ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

The Boundaries of Freedom in the Use of the Internet in Cyberspace

Ihsan Ali Chichan Alsamauauly. Alsamauauly[1] , Leila. Raisi[2*] , Maher Ibrahim Qanbar. Al-Azzawi[3] , Mahmood. Ashrafi[4]

1 PhD student, Department of Public Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
2 Professor, Department of Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran
3 Assistant Professor, Department of Law, University of Iraq, Baghdad, Iraq
4 Assistant Professor, Department of Law, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran

* Corresponding author email address: raisi.leila@gmail.com

This article explores the multifaceted implications of Internet usage within cyberspace, focusing on its positive contributions, inherent challenges, and the boundaries of freedom associated with its use. The Internet has transformed communication, information exchange, and societal development, enabling global connectivity and providing access to vast resources across diverse fields. It highlights the benefits of the Internet, such as facilitating education, commerce, and interpersonal relationships while promoting knowledge dissemination and cultural integration. However, the article delves into the negative consequences, including data breaches, cybercrimes, privacy violations, and the proliferation of harmful content, such as extremism and misinformation. It also underscores the social and psychological impacts, such as addiction, isolation, and moral decline, particularly among youth. The analysis identifies the Internet as a double-edged sword, with its potential for misuse requiring ethical and legal frameworks to guide responsible use. The article emphasizes the critical need for balancing freedom of expression with societal responsibility, safeguarding individual privacy, and mitigating risks associated with unrestricted access to personal and sensitive data. It calls for the development of national and international regulations to address these challenges, ensuring effective protection of users and the establishment of a safe digital environment. The article also explores the contradictions between privacy rights and the demand for transparency in public and private domains, highlighting the complexities of navigating these tensions in the digital age. In conclusion, the article advocates for a collaborative approach involving governments, institutions, and individuals to create a framework that upholds ethical Internet use, protects individual freedoms, and fosters trust in digital interactions. This comprehensive perspective seeks to strike a balance between maximizing the Internet's potential and minimizing its risks.

Keywords: Internet Freedom, Cybersecurity Challenges, Privacy and Data Protection, Ethical Internet Use.

How to cite this article:

1. Introduction

Scientific and technological advancements and the inherently global and dynamic nature of cyberspace—characterized by its continuous transformation—are defined by the combined use of electronics and the electromagnetic spectrum. The purpose of cyberspace is to create, store, modify, exchange, retrieve, delete, and utilize information, rendering physical resources inactive. From this

perspective, this chapter is titled "The Boundaries of Freedom." Based on scientific analyses, the subject of "Internet use in cyberspace" will be examined. This chapter is divided into two sections: "Internet Freedom and Its Applications in Cyberspace" and "Cyberspace and the Possibility of Its Utilization." (Al-Shawabkeh, 2002; Ayoub, 2009; Bari, 2018).

We often hear about cyberspace through news networks or audiovisual broadcasts. Many perceive it as synonymous with space or spacecraft, a notion echoed by some. However, in reality, the term is comprehensive and encompasses a wide range of meanings, including all electronic devices with which the world and humanity interact (Al-Awadi, 2020; Al-Mousawi & Fadlallah, 2014). These devices are neither geographically confined nor limited in scope. They can be operated from any point and provide access to any location worldwide. Regardless of a country's cybersecurity robustness, these tools are utilized for commerce, economic activities, scientific endeavors, and other purposes, enabling penetration into the depths of a nation's cyber and virtual domain. This claim will be substantiated through study and evidence.

The Internet functions as a double-edged sword, serving as a gateway to numerous beneficial resources while, unfortunately, opening pathways for harmful elements to infiltrate systems. Numerous security considerations must be addressed to ensure the proper functioning of computers, networks, and servers. This article will discuss the most significant security concerns and propose several solutions.

Conflicts arising from internet applications are technical in nature. Information technology (IT) is utilized as a tool of unprecedented speed, power, and precision, equipping parties involved in disputes with unparalleled capabilities. However, information warfare views information itself as a distinct entity—either as a weapon or a target. The historical competition for information spans centuries, with nations, institutions, and even individuals striving to protect the information they possess while attempting to restrict the information known to their adversaries. This concept has seen historical evolution. From a historical perspective, information warfare can be traced across eras and periods by extrapolating from the history of wars, as its principles have evolved alongside the development of warfare. For example, in 400 BCE, the Chinese thinker

Sun Tzu identified five types of agents for obtaining information: native, inside, double, covert, and expendable agents. Before the advent of Islam, Arabs employed reconnaissance forces after settling in specific locations to report on the strength, readiness, and movements of their enemies. They used symbols and codes to convey reports and employed traders and travelers for espionage.

