despite this, a number of researchers have contributed to the growth of a deeper knowledge of the role of ethics in the digital world. The objective of this literature review is to explore the contributions that these researchers have made and to expand knowledge concerning ethical approaches within the cybersecurity domain.

First, Marisa Cleveland and Tonia Spangler published their article "Toward a Model for Ethical Cybersecurity Leadership" in IGI Global's "Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications" (Cleveland & Spangler, 2020). They discuss the urgent need for ethical leadership in cybersecurity in their paper. They state that the absence of regulations and established norms in cyberspace led to problematic situations. They emphasize the challenges posed by technological advancements and the Internet of Things, which have rendered traditional security approaches obsolete, and the resulting need for ethical leadership in the field. In response to the paucity of literature on identifying a set of global ethical standards for cybersecurity executives, the authors present a global model of ethical standards and three ethical propositions. The ethical standards and propositions are to ensure that technology consumers in today's global business environment maintain trust in the organizations with which they have entrusted their data.

The essay "The Ethics of Cybersecurity" by Markus Christen, Bert Gordijn, and Michele Loi (Christen et al., 2020) explores the ethical issues and dilemmas associated with cybersecurity. The authors claim that it is necessary to protect fundamental values such as equality, justice, freedom, and privacy in the realm of cybersecurity. They underline the important role that values and ethics play in sustaining trust and confidence in digital infrastructure. The writers present insightful explanations regarding the significance of ethics in the realm of cybersecurity and provide concrete examples of ways to manage ethical conundrums in the IT industry. When seen from this angle, the cases, and analyses that they present addressing the significance of ethics in the cybersecurity industry are highly relevant.

"A Principlist Framework for Cybersecurity Ethics," a publication by Paul Formosa, Michael Wilson, and Deborah Richards from Macquarie University, came out in 2021 (Formosa et al. 2021). Their work highlights how an ethical framework is preferable for more comprehensive cyber capacity building. They

propose a set of ethical frameworks for cybersecurity that are founded on ethics, bioethics, and artificial intelligence ethics in an effort to address the preexisting problems and weaknesses within the digital ecosystem. In the AI4People framework, they devised a domain-specific specification of five ethical principles in cybersecurity: beneficence, nonmaleficence, autonomy, fairness, and explicability. They illustrate the advantages of this framework by addressing the ethical challenges in certain cyber-related areas. These include pen testing, distributed denial-of-service (DDoS) attacks, ransomware, and system administration. Their study exemplifies the efficacy of this framework as a fundamental basis for comprehending the ethics of cyberspace while also fostering ethical competence and cultivating sensitivity among cybersecurity professionals and other pertinent stakeholders.

In a 2019 article, "Ethics and cybersecurity are not mutually exclusive," published in the EDP Audit, Control, and Security Newsletter, the authors Dan Shoemaker, Anne Kohnke, and Greg Laidlaw examine ethics and cybersecurity issues from the perspective of an organization (Shoemaker et al., 2019). Their paper explains why ethics are always a lower priority when it comes to organizational cybersecurity and why this situation is fundamentally problematic. They contrast this issue with the fundamental prerequisites of cybersecurity. The degree of sincerity with which an organization commits to maintaining the confidentiality, integrity, and accessibility of its data is determined by its understanding of ethical obligations, as demonstrated by its actions. As a consequence of this, ethics form the basis of everything that is tied to cybersecurity in a number of different ways. They highlight the need for defining ethical concepts to emerging technology trends. Based on their findings, they conclude that the CSEC 2017 model is useful for learning more about the model's proposed ethical elements for cybersecurity and how they relate to the development of practical measures.

The article "Cybersecurity Description and Control Criteria to Strengthen Corporate Governance," which was written by Hugh Grove, Mac Clouse, and

Laura Georg Schaffner and published in 2019, focuses on the recent cyberattacks and highlights the dangers of failing to adequately address cybersecurity vulnerabilities (Grove et al., 2019). This paper emphasizes the pivotal role corporate executives and boards of directors play in safeguarding and advancing the interests of a company's stakeholders. It highlights the imperative of implementing effective governance practices to ensure cyber hygiene. They suggest that leaders and boards of directors, equipped with information from authoritative sources such as the AICPA Cybersecurity Guide, can construct cybersecurity plans to mitigate such issues.

"The Role of Governments, Businesses, and Individuals," by Arben Asllani, Charles Stephen White, and Lawrence Ettkin, was published in the Journal of Legal, Ethical, and Regulatory Studies in 2013 (Asllani et al., 2013). Their article investigates the government's involvement in developing an acceptable legal, social, and ethical framework to improve cybersecurity posture. Preceding cybersecurity doctrines are briefly examined, and the concept of cybersecurity as a public benefit is investigated. In order to defend the security of national, federal, and local governments, organizations, and individuals must implement good cybersecurity controls. The study finishes with a set of examples highlighting the government's role in boosting cybersecurity and decreasing cyber insecurity.