The establishment of the first Arab intelligence service occurred after the advent of Islam, with its membership numbering no more than five individuals. During the planning of the migration from Mecca to Medina, Prophet Muhammad utilized this intelligence service to obtain information about the Quraysh, ensuring the mission's success. The Mongols demonstrated their ingenuity in warfare by relying on highly accurate intelligence gathered by specialized and professional individuals known as "Arrow Knights," enabling them to control conflicts and execute attacks on enemy capitals with precision.

The emergence of new forms of information warfare coincided with inventions like the telephone and telegraph—first used in June 1861 during the American Civil War, when 15,000 miles of telegraph cables were extended, transmitting 133,000 messages daily. World Wars I and II showcased developments such as encoded messages, the invention of radar, and extensive psychological warfare techniques directed via radio broadcasts. These wars also saw the beginnings of electronic warfare, which continued to evolve.

The early 1990s, particularly during the Gulf War of 1991–1992, marked the true advent of modern information warfare, bringing its contemporary form into focus.

2. The Internet and Its Applications in Cyberspace

The Internet offers numerous benefits and, under the constant and continuous progression of development without restrictions, has led to the emergence of various interpretations tracing back to its early expansion. It has often been referred to as a "separate and distinct" world apart from daily reality. In the electronic space, individuals can conceal themselves behind false identities, much like the famous New Yorker cartoon suggests (Thil, 2009; Turki & Sirel, 2013). This term, originating from science fiction and art, has entered popular culture. Today, it is employed by technology

strategists, security experts, governments, militaries, industry leaders, and businesspeople to describe the domain of global technological environments more broadly. It is defined as a global network of interconnected information technology infrastructures and networks, as well as communication and computer processing systems. Some define cyberspace simply as a virtual environment where communication takes place through computer networks. This term gained prominence in the 1990s as internet use and digital networking and communications grew significantly (Al-Shammari & Ismail, 2020; Al-Shawabkeh, 2002).

Remarkably, the term "cyberspace" has been able to represent new ideas and phenomena that have emerged. It provides individuals with a social experience where they can interact, exchange ideas and information, offer social support, conduct business, organize direct actions, create art, engage with technical tools, play games, and participate in political discussions, among other activities. All of these are made possible through this global network. The term "cyberspace," occasionally referred to as "cybernauts," has become a common way to describe anything related to the internet and its diverse culture. The United States recognizes interconnected information technologies and networks, which operate through this medium, as part of its national infrastructure.

Among individuals in cyberspace, it is believed that shared laws and ethical regulations benefit everyone, a concept referred to as cyber ethics. Many argue that the right to privacy is of paramount importance within a functional ethical code for internet usage. Such ethical responsibilities align closely with global networks, especially when opinions are tied to online social experiences.

For us, "cyberspace" is primarily associated with the management of spaces. There is nothing inherently mystical about it. It cannot even be strictly labeled as digital; rather, it is merely a tool. Furthermore, the space is tangible and physical.

The term "cyberspace" first appeared in the 1980s in the works of cyberpunk science fiction writer William Gibson, notably in his 1982 short story *Burning Chrome* and later in his 1984 novel *Neuromancer.* In subsequent years, the term became prominently associated with computer networks via the internet. It is often linked to *Neuromancer*, where excerpts related to this concept are frequently cited.

The term "cyberspace" also emerged in visual arts during the late 1960s when Danish artist Susanne Ussing (1940–1998) and her collaborator, architect Carsten Hoff (born 1934), introduced themselves as the Atelier Cyberspace. Under this name, they created a series of installations and images titled "Sensory Spaces," based on the principle of open systems adaptable to various influences, such as human movement and the behavior of new materials.

Cyberspace is a comprehensive consensual illusion encountered daily by millions of legitimate operators in every country, ranging from teaching mathematical concepts to children to graphically representing data extracted from computer systems in human networks. The unimaginable complexity of lines of light within the decentralized space of the mind and data sets fluctuates like city lights.