A 2017 publication by Mary Manjikian titled "Cybersecurity Ethics: An Introduction" provides a basic introduction to the subject of cybersecurity ethics (Manjikian, 2017). The book consists of three sections. Part one introduces the fields of ethics and philosophy of science, as well as three ethical frameworks — virtue ethics, utilitarian ethics, and communitarian ethics — and the concept of ethical hacking. The second section applies these frameworks to specific cybersecurity issues, such as privacy rights, intellectual property, surveillance, and cyber ethics in military affairs. The third section concludes with an examination of current codes of ethics in cybersecurity. The overarching goals of the book are to provide ethical frameworks that can be used to make better decisions, to

introduce the most pressing ethical concerns related to computer security, and to draw attention to the relationship between personal values and professional ethics. The paper also includes three additional features such as "Going Deeper" which provides background information on key individuals and concepts; "Critical Issues" which presents contemporary case studies; and "Applications" which investigates specific technologies or practices that raise ethical concerns.

## METHODOLOGY

This study delves into the impact of ethical approaches on cybersecurity posture, examining the organizational, leadership, decision-making, and behavioral aspects within the digital sector and cyberspace. It aims to illuminate the part ethics can have in the digital domain by investigating diverse cyber threats and demonstrating how ethical approaches can effectively address and mitigate them. Thus, this analysis attempts to elucidate the profound influence wielded by ethical leadership and decision-making patterns on the behaviors of both public and private actors in the realm of cyberspace. Accordingly, the research aims to shed light on the consequential outcomes that ensue from such ethical approaches, thereby contributing to the scholarly discourse on the subject matter. Given the aforementioned context, the analysis employed a qualitative technique as a methodological approach. The adoption of a qualitative approach facilitates a comprehensive examination of real-world incidents, characterized by the absence of ethical governance, thereby resulting in compromised cybersecurity measures and the erosion of trust at a considerable magnitude. This method sheds light on the crucial role of ethical methods and values in reducing cybersecurity risks and offers significant insights into the complex elements that contribute to failures in this area. Real-world case studies, which provide situations that are both pertinent and concrete, have been added to the research. Through the incorporation of qualitative analysis and pertinent case studies, this research attempts to illustrate the vital implication of values and ethics in nurturing a culture of heightened

cybersecurity awareness and encouraging adherence to relevant laws and regulations. Ultimately, it is crucial to embrace thorough and holistic strategies for cybersecurity that surpass the limitations set by purely technical capabilities. By doing so, organizations can effectively address the multifaceted challenges of cybersecurity by integrating more expansive perspectives that encompass social, ethical, and regulatory dimensions. Using this method, the study demonstrates the importance of addressing cybersecurity from both a technical and psychological perspective. In doing so, it aims to contribute to the ongoing discussion regarding the complex interplay between technical proficiency and human factors, highlighting the importance of addressing both factors in the pursuit of robust cybersecurity measures.

## ETHICAL APPROACHES TO CYBERSECURITY

### Various Types of Ethical Approaches that Can Be Implemented in Cybersecurity

The growing reliance on technology and the internet has led to a proportional rise in the number of cyberattacks, which has necessitated the deployment of new preventative defensive measures. It is becoming increasingly important to govern and oversee the implementation of cybersecurity methods with ethical considerations as a result of the proven effectiveness of these methods in protecting sensitive data. When it comes to ensuring that cybersecurity practices are not just successful but also ethical, organizations and individuals alike have access to a variety of distinct ethical methods from which they can make their selections. Some of the most common approaches for tackling various issues are illustrated below.

When it comes to cyber security, the utilitarian approach can be implemented to maximize the overall benefits for all involved stakeholders. This strategy is based on utilitarian ideas, which put an emphasis on providing the greatest possible benefit to the largest possible number of people (Asllani et al., 2013). Efforts

made in the realm of cybersecurity should result in the greatest possible good for everyone concerned. In practice, this implies that organizations and individuals must place the highest priority on protecting sensitive information than anything else. Organizations ought to ensure that their approach to cybersecurity is ethical, effective, and beneficial to the greatest number of individuals by placing a premium on the security of sensitive data and routinely reviewing and updating their policies and practices. For instance, businesses may establish strict security controls to employ effective encryption mechanisms to protect sensitive data such as personal information and financial records. By making this practice a core organizational value, the company not only assures the security of its own database but also provides its employees and customers with peace of mind that their information safety is prioritized above else. In addition, the utilitarian approach requires organizations to continually evaluate their policies and practices in light of new advancements in cybersecurity. For instance, as technology evolves, businesses must assess whether their encryption methods are still relevant and effective. Otherwise, necessary adjustments can be made to continue to serve the greatest number of people.

Deontology is a second ethical approach that emphasizes the significance of adhering to ethical principles and duties. This strategy is based on deontological principles, which assert that individuals and organizations have certain moral obligations and responsibilities to pursue correct actions established by rules (Christer et al., 2020). In the field of cybersecurity, these responsibilities entail adhering to established security protocols and standards protecting sensitive data. The deontological approach promotes a culture of trust, respect, and honesty. By adhering to ethical rules and responsibilities on a consistent basis, organizations can earn the confidence of stakeholders, who are confident that their data is secure. When individuals have faith that their private data will be safeguarded, they are more likely to build trust with organizations and institutions. Importantly, the deontological approach requires the consistent application of ethical rules and

duties. If these obligations are not fulfilled, stakeholders may be less inclined to entrust the organization with their sensitive information. Ultimately, if organizations fail to consistently uphold cybersecurity regulations, even the public's trust in the government's ability to protect their data can be eroded, leading to a loss of faith in the capacity of the state to safeguard security and fundamental rights.