The term has been widely used and critiqued by Gibson himself. Reflecting on its etymology in the 2000 documentary *No Maps for These Territories,* he remarked, "All I knew about the word 'cyberspace' when I coined it was that it seemed to be an effective buzzword. It sounded evocative and impactful but was fundamentally meaningless. It referred to something, yet had no real semantic meaning, even for me as I saw it appear on the page." During the internet boom of the late 1990s, the term gained increasing traction as efforts by figures like John Perry Barlow and the Electronic Frontier Foundation (EFF) promoted the idea of "digital rights."

This concept can be elaborated upon as follows:

1. **Environmental Virtualization**: Although the current widespread use of "cyberspace" no longer exclusively refers to immersion in virtual reality, contemporary technology allows for the integration of various capabilities (sensors, signals, connections, transmission systems, processors, controllers) to create an interactive virtual experience accessible regardless of geographical location. For these reasons, cyberspace has been described as the ultimate tax haven. In 1989, Autodesk, a multinational company specializing in 2D and 3D design software, developed a virtual design system called Cyberspace.

2. **Cyberspace**:

- o a) The physical infrastructure and communication devices enabling connections between technological networks and communication systems (e.g., SCADA devices, tablets, smartphones, computers, servers, etc.).
- o b) Computer systems and associated software (sometimes embedded) ensuring basic operational functionality and domain connectivity.
- o c) Networks linking computer systems.
- o d) Networks connecting systems (with distinctions between networks and organizational "network networks").
- o e) Access nodes for user-routing nodes and intermediaries.
- o f) Constituent data (or data at rest) (Bassiouni, 2016; Bouzid, 2018).

In colloquial terms (and sometimes in commercial language), computer networks are often referred to as "intranets," while interconnected networks are labeled "internet." The Internet (capital "I") is sometimes called "the Net" in journalistic contexts and can be considered part of System A. Cyberspace or "information space" is understood as the container where information is stored, and messages are exchanged between devices (e.g., computers, phones, etc.) and other systems. The *Oxford Dictionary* defines cyberspace as:

Before highlighting the concept of "cyberspace," it is necessary to explain its meaning and emphasize its essence. The term derives from the field of cybernetics, referring to the science of automated control, and has been used to describe the interconnected networks of computer systems. The National Cybersecurity Organization defines it as the interconnected network of IT infrastructures (including the internet, communication networks, computer systems, and connected devices, as well as their associated processors and arbitration devices). It can also denote an imagined or hypothetical realm, like an experiential phenomenon or abstract concept. The Communications and Information Technology Commission defines cybersecurity as "the protection of networks, IT systems, and operational technology systems and their hardware and software components, as well as the services they provide and the data they transmit, against any hacking, disruption, alteration, or unauthorized login, use, or

exploitation." Cybersecurity encompasses information security, electronic security, digital security, and more (Ayoub, 2009; Bari, 2018).

The use of the internet can yield inverse outcomes. On the one hand, its positive applications can play a fundamental role in societal advancement and the development of nations. On the other hand, it may lead to numerous abuses and negative indicators, resulting in the destruction of societies.

2.1. Freedom of Positive Use in Cyberspace

The Internet has numerous positive aspects, reflecting diverse cultures and fostering significant intellectual growth. Through the Internet, we can access any information worldwide, regardless of distances and language barriers. It even facilitates communication between individuals in entirely different continents or remote geographical locations. In reality, it would be impossible for one person to connect with another within a few seconds, but with this technological advancement, information can be disseminated broadly without causing embarrassment or severe inconvenience due to ignorance of certain issues.

Consequently, the Internet has witnessed the growth of data collection processes from the real world, as the online environment has become more accessible and computational technologies have made tabulation more convenient. Furthermore, information exchange tools in all forms (made available through the Internet and web browsing software) have made communication much easier. Traditional and classical access to information is increasingly reliant on the Internet because it serves as a rich source of knowledge on almost everything, particularly in areas concerning personal and private matters. The Internet provides access to information about individuals, their habits, hobbies, behaviors, opinions, and purchasing tendencies (Bassiouni, 2016; Bouzid, 2018; Hasbo, 2000).

Among the positive aspects of Internet use, its ability to create security and benefits stands out. In 1948, Norbert Wiener, a mathematician, authored works on "cyberspace or control and communication in animals and machines," focusing on control and communication. The term "cybersecurity" that concerns us today originates from a Greek word and predates the French ampere in 1834. It emerged from the logic of systems and the unity of knowledge, used in automatic control

techniques within electronic communication frameworks. Initially, electronic security applications focused on protecting the physical devices and infrastructure of institutions from environmental or natural risks, which became known as information security.

David Smith, in his study titled "How Russia Uses Cyber Warfare," suggests that Russia relies on a broad concept of information warfare. This includes intelligence, counterintelligence, deception, misinformation, electronic warfare, disruption of communication systems, and more—such as interference with navigation support systems and psychological pressure, alongside propaganda and damage to information systems.

The number of active users on social media networks (such as Facebook) has surpassed 1.5 billion in recent months. Statistics indicate that Arab users account for approximately 100 million of these users, with a significant portion accessing these platforms through modern mobile phones. Encryption of electronic transactions ensures that no hacker or attacker can easily access this data or applications. Encryption serves as a protective method, making decryption difficult (Al-Shawabkeh, 2002; Ayoub, 2009).

Encryption can preserve confidentiality and privacy by transforming messages into encrypted texts, making them unreadable to unauthorized individuals. Only the intended recipient can interpret the information. If the information reaches unintended individuals, they cannot benefit from it or even understand its meaning.

To encourage secure and appropriate participation in the information society and to benefit from the knowledge society's potential for growth and development, suitable laws must be enacted:

1. **Regulating E-commerce**: Countries increasingly rely on electronic systems for trade, significantly speeding up processes and preserving data and information exchanged in domestic or international trade.

2. **Privacy Protection and Freedom of Expression**: Enacting laws to prevent violations of personal privacy is essential. Without legal deterrents, everyone's privacy is at risk in the cyber world.

3. **Guaranteeing the Right to Access Global Information Networks**: This fundamental right must be preserved, particularly in virtual spaces. However, these networks require regulation rather than absolute freedom.

4. **Protecting Personal and Sensitive Data**: Critical and sensitive data may have security implications. If left unregulated, such information could expose individuals or even national economies to risks.

5. **Content Regulation**: This involves curbing the spread of materials that are offensive to public morals, disrespect societal traditions, or adversely influence generations by altering values and principles.

6. **Intellectual Property Rights Protection**: Intellectual property, including scientific or cultural endeavors, may be stolen or attributed to others without merit, undermining the work of thinkers who contribute significantly to societal and cultural growth.

7. **Child Protection Online**: Laws must safeguard children from harmful influences or ideologies that aim to distort Islamic thought or deviate from moral and ethical principles. Families and governments bear the responsibility of restricting malicious actors and promoting proper child upbringing.

8. **Regulating Electronic Transactions**: Simplifying administrative processes, such as property registration or vehicle registration, through digital systems saves time and resources, enhancing national efficiency.

9. **Cloud Computing Responsibility Regulation**: Legal frameworks are required to ensure accountability for cloud services, providing clarity and confidence in their operations.

10. **Adopting Objective Criminalization Principles**: Laws that define and penalize cybercrimes are crucial, evolving with societal and technological advancements to remain effective.

11. **Establishing Prosecution and Enforcement Standards for Cybercrimes**: Enforcing legal provisions against cybercrimes requires comprehensive legal frameworks without infringing on individual freedoms.

12. **Promoting National, Regional, and International Cooperation**: International

conferences and agreements are necessary to address the borderless nature of cyberspace and mitigate its associated challenges.

13. **Encouraging Public-Private Cooperation Against Cybercrimes**: Collaboration among governments, private entities, and citizens is vital for safeguarding the virtual environment and managing information and ideas responsibly.

Data exchanged over the Internet—sometimes called "information rivers"—may include users' IP addresses, browser types, computer types, and the activities undertaken during previous site visits. While some of this information is essential for network operations, others are not. Misuse of these data can lead to privacy concerns and potential harm to individuals or businesses.

Positive Aspects of Internet Usage:

1. Facilitating knowledge acquisition and the exchange of ideas in scientific, cultural, or experiential fields.
2. Connecting individuals and fostering convergence of ideas across diverse cultural and social contexts.
3. Strengthening social bonds through continuous communication with family and friends, facilitated by platforms like WhatsApp.
4. Managing crises, such as during COVID-19, by enabling remote communication, spreading health updates, and coordinating responses.
5. Promoting e-learning and enhancing student capabilities through scientifically designed online education.
6. Advancing scientific research and reducing reliance on traditional methods of dissemination.
7. Supporting commercial, economic, and financial activities, making them more efficient and cost-effective.
8. Reducing the time required for communication, mail delivery, and data transmission.
9. Generating substantial profits through online work, including e-marketing projects.
10. Simplifying daily tasks such as booking flights, finding entertainment, or locating information.
11. Allowing individuals to learn and explore discreetly, overcoming social stigma around ignorance.
12. Assisting in navigation using maps and GPS, enabling users to reach destinations efficiently.
13. Enhancing security through surveillance of homes, streets, and institutions via online monitoring systems.