The virtue ethics perspective on cybersecurity emphasizes the importance of creating conditions where good ethical judgment becomes the embodiment of the behavior of cybersecurity professionals. This means that instead of relying solely on rules and regulations, individuals must cultivate a moral character that guides their actions and decisions in the field. (Manjikian, 2017). Originally, this viewpoint derives from the notion that morally sound personality attributes such as honesty, integrity, and responsibility are required for making moral decisions. When compared to a deontological framework, which focuses primarily on duty fulfillment, the virtue ethics approach emphasizes, to a higher degree, the development of one's character and the cultivation of positive attributes. Within the digital ecosystem, it becomes imperative for individuals to cultivate virtuous traits to uphold ethical cybersecurity practices. In this regard, the virtue ethics approach underscores the paramount importance of fostering a workplace culture that actively promotes and rewards ethical conduct while nurturing positive attributes. To achieve this objective, the virtue ethics approach accentuates the criticality of cultivating a workplace culture that proactively encourages and incentivizes ethical behavior while fostering positive character traits. A company may have an open attitude regarding the reporting of cybersecurity incidents, which can encourage transparency and accountability. This type of policy can foster a culture of honesty and integrity, which are essential for the security of cyberspace globally. In addition to the promotion of positive character traits, the virtue ethics approach acknowledges the significance of continuous learning in developing positive outcomes. In the context of mounting cybersecurity

challenges, individuals are compelled to enhance their understanding of events and cultivate ethics to make better decisions. By recognizing the imperative nature of continuous improvement, individuals are better equipped to navigate and respond to the evolving landscape of cybersecurity.

Care ethics is another approach in which the importance of compassion and caring in decision-making are emphasized and centralized. This concept implies that while making decisions on digital platforms, the care for the welfare and security of individuals should take precedence over other considerations such as financial gain or other benefits (Collins, 2015). The care ethics perspective on cybersecurity would stress the importance of companies accepting responsibility for their activities and considering the safety and security of others before operating (Morgan & Gordijn, 2020). This would include not just having transparent policies and procedures for how to respond to security issues but also addressing them with responsibility and determination. To illustrate this point, a social media company can be imagined. If the company incorporated care ethics into its operational aspects and procedures, it would prioritize consumer privacy over the potential financial gains derived from the selling of its user data to third parties without any consideration. This reflection in itself illustrates the concern for the security of others and a willingness to prioritize that above financial interests even if there are no laws present such as GDPR. The approach of care ethics recognizes the significance of cultivating relationships and constructing trust, in addition to putting an emphasis on the well-being of stakeholders and customers. In the realm of cybersecurity, it is crucial for organizations to prioritize openness and foster a culture of open communication. Such an emphasis ensures that individuals feel a sense of security and confidence when engaging with these organizations.

In conclusion, businesses and individuals can adopt a variety of ethical approaches to ensure that their cybersecurity practices are both effective and ethical. These methods can be found in a variety of settings. Despite the fact that each strategy

emphasizes a distinct set of values and principles, the ultimate goal of each can be to create a safe and secure cyberspace. To ensure that the internet remains a secure and safe space for all users, it is crucial that organizations and individuals think about the ethical implications of their cybersecurity operations and align those actions with a set of ethical principles. This will guarantee that the internet remains a valuable resource.

**Enhancing Ethical Leadership: Investigating the Causes of Ethical Deficiencies Among Leaders and Theories for Encouraging Ethical Conduct Within the Organizations**

The study of ethics spans millennia, but the characteristics of ethical leadership in the digital domain are an emerging subject. While leadership encompasses authority, power, and influence, they must conduct themselves according to some ethical principles. Ethical systems provide a set of ideas that can direct people in positions of power toward the correct ways of thinking and acting. Respect for value systems and principles, as well as the rights and dignity of others, characterize ethical leadership. Thus, it is associated with concepts such as trust, honesty, deliberation, charisma, and justice (Brown, Treviño, & Harrison, 2005). Ethical leaders are those whose actions serve as an example to their subordinates. The social learning theory and the social exchange theory are two different theoretical perspectives that can be taken when addressing ethical leadership. On the one hand, in social learning theory, ethical leaders serve as role models for their adherents. The followers carefully observe and subsequently embrace specific behavioral patterns that align with ethical concepts and judgments. A second layer of social learning can be developed through rewards and punishments from the leadership, reinforcing learning about acceptable and unacceptable behavior (Ko et al. 2017). On the other hand, in social exchange theory, ethical leadership is described in terms of transactional relationships between a leader and their follower. The fair treatment of the followers by the

leader and their sympathy for those followers initiate a process of reciprocation in which the followers react to the leader in a consistent manner (Ko et al. 2017). As a result, managers have the ability to effectively inspire people when they establish personal examples for their teams.