2.2.   Freedom for Negative Uses in Cyberspace

It is often noted that excessive freedom, which disrupts societal peace, may transform into unrestricted or limited freedom, eroding the notions of justice, equality, and reason that define freedom. As the saying goes: "Your freedom begins where the freedom of others begins." The freedom under discussion here requires controls, much like a citizen's freedom to walk in parks or streets. However, does this mean that individuals wandering in parks or streets have the right to break or destroy objects? Certainly, such behavior contradicts human reason and innate nature. Thus, moral and conscientious controls must complement laws. For this reason, unrestricted Internet usage and unmeasured actions may harm others, prompting all countries to establish systems and controls for the use of cyberspace. These systems are based on the principle of standardizing legal rules for criminalizing cyber-related offenses and ensuring their prosecution and enforcement. Each country adopts legal frameworks allowing it to apply the principle of dual criminality and facilitate effective cooperation (Al-Ashqar, 2016).

When electronic systems were invented, a new type of war began. In 1957, when the Soviet Union launched the Sputnik satellite, the battlefield shifted to cyberspace. This sparked alarm in the United States, motivating increased government investment in science and technology.

Tracing the history and emergence of electronic wars reveals their roots before and after World War I. Communication between different parts of the world began with wired communication using Morse code through the "acoustic telegraph" in 1837. Beyond this, communication involved exchanging messages by ship between seaports. During the U.S. Civil War, beginning in April 1861, telegraph lines became strategic targets for opposing forces. Signal workers interfered with wired communication lines, intercepting conversations by

connecting telephones in parallel. Both sides cut communication lines when necessary to prevent interference. Wireless communication began in 1888 with the work of Heinrich Hertz, and by mid-1897, Italian engineer and inventor Guglielmo Marconi created a wireless device suitable for maritime use. Wireless communication was later employed in naval theaters in Europe by 1901 (Al-Ashqar, 2016).

The Internet emerged in the 1960s through a U.S. government project called ARPANET. This project aimed to secure an indestructible private communication network for activation during sudden warfare. Four large supercomputers were connected to test the system. By the early 1990s, interest in information as a source of competitive advantage grew. Security measures were developed to protect information collection, storage, processing, and communication within organizations from competitors' illegal access. Beyond physical protection, the term "information security" or "information systems security" gained prominence. With the proliferation of information and communication technologies, the concept expanded to include electronic security, safeguarding electronic business, and managing electronic transactions. This evolved into a comprehensive concept, adapting to technological developments and threats.

Electronic and digital strategies, such as electronic warfare and digital defense, legal surveillance and privacy protection, and economic competitiveness, illustrate a broader, integrated concept known as "cybersecurity." This necessitates a national-level protective strategy (Rustam, 2009).

By the late 1970s, the first protocol (X.25) was introduced to connect computers. The term "hacking" emerged, focusing on software vulnerabilities. The digital revolution and advances in communication systems exposed information to threats endangering individuals, groups, and organizations. These digital changes made information security an urgent concern for policymakers and experts, affecting all societal sectors regardless of age, occupation, or interests, including service providers, recipients, legislators, and security professionals (Hasbo, 2000).

In the 1980s, the World Wide Web was invented in Geneva, Switzerland, in nuclear research laboratories. This innovation is attributed to a young researcher, Tim Berners-Lee, who developed a popular text encoding language to enable computers to communicate with one another (Rustam, 2009).

Cybersecurity has been recognized as dependent on a complex mix of political and social challenges. As recommended by the International Telecommunication Union, cybersecurity's credibility relies on the following principles:

1. Developing and expanding a national strategy for cybersecurity and protecting critical information infrastructures.
2. Fostering constructive collaboration between governments and telecommunication and information companies.
3. Preventing cybercrimes.
4. Establishing national capabilities for managing computer incidents.
5. Promoting a national culture of cybersecurity.

Key Reasons Necessitating Cybersecurity:

1. The necessity of connecting to communication and internet systems.
2. Dependence of various institutions on effective information utilization, which grows with technological advancements.
3. Challenges in managing and controlling risks or prosecuting and punishing offenders.
4. Continuous growth in electronic applications and the emergence of e-commerce.
5. The direct relationship between security and technology, where cyber risks threaten strategic interests.
6. The international dimension of cybersecurity, requiring adaptable strategies to address ongoing changes in mechanisms and tactics.
7. The expansion of cybersecurity concerns beyond technical aspects to include cultural, social, economic, and military dimensions.
8. The regulation of standards and procedures to prevent non-peaceful uses of cyberspace.
9. The growing influence of non-state actors in international relations, particularly with the rise of transnational technology companies, impacting state sovereignty.

The relationship between security and technology, coupled with strategic interests' exposure to electronic risks, poses the threat of cyberspace becoming a medium—or even a source—of new tools for international conflict.

Based on the above points, after discussing the quality or benefits of Internet usage in various ways and addressing the negatives and associated problems, we can highlight the most critical negative aspects accompanying the cyber or electronic Internet system, including:

1. **Isolation and Addiction to Virtual Life**: Internet users often suffer from mental disorders and major health issues, including obesity and neurological conditions, caused by excessive use of the Internet.

2. **Espionage, Hacking, and Easy Access to Data**: Unauthorized access to personal or confidential information leads to significant domestic and international issues.

3. **Negative Influence on Youth and Adults**: The proliferation of obscene websites and weak family supervision negatively impacts users.

4. **Spread of Extremism and Sectarian Ideas**: Individuals with weak resolve or those subjected to brainwashing are exploited and recruited for ideological or armed conflicts. Many extremist movements recruit youth online, encouraging unusual relationships, religious extremism, violence, killings, and displacement.

5. **Deteriorating Health of Internet Addicts**: Symptoms of excessive use manifest in social and familial realities.

6. **Loss of Time**: Many users waste time on distractions without deriving meaningful benefits.

7. **Widespread Unemployment**: Internet usage can lead to neglecting legitimate job searches or income opportunities, exemplified by selling goods via social media.

8. **Promotion of Defective Drugs**: These are often sold cheaply online without proper oversight, aiming for maximum sales.

9. **Moral Decline in Society**: Internet publications lacking public morality erode traditions and good customs.

10. **Western Influence on Arab-Islamic Societies**: Imposing unacceptable customs, such as inappropriate clothing and unsuitable fashion trends.

11. **Online Drug Trade**: Security sources report the online beautification and promotion of drugs to attract users.

12. **Cyber Extortion Crimes**: Coercion of individuals into obscene acts or submission to perpetrators.

13. **Rapid Spread of Rumors**: False information and anxiety-inducing content circulate quickly online.

14. **Sexual Exploitation and Youth Manipulation**: Internet use has contributed to the collapse of conservative families.

15. **Neglect of Education**: Some youths abandon schools and colleges due to their preoccupation with the Internet.

16. **Defamation and Character Assassination**: Slander and publication of defamatory content targeting individuals and institutions.

17. **Fraudulent Identities**: Fake profiles and impersonations are prevalent online.

18. **Malicious Viruses**: Designed to drain users' resources and disrupt technological devices.

19. **Negative Impact on Professions and Industries**: Hindering competition and reducing quality production.

20. **Cybersecurity Threats**: Targeting governmental institutions or exposing malicious software from anonymous entities.

21. **Difficulty Identifying Users**: Challenges in recognizing individuals lead to delays and opportunities for misuse.

22. **Specialized Hackers**: Those with expertise in electronic systems pose significant security threats.

23. **Bullying and Mockery**: The Internet is a tool that encourages ridicule of others.

24. **Privacy Breaches**: Threats from hacking tools remain a major concern for users.

25. **Misinformation**: Misleading information impacts generations and demands accountability.

26. **Overreliance on the Internet**: Diminishing traditional academic research and critical thinking skills.

27. **Unsafe for Children**: Parents often fear their children's exposure to harmful online content.