The organizational environment and culture also have a significant impact on encouraging and upholding ethical leadership (Kuenzi et al., 2020). Within a corrupt organizational culture, subordinates are more likely to imitate a leader's corrupt behavior than observe their own moral compass, if they want to remain and rise in their positions within that company. If leaders consistently attempt to bend and break the rules, they create a perpetually toxic environment that encourages followers to engage in unethical conduct. Even though ethical conduct is expected of leaders, they are especially susceptible to unethical conduct under certain circumstances for a variety of reasons. Power, authority, and influence may eliminate checks and balances in certain cases, allowing leaders to act unethically without the need to justify their actions. Undoubtedly, people frequently uphold a steadfast belief in their moral rectitude as conscientious agents in both societal and organizational contexts, justifying their steadfast commitment to ethical behavior regardless of their position within the organizational hierarchy. However, it is essential to acknowledge that one's ethical fallibilities can arise from a dearth of introspection regarding personal acts. Furthermore, in instances where leaders consistently garner accolades and acclaim for their exceptional leadership abilities, propelling organizational growth and value, there exists a propensity for them to succumb to the fallacious notion that they possess carte blanche to act with impunity, owing to the perceived infallibility of their actions and the positive outcomes of their previous undertakings both for their personal success and the organization's well-being. Due to such circumstances, it may be challenging for them to take a step back and give some reflection on the decision-making process. This overconfidence and lack of self-reflection frequently lead to compromises on the ethics part. Power, authority,

and a superior position in the social hierarchy make leaders especially susceptible to such conditions.

Moreover, "immediate entitlement bias" is an additional factor that may result in unethical conduct. It occurs when those in authoritative positions think they have a right to special treatment and use their position to benefit themselves, their families, and their social circles at the expense of those below them (Prentice, 2014). A person in a position of authority who possesses such a mindset is susceptible to entitlement bias. Dacher Keltner, a distinguished professor at the University of California, Berkeley, highlights that leaders, paradoxically, can display ethical myopia, exhibiting a self-serving mindset that rationalizes their immoral conduct, primarily prioritizing personal privileges while disregarding the nuanced considerations towards the concerns and interests of others (Keltner et al., 2006). Moreover, as individuals ascend the social hierarchy, the number of individuals to whom they must report decreases. As their rank and authority increase, they are entrusted with more responsibility, necessitating a staunch ethical stance. In the absence of checks and balances, an authority can progressively become corrupted, which can lead to unfair acts and decisions. Yet, an ethical leader is someone who puts the needs of others before their own, who listens carefully to those who disagree with them, who puts the group's interests ahead of their own, and who serves others without expecting anything in return other than the satisfaction of doing good (Treviño et al., 2000). It is first and foremost a willingness to interact with the greater community, while fairness is at the center of the decision-making process for ethical leadership. This self-reflection, interaction, receptivity, and commitment will enable the leadership to comprehend and respond to diverse demands and concerns.

There are several different conditions that need to be met before ethical leadership can take place. The values and personality of a leader could be the starting point. Leaders should consider how their decisions will affect the public at large. This requires a degree of personal mastery, as Philip Massinger once

remarked: "He who would govern others must first rule himself" (Massinger, 1624). Ethical leadership can be developed through the cultivation of traits like honesty, consideration, and social awareness. It is also essential to cultivate a communal feeling. Leaders should value developing relationships with a variety of stakeholders. Setting goals and values for these relationships helps leaders consider the impact of their choices on the broader public and stakeholders. This fosters positive connections between leaders, subordinates, and the general public. Additionally, an ethical leader should be able to promote ethical behavior within the organization. This trait is essential for a leader because it fosters an environment of moral conduct (Downe et al., 2016). A feedback mechanism between leadership, personnel, and the community can help establish trust and encourage transparency. For this reason, the leadership should outline a vision and a set of values and be willing to uphold them regardless of their position or authority. It is important that the goals, ethics, and values of the organization are reflected in the policies that are in place. Having said that, the culture of the organization should also be transparent with reference to the ethical standards it promotes. There needs to be harmony between what is being done and what is being reported. There is often a discrepancy between stated and actual instances. If there is a mismatch between what is actually happening and what is written down, corrective action should be taken. Ensuring congruence in values between organizational members and the organization itself is of critical importance.

In conclusion, given the concerted efforts to promote ethical leadership, the establishment of an ethical ecosystem is essential. A robust interpersonal leadership structure is indispensable for facilitating the transformation of an organization's management into a self-sustaining ethical leadership framework. This necessitates the implementation of procedures and the establishment of advisory systems geared toward enhancing the leadership qualities of personnel. In addition, an intra-organizational component is required, in which organizational procedures are meticulously crafted to promote ethical conduct

among all employees. This objective requires an investment of time and effort to accomplish.