28. **Financial Fraud**: Numerous phishing websites exploit unaware users.
29. **Erosion of Trust**: The Internet has fostered skepticism and distrust among users.
30. **Unreliable Information**: The circulation of dubious or incorrect information affects credibility.
31. **Intellectual Property Theft**: Copying research and claiming it as original work violates copyrights.
32. **Weaponization of Stored Data**: Large amounts of data in cyberspace become a powerful tool for criminals.
33. **Database Theft**: Programmers can easily steal information from personal accounts or institutional systems.
34. **Piracy**: Unauthorized distribution of movies, music, and series undermines intellectual property.
35. **Economic Damage**: Piracy devastates content production industries worldwide.
36. **Fraudulent Tools**: Advanced communication tools in cyberspace have made fraud easier for criminals.

2.3. *The Limits of Freedom in Using the Internet in Cyberspace*

We have previously discussed the freedom to use the Internet, highlighting its importance and the benefits it offers for serving humanity and advancing various fields. We have also examined many of the problems and negative aspects arising from the Internet. Internet use, even if driven by individuals drawn to pleasures or whims, places them in a labyrinthine world. Whether the actions are criminalized, violate public morals, or offend customs and traditions, there must be clarity on the limits of freedom in Internet use, emphasizing public morality and avoiding misuse through offensive language or inappropriate behavior.

From the above, it is evident that there are no inherent limits to the Internet. As a network that reaches the farthest geographical points in the world, it enables individuals—young or old, male or female—to use it, provided it extends to those regions while preserving the privacy it offers. Internet privacy is fundamentally different from other tools, encompassing private relationships. Among the most pressing challenges faced

by nations is the protection of Internet users, particularly children. These challenges include:

1. **Growth of Data Collection and Processing**: The Internet facilitates the collection, processing, and creation of vast amounts of data. It has driven the trend of real-world data aggregation, offering greater accessibility and computational tools that streamline data management. Traditional means of accessing information have been surpassed as individuals increasingly rely on the Internet, which serves as a rich source of knowledge on various topics, particularly personal privacy matters like habits, hobbies, behaviors, opinions, and purchasing tendencies.

2. **Globalization of Information and Communication**: In the Internet environment, information and communication transcend geographical boundaries and sovereignty. Individuals share their information with domestic and international parties, often with no defined location, increasing the risk of misuse, especially in jurisdictions lacking robust data protection laws. National regulations may be insufficient without coordination or guarantees ensuring the security of transferred data. Safe havens with no restrictions on data processing or collection serve as escapes for businesses seeking to avoid legal constraints, creating a global challenge requiring bilateral and international agreements on personal data protection.

3. **Loss of Focus and Control Mechanisms**: Enacting national laws or strategies for human rights protection might be effective but faces challenges related to control and governance. The absence of a central authority capable of monitoring and preventing attacks complicates the provision of legal protection or compensation. Many mobile devices, laptops, and portable tools connected to the Internet enable users to interact freely. Studies, such as one conducted in Yemeni universities during 2010-2011 involving 400 students, revealed the widespread possession and use of personal computers. This indicates societal awareness and the importance of technology in education,

despite economic disparities limiting access for some.

Robert M. Bowie has commented on technocracy, stating that individuals with computers risk reducing private life to limited boundaries, adapting personal and familial life to technological tools. While this might bring economic or social benefits, it can also strip individuals of their autonomy, treating them as mere numbers and diminishing their humanity. The threats here are not of nuclear war but involve cyber warfare using computers. The right to freedom and its limits, as recognized in legal frameworks, presents several contradictions worth addressing. It is crucial to distinguish between individual rights to privacy, access to information, and the pursuit of knowledge. These include:

1. **Contradiction Between Privacy and Disclosure**: Individuals have the right to keep their information private or disclose it for personal benefits. However, such voluntary disclosures can be exploited for purposes other than intended, violating confidentiality.

2. **Public Figures and Disclosure**: Fans may feel entitled to know details about celebrities' lives. However, revealing such information could endanger their personal lives and careers.

3. **State Access to Personal Information**: Governments may intrude into private lives, using personal data in ways that conflict with protection and respect for individual rights.

4. **Research vs. Personal Life**: There is a contradiction between the right to conduct academic research and the right to privacy, particularly when investigating public figures.

5. **Freedom of the Press vs. Privacy**: A balance must be struck between personal life rights and the global freedom of information exchange.

The researcher believes that seeking information is an individual's right and essential for awareness. However, it must not tarnish reputations or be used for blackmail. Individuals posting personal information on platforms like Facebook are aware of the potential monitoring and can modify or conceal such data. Thus, real rights, such as personal dignity and respect in public discourse, should be clearly defined and protected.

While discussing public figures might be acceptable, the intent and manner of engagement remain critical.

Actions involving disrespect or malicious intent need careful examination and legal redress.

3. Conclusion

In conclusion, the use of the Internet presents both vast opportunities and significant challenges, particularly in the realm of privacy, security, and the balance between individual freedoms and public order. As the digital world continues to expand and shape various aspects of human interaction, it is crucial to acknowledge both the positive and negative implications of unrestricted access to information. While the Internet has democratized knowledge and communication, facilitating global connectivity and the exchange of ideas, it has also given rise to complex issues surrounding personal data, exploitation, and the erosion of privacy. The growth in data collection, the proliferation of global information flows, and the potential for abuse highlight the urgent need for robust legal frameworks that can protect users' rights without stifling innovation or the free flow of information. Furthermore, the expansion of the Internet across borders, where different nations have varying degrees of protection for personal data, necessitates international cooperation and the creation of global standards to address the risks of data misuse, cybercrime, and privacy violations. These challenges require not only technical solutions but also ethical considerations that take into account the diverse social, political, and cultural contexts in which the Internet is used.

Moreover, the inherent contradictions between individual rights and the public's interest, between personal freedom and societal responsibility, must be carefully navigated. The tension between an individual's right to privacy and the desire to share personal information freely in exchange for perceived benefits underscores the complexity of digital citizenship in the modern world. While legal protections are essential, there is also a pressing need for greater public awareness and education regarding digital literacy and the responsible use of technology. As individuals increasingly find themselves navigating a world where personal data is commodified, and where every online action leaves a trace, the importance of safeguarding

personal freedom, dignity, and autonomy becomes ever more critical. Governments, businesses, and individuals must collaborate to create a digital landscape that respects privacy, promotes informed decision-making, and ensures that the freedoms granted by the Internet are exercised responsibly. The Internet, at its best, should empower individuals and foster greater understanding across boundaries, but it must also be framed within the context of a shared commitment to ethical use and mutual respect for personal and collective rights. The future of the Internet hinges on striking this delicate balance.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Al-Ashqar, J. M. (2016). *Cybernetics: The Preoccupation of the Age*. League of Arab States; Arab Center for Legal and Judicial Research.

Al-Awadi, H. (2020). Protecting Iraqi Cybersecurity: The Lost Strategy. *Ktebat Newspaper*.

Al-Mousawi, M. T., & Fadlallah. (2014). Information Privacy: Its Importance and the Risks Posed by the Internet. 222.

Al-Shammari, S. M. H., & Ismail, Z. M. A. (2020). Cybersecurity as a New Pillar in the Iraqi Strategy. (62), 291-292.

Al-Shawabkeh, M. A. A. (2002). *Crimes Committed over the Internet*

Master's Thesis Arab Institute for Research, Education, Culture, and Sciences; League of Arab States]. Cairo, Egypt.

Ayoub, P. A. (2009). *The Legal Protection of Personal Life in the Field of Informatics* (Vol. 1). Al-Halabi Legal Publications.

Bari, M. (2018). *Cybernetics (Cybernetic): The Science of Communicating, Controlling, and Dominating* (Vol. 1). Al-'Ataba al-Abbasiyah al-Muqaddasah; Islamic Center for Strategic Studies.

Bassiouni, A. F. (2016). *The Cybernetic Information Space and Transformations of Creativity* (Vol. 1). Arwaq Institute for Studies, Translation and Publishing.

Bouzid, H. S. (2018). *Cybersecurity as a Necessity for the Success of the E-Governance Project: The Case of Algeria*

Unpublished Thesis University of Algiers, Faculty of Economic and Commercial Sciences]. Algiers, Algeria.

Hasbo, A. (2000). *Protecting Freedoms in the Face of Information Systems: A Comparative Study* (Vol. 4). Dar Al-Nahda Al-Arabia.

Rustam, H. (2009). Computer Crimes as a Form of Emerging Economic Crimes. *Journal of Legal Studies, Assiut University*(17).

Thil, S. (2009). March 17, 1948: William Gibson, Father of Cyberspace. *WIRED*.

Turki, M., & Sirel, J. (2013). Information Privacy: Its Importance and the Risks of Modern Technologies. *Journal of the College of Baghdad for Economic Sciences (Special Issue for the College Conference)*, 6-7.