**Ethical Leadership and Decisionmaking in the Information Technology Sector: Nurturing a Responsible Organizational Environment**

Maintaining good cybersecurity standards necessitates the utmost diligence and self-reflection in various critical areas to support the robust security of digital platforms. With technology's widespread influence on people, organizations, and communities, ethical questions are becoming more important. Rapid advancements in the IT industry have created complex ethical dilemmas, such as data privacy, algorithmic biases, and the responsible application of emerging technologies such as artificial intelligence and automation. Fostering an ethical culture in the IT industry is crucial not only for maintaining trust and credibility but also for ensuring the equitable and responsible development and deployment of technology for the benefit of all stakeholders.

The most effective cybersecurity measures stem from mission-driven and risk-adjusted approaches to information security, striving to maintain rigorous standards for information confidentiality, integrity, and availability through harmonious integration of user, policy, and technology components. In the absence of a set of values and ethical practices, the majority of these essential cybersecurity principles can be easily compromised. In order to remain competent and competitive in the digital world, it is essential to develop norms and values that inspire trust without stifling sectoral innovation with arbitrary and unidirectional directives. Ethics in cybersecurity can aid in establishing a culture that values trust, honesty, and consideration within the organization and among its stakeholders. Ethical decision-making, values, goals, and missions can all serve as guides for the development of a thriving and healthy culture within an IT organization.

Organizational values are indispensable as they serve as foundational predictors of behavior. Many abstract concepts in cybersecurity could be compromised without values and this is why they are also essential in the digital sector (Huang & Pearlson, 2019). Notably, from a leadership perspective, its significance assumes paramount importance. Leaders are responsible for setting a positive example and emphasizing organizational values through their own actions. As they have a greater impact on the formation of attitudes and behaviors if the leadership of the organization exhibits the proper attitude and practices, the organizational culture can be shaped positively, while the members can be exposed to good ethical conduct. Furthermore, privacy is an essential component of cybersecurity. If an organization or business collects user data, it must process it with care and consideration for the rights of the users. As the concept goes, data is the new oil of the 21st century (Stach, 2023). Large technology companies can derive significant financial value from the user data they collect. In the absence of diligent measures for information security, there exists a vulnerability wherein sensitive information may be susceptible to unauthorized access and compromise. This form of data breach can lead to far-reaching consequences, while profoundly undermining the trust that users repose in service providers. For this reason, diligence and a staunch commitment to these values should be the pillars of the organizational culture. Ultimately, every individual within the organization, be it in a leadership or staff role, actively contributes to the collective success of the organization. Consequently, it becomes indispensable to ensure consistency and congruity across all aspects of the organizational framework. This is no different for the IT sector and institutions.

When it comes to the security of computer networks and data, one particular organization has long been seen as the industry standard-setter. The National Institute of Standards and Technology (NIST) is a laboratory and non-regulatory agency for physical sciences within the United States Department of Commerce. Its purpose is to enhance innovation in the United States and improve US

competitiveness in international markets. Beyond the realm of information security, the NIST directs its focus toward a diverse range of disciplines including engineering, information technology, nanoscale science and technology, neutron research, material measurement, and physical measurement (Covahey et al., 1988). Consequently, NIST rose to prominence as an organization that developed and disseminated vital standards, measures, and guidelines for ensuring the security of digital technologies and online infrastructure. Organizations can efficiently identify and handle numerous cybersecurity threats by referring to the institute's extensive guidelines and definitions. Ethical considerations are a central pillar of these standards, recognizing the inherent importance of integrity, accountability, and fairness in the domain of cybersecurity. These guidelines provide a firm foundation for evaluating and enhancing cybersecurity practices and fortifying digital infrastructure against evolving threats, making them an invaluable resource. Integrity, confidentiality, and availability are three crucial conditions for protecting data and information systems from unauthorized access, use, exposure, interruption, alteration, damage, or loss (NIST SP 800-66 Rev. 1).

According to NIST, confidentiality is about taking preventative steps to prevent unauthorized individuals from gaining access to sensitive data (NIST SP 800-66 Rev. 1). Confidentiality entails disclosing accurate information only to authorized parties, whether they are inside or outside the company or organization. This is especially crucial when handling sensitive data such as financial information, personal identification information, and trade secrets. Loss of trust, legal action, and financial losses may result from a failure to maintain confidentiality. The significance of ethical considerations in maintaining confidentiality cannot be overstated, as they serve as a crucial governing principle that discourages individuals from engaging in actions that could compromise the security and privacy of sensitive information. Adherence to ethical standards provides members of an organization with a moral compass to maintain the highest level

of protection for sensitive information and create trust among individuals, businesses, and the general public.

In addition to confidentiality, the NIST lists integrity as another important criterion for cybersecurity. It defines integrity as the protection of information against unauthorized modification or destruction, as well as the assurance of non-repudiation and authenticity (NIST SP 800-66 Rev. 1). It is essential that the data remain secure and unaltered throughout its lifecycle. Inaccurate data poses a substantial risk to decision-making, potentially jeopardizing the validity of choices and leading to negative consequences. Consequently, data accuracy and integrity serve as the basis for making informed decisions. Given the importance of accurate data for better decisions in today's data-driven world, it is imperative that rigorous data quality standards and ethical practices be upheld.

Finally, availability is the provision of uninterrupted, timely, and stable access to information (NIST SP 800-66 Rev. 1). The information should be accessible wherever it is required and should fulfill the requirements of those who are authorized to access it. For information to be available to those who require it, ethical reflections are indispensable. Access to information should not be unduly restricted or biased, but rather granted in accordance with legitimate requirements and authorized permissions. Individuals who need their data should be able to access it without the need for additional obstacles. Otherwise, it can impact the reliability of the entire digital infrastructure. In order to assure greater levels of productivity and effectiveness, ethics are significantly consequential.

In conclusion, the principles of confidentiality, integrity, and availability constitute an essential ethical foundation for the field of cybersecurity. The observance of these principles encourages responsible behavior, promotes data protection, ensures the accuracy and dependability of information, and ensures continuous access to vital resources. By adhering to these ethical considerations, organizations and individuals can establish a culture of trust, accountability, and integrity in their cybersecurity practices, thereby mitigating risks and protecting

themselves from potential digital threats. In addition, given that digital platforms offer access to users all over the world and that cyberspace is not divided by the same political boundaries, the repercussions of cyber issues can have a ripple effect on an international level. The following section will examine how unethical decisions and actions can cause problems not only at the local level but also on a global scale.

**Recent Events That Put Big IT Firms Under the Spotlight**

A number of recent significant incidents have spurred the public to be upset about the influence and power of big technology companies. Some of the decisions made by the leaders led to some of the most well-known internet scandals in history. One such incident occurred on Facebook when certain application developers were granted permission to access users' personal data, including the names and contact details of those who had downloaded their apps. According to company representatives, this type of data collection would help improve the user experience (Rosenberg & Dance 2018). Nevertheless, Facebook did not verify how developers utilized the data or whether they provided any Facebook experiences. The scandal was exposed by the Cambridge Analytica questionnaire that collected user information. The poll was hosted on the servers of online survey solution provider Qualtrics. The questionnaire included a variety of assessments that psychologists frequently use to assess personality traits. These questions included information pertaining to introversion, extroversion, and preferences for group or individual activities. When users gave the program permission to access their Facebook profiles, it was able to gather information on the users and their friends (Rosenberg & Dance 2018).

Selling the personal information of Facebook users at the time would have been a significant breach of the company's regulations. Nevertheless, the company did not ensure that applications were compliant with its standards. Cambridge Analytica utilized Facebook data to assist in the development of tools that claimed

to assess the personalities of American voters and influence their decisions. After the corporation claimed that Donald Trump employed its psychology and personality modeling techniques in the 2016 presidential election, a question that has yet to be answered is whether or not the company's technology was responsible for manipulating the choices of the American people in that election (Rosenberg & Dance 2018). In addition, the claims implied that some of the advertising campaigns originated in Russia and received support from the government (Rosenberg & Dance 2018). This scandal, in conjunction with other breaches involving the collection of data, generated concerns over democratic standards and society in the digital environment of the twenty-first century.

As a new and disruptive market force, big tech industries have become technological bullies by intensely leveraging their dominance over platforms and markets to reduce competition that could develop alternative products (Tokat, 2022). In response to the Cambridge Analytica scandal, which revealed the potential abuse of Facebook's enormous influence over user opinions, there has been an antitrust crackdown on large IT companies. Numerous significant data misconduct incidents have compromised the privacy and security of consumers over the years (Paul, 2020). The US Department of Justice filed antitrust claims against Google Inc., posing a significant legal impediment for the company. In September 2019, fifty U.S. state and territory attorneys general launched an investigation into possible monopolistic behavior by Google and Facebook (Paul, 2020).

Furthermore, a pivotal report detailing a House judiciary committee investigation indicated that big tech exercised a disproportionate amount of influence, crippling the nation's economic engine by limiting political expression and disseminating misinformation (Romm, 2020). The investigations are further complicated by the partisan nature of the backlash against big tech, with Democrats targeting companies largely for their monopolistic characteristics and Republicans accusing them of stifling conservative dissent (Romm, 2020). The accusations made

against Google, which appears to be a dominant gatekeeper platform, reflect a shift in public perception of technology companies from pioneering innovators to menacing corporate titans. The precedent that the Justice Department has created by targeting Google's advertising and search functions will have far-reaching effects across the entire internet sector. The ascent of Google exemplifies the multifaceted challenges posed by prominent technological enterprises.

A group of privacy advocates and browser developers have taken aim at Google and the advertising technology sector over concerns about widespread and persistent data infiltration that affects internet users. It has been argued that these large technology companies did not take adequate security measures before sending users' personal information to a variety of third-party providers. The group's evidence suggests that this database might contain private information about people, such as their race, disabilities, and gender identity. Because of the sensitive nature of the data, individuals with eating disorders and those who have been the victims of abuse or sexual assault may be targeted specifically in the advertisements (Meyer, 2019). Behavioral advertising is a technique employed by the internet advertising industry to monitor users across the web and develop profiles based on their activities. When visitors access a website employing behavioral advertising, a bidding process is typically conducted automatically, with the winner receiving the right to display an ad that appears to match the visitor's profile. Real-time bidding reveals personal profile data to marketers in the form of bid requests, which are then tailored (Meyer, 2019). The fact that the overwhelming majority of the growth in internet advertising has been concentrated primarily within the domains of Google and Facebook is a further thought-provoking factor. (Ingram, 2017).

## CONCLUSION

In conclusion, the implementation of diverse ethical approaches in cybersecurity holds great promise for addressing the ethical deficiencies that have been observed among leaders in the field. Since user trust and confidence in digital infrastructure are crucial for the maintenance of a strong and democratic society in modern times, the importance of values and ethics in the field of cyber security is increasing (Tokat, 2022). Developing ethical guidelines and standards for cyber security professionals is vital to making sure that their actions are consistent with values and norms. Moreover, promoting transparency and accountability in digital infrastructure can aid in fostering user confidence and preventing potential security breaches. Hence, complete cyber hygiene and security are improbable without respecting fundamental values like justice, equality, freedom, and privacy. Since fundamental vulnerability and defense begin with the user and the people, the ethical leadership paradigm may contribute to an enhanced cybersecurity posture.

By engaging in comprehensive studies to examine the underlying factors contributing to ethical deficiencies and exploring a multitude of hypotheses to promote ethical behavior, it becomes feasible to foster a culture of accountability within organizations. Moreover, given the recent events that have subjected prominent IT corporations to meticulous scrutiny, it becomes imperative for leaders and decision-makers in the IT sector to demonstrate unwavering ethical conduct. The leaders of a business or organization may start to care less about the ethical components of management if financial goals take precedence over all others. The potential for financial growth and dominance can convince executives not to slow down and play it safe, as power and profit may make it difficult for them to decelerate and evaluate their decision-making procedures. Furthermore, a position of authority and power may remove counterbalances, enabling a leader to act unethically without having to reconsider or even notice their actions. Recent incidents involving Google and Facebook provide a useful illustration of this

point. For instance, if the executives of large tech companies lack self-reflection and a set of principles and values, the internet's anonymity and enormous revenue potential may entice them to act for their own benefit while abusing the poisons within their organization. The pervasive influence of technology on a global scale amplifies the inherently problematic nature of these breaches, as they possess the potential to engender far-reaching consequences that transcend geographical boundaries. This is of paramount significance, particularly when considering the profound impact that disasters within the tech industry can exert on a worldwide scale, thereby underscoring the significance and urgency of addressing and mitigating such breaches.

The IT industry can manifest its dedication to responsibility and accountability by upholding rigorous ethical standards, thereby fostering enhanced trust among a multitude of stakeholders, and safeguarding the long-term integrity of the online environment.

The endeavor to enhance ethical leadership, integrate ethical principles, and prioritize ethical conduct within the cybersecurity domain necessitates a synergistic approach. This comprehensive strategy holds immense promise in laying the foundation for a digital landscape characterized by trustworthiness, security, accessibility, and reliability. Since cyberspace is a highly dynamic environment characterized by ever-changing technologies, people, ideas, and networks, continuous adaptability, and innovation to new circumstances and conditions are required. An environment that is trustworthy and unthreatening is necessary for innovative ideas. While organizational culture can serve as a bedrock for perpetuating ethical behaviors among its members, the presence of ethical leadership assumes a paramount role in fostering a culture characterized by creativity, trust, and awareness. By doing so, ethical leadership not only cultivates an environment conducive to innovation and adaptability but also instills confidence among clients and the broader public. In the end, more and more technology businesses with ethically sound management will be able to transform

the digital world into one that is less cohesive and more collaborative. This encapsulates the original intent and visionary aspirations of the pioneering architects of the internet.

## SOURCES


1. Asllani, A., White, Ch.S. & Ettkin, L., 2013. Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals. *Journal of Legal, Ethical, and Regulatory Issues*, 16(1), 7-14. Available at: https://www.proquest.com/openview/99d61ac21426edd17a928d278dec115e/1?pq-origsite=gscholar&cbl=38868 (16.06.2023)
2. Brown, M.E., Treviño, L. K. & Harrison, D.A., 2005. Ethical leadership: A social learning perspective for construct development and testing. *Organizational Behavior and Human Decision Processes*, 97(2), 117-134. https://doi.org/10.1016/j.obhdp.2005.03.002
3. Christen, M., Gordijn, B. & Loi, M., 2020. The ethics of cybersecurity. Springer Nature. https://doi.org/10.1007/978-3-030-29053-5
4. Cleveland, M. & Spangler, T., 2020. Toward a Model for Ethical Cybersecurity Leadership. In: *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications* (pp. 294-302). IGI Global.
5. Collins, S., 2015. *The core of care ethics*. Springer.
6. Covahey, V., Ford, S., Porter, G. & Shaffer, S., 1988. *'Guide to NIST'. NIST special publication* 858. p.1-5. Available at: https://ia902700.us.archive.org/34/items/guidetonist858cova/guidetonist858cova.pdf (16.06.2023)
7. Downe, J., Cowell, R. & Morgan, K., 2016. What determines ethical behavior in public organizations: Is it rules or leadership? *Public Administration Review*, 76(6), 898-909. https://doi.org/10.1111/puar.12562
8. Formosa, P., Wilson, M. & Richards, D., 2021. A principlist framework for cybersecurity ethics. *Computers and Security*, 109, 1-15. [102382]. https://doi.org/10.1016/j.cose.2021.102382
9. Grove, H., Clouse, M. & Schaffner, L.G., 2019. Cybersecurity description and control criteria to strengthen corporate governance. Journal of Leadership. *Accountability and Ethics*, 16(1), 86-96. https://doi.org/10.33423/jlae.v16i1.1366
10. Huang, K. & Pearlson, K., 2019. For what technology can't fix: Building a model of organizational cybersecurity culture. http://hdl.handle.net/10125/60074
11. Ingram, M., 2017. *How Google and Facebook Have Taken Over the Digital Ad Industry*. Fortune. Available at: https://fortune.com/2017/01/04/google-facebook-ad-industry/ (16.06.2023)

12. Keltner, D., Carrie A.L. & Allison, M.L., 2006. Power and Moral Leadership. In: *Moral Leadership: The Theory and Practice of Power, Judgment, and Policy,* edited by Deborah L. Rhode, 177-194. San Francisco, CA: Jossey-Bass.

13. Ko, C., Ma, J., Bartnik, R., Haney, M.H. & Kang, M., 2017. Ethical Leadership: An Integrative Review and Future Research Agenda. *Ethics & Behavior*, 28(2), 104–132. https://doi.org/10.1080/10508422.2017.1318069.

14. Kuenzi, M., Mayer, D.M. & Greenbaum, R.L., 2020. Creating an ethical organizational environment: The relationship between ethical leadership, ethical organizational climate, and unethical behavior. *Personnel Psychology*, 73(1), 43-71. https://doi.org/10.1111/peps.12356

15. Manjikian, M., 2017. Cybersecurity Ethics: An Introduction (1st ed.). Routledge. https://doi.org/10.4324/9781315196275

16. Massinger, P. 1624. *The Bondman*. Act I, scene iii.

17. Meyer, D., 2019. Google and the Ad Industry Accused of "Massive" Abuse of Intimate Personal Data. Fortune. Available at: https://fortune.com/2019/01/28/google-iab-sensitive-profiles/ (16.06.2023)

18. Morgan, G. & Gordijn, B., 2020. A care-based stakeholder approach to ethics of cybersecurity in business. The Ethics of Cybersecurity, 21, 119-138.

19. NIST SP 800-66 Rev. 1 under Security from 44 U.S.C., Sec. 3542. Available at: https://csrc.nist.gov/glossary/term/security (16.06.2023)

20. Paul, K., 2020. Washington's crackdown on Google is the greatest threat yet to big tech. The Guardian. Available at: https://www.theguardian.com/technology/2020/oct/20/google-antitrust-charges-threat-big-tech (16.06.2023)

21. Prentice, R., 2014. Ethical Leadership, Part 1: Perilous at the Top. The University of Texas at Austin. Available at: https://docplayer.net/60911681-Ethical-leadership-part-1-perilous-at-the-top-questions-for-classroom-discussions.html (16.06.2023)

22. Romm, T., 2020. Amazon, Apple, Facebook, and Google grilled on Capitol Hill over their market power. The Washington Post. Available at: https://www.washingtonpost.com/technology/2020/07/29/apple-google-facebook-amazon-congress-hearing/ (16.06.2023)

23. Rosenberg, M. & Dance, G., 2018. You Are the Product': Targeted by Cambridge Analytica on Facebook. The New York Times. Available at: https://www.nytimes.com/2018/04/08/us/facebook-users-data-harvested-cambridge-analytica.html (16.06.2023)

24. Shoemaker, D., Kohnke, A., & Laidlaw, G. 2019. Ethics and cybersecurity are not mutually exclusive. *EDPACS*, 60(1), 1-10. https://doi.org/10.1080/07366981.2019.1651516

25. Stach, C., 2023. Data Is the New Oil–Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration. *Future Internet*, 15(2), 71. https://doi.org/10.3390/fi15020071

26. Treviño, L.K., Hartman, L.P. & Brown, M., 2000. Moral person and moral manager: How executives develop a reputation for ethical leadership. *California management review*, 42(4), 128-142. https://doi.org/10.2307/41166057

27. Tokat, Y. 2022. The Big Tech versus the Nation-States: Clash of Economic Interests and Struggle to Compete on a Global Scale. In Eurasian Conferences on Language & Social Sciences. Retrieved from https://publicatio.bibl.u-szeged.hu/26368/1/Mypart.pdf (16.06.2023)

28. Tokat, Y. 2022. Are Internet Regulation and Freedom of Speech at odds? How can the Balkanization of the Internet Affect Users' Freedoms on the Internet? Gondolat Kiadó. Retrieved from http://publicatio.bibl.u-szeged.hu/26379/1/DoctoralWorkingPapers-UniversityofGyor.pdf (16.06.2023)

ISSN 2630-886X

18 57

BGE