MODERN HUMAN RIGHTS CHALLENGES: CYBERSECURITY

Kovalenko Iryna

State University of Trade and Economics

Supervisor– PhD (Law), Associate Professor Ilchenko Hanna

Kyiv

The rapid progress in digital technologies has significantly expanded the scope of literary sources and information accessible to individuals worldwide. However, this proliferation of digital literary sources has simultaneously introduced a myriad of challenges in the realms of human rights and cybersecurity, necessitating a comprehensive examination. In this research paper, our primary objective is to conduct a meticulous analysis of the prevailing human rights issues stemming from the utilization of digital literary sources within the digital landscape, with a specific focus on the interconnected challenges of cybersecurity. In doing so, we intend to closely investigate the potential risks associated with the extensive use of digital literary sources, particularly concerning privacy breaches and the unauthorized exposure of sensitive data.

The remarkable advancements in digital technologies have brought about a fundamental transformation in the ways people engage with and disseminate information, thereby fostering enhanced opportunities for self-expression and knowledge acquisition. Nevertheless, this digital evolution has simultaneously presented novel challenges, deeply impacting the spheres of human rights and cybersecurity.

It is evident that digital technologies have considerably expanded the freedom of expression, empowering individuals to actively access information and express their viewpoints across various platforms. However, the presence of widespread disinformation and aggressive hate speech in the digital space poses significant challenges to the legal framework. It is necessary to provide an effective mechanism for responding to harmful content that threatens public safety and the health of the information environment, and it should not be forgotten that

people should not be deprived of their freedom of speech, so it is crucial to maintain a balance.

It is worth noting that cybersecurity issues are not local, but global, as they are a matter of global information security, which is extremely important. Therefore, this issue is currently being raised at various conferences to minimise cybercrime as much as possible. The phrase "software is taking over the world" emphasises the profound impact of digital transformation on the global economy, with software penetrating international politics. This shift has increased the importance of technology in economic growth, national security and geopolitical dynamics. The COVID-19 pandemic has further accelerated these trends, amplifying both the benefits and challenges of digital dependence, including a widening digital divide and growing cyber threats. Against this backdrop, major powers such as the United States, China and Europe are actively shaping global technology policies to respond to these new challenges and opportunities. [1]

China's Cybersecurity Law, enacted in 2017, has significantly enhanced the country's surveillance capabilities by enforcing data localization, mandatory real-name registration, and requiring internet service providers to cooperate with law enforcement. The law has eroded privacy protections, allowing authorities to access user data and inspect internet companies' premises for cybersecurity reasons. This regulatory framework has raised concerns about the extent of individual privacy and freedom in the digital landscape within China. [2]

In the contemporary landscape of the information environment, the utilization of digital literary sources is inherently intertwined with a spectrum of potential risks, prominently featuring privacy violations and the looming specter of data leakage. A critical underpinning of comprehending the essence of cybersecurity lies in acknowledging the imperative need for safeguarding not solely classified or sensitive information, but also recognizing the profound implications of alterations to unclassified data, which can precipitate the inadvertent leakage of confidential data or the erroneous transmission of inaccurate information to the intended recipient. The inadvertent loss or accidental destruction

of accumulated data reserves can potentially engender irreversible consequences, warranting a comprehensive and holistic approach towards fortifying data security.

Professionals specializing in cybersecurity meticulously investigate an array of data security breach scenarios, ultimately converging on the foundational understanding that the essence of such breaches can invariably be distilled down to the scenarios delineated above. Depending upon the expanse and scale of data processing systems, the implications of information loss or leakage can reverberate across a diverse spectrum of consequences, ranging from seemingly innocuous jests to precipitating severe economic and political crises of unprecedented magnitudes. Consequently, it is quintessentially imperative to adopt a systematic and proactive approach to forestall and preemptively detect potential cybersecurity breaches.

Cyber threats also notably amplify the vulnerabilities of certain groups, such as human rights advocates and civil society members. They encounter heightened surveillance, often coupled with targeted assaults on their digital identities, ranging from intrusions into their personal social media accounts to the unauthorized disclosure of sensitive personally identifiable information. These targeted attacks substantially curtail their operational capacities, undermine their ability to effectively articulate their views, and may even pose physical threats to their well-being, thereby impinging upon their rights to privacy and security as protected under international human rights law. In response, it is imperative for legal systems to expedite the development and enforcement of comprehensive cybersecurity regulations that effectively preserve and safeguard human rights within the digital sphere.

A serious threat arises from the fact that cyber-attacks can be aimed at destabilising the work of human rights NGOs by destroying or modifying important information or preventing them from achieving their goals through digital channels. This can seriously impede the operations of such organisations and limit their ability to protect human rights from violations. Therefore, ensuring robust cybersecurity for these groups becomes a necessity to preserve their ability

to operate effectively and play an important role in protecting human rights. One of the key areas of protection against these threats is the implementation of effective cybersecurity strategies, including the widespread use of data encryption to ensure the confidentiality and integrity of information. In addition, the use of multi-level authentication can help prevent unauthorised access to personal accounts and data.

Cyber threats also notably amplify the vulnerabilities of certain groups, such as human rights advocates and civil society members. They encounter heightened surveillance, often coupled with targeted assaults on their digital identities, ranging from intrusions into their personal social media accounts to the unauthorized disclosure of sensitive personally identifiable information. These targeted attacks substantially curtail their operational capacities, undermine their ability to effectively articulate their views, and may even pose physical threats to their well-being, thereby impinging upon their rights to privacy and security as protected under international human rights law. In response, it is imperative for legal systems to expedite the development and enforcement of comprehensive cybersecurity regulations that effectively preserve and safeguard human rights within the digital sphere.

With the development of modern technologies and digital platforms, new challenges in the field of human rights protection arise, including those related to cybersecurity. Cyberattacks are becoming a serious threat to privacy, freedom of expression and access to information, especially for vulnerable groups such as human rights activists. To effectively counter these threats, it is necessary to improve cybersecurity strategies, including data encryption, multi-level authentication and systematic software updates. Cybersecurity and the protection of human rights in the digital environment are supported by numerous international and national legal acts. For example, Article 19 of the Universal Declaration of Human Rights enshrines the right to freedom of opinion and information, which includes the right to seek, receive and impart information through any media without restriction or hindrance. [3,4]

Cybersecurity-related legislation and regulations exist in many countries around the world. Some of them include the United States, which has the Cybersecurity and Infrastructure Act; China, which has the Cybersecurity Law, the European Union, which has the General Data Protection Regulation (GDPR). Cybersecurity legislation exists in various countries around the world, and each of them is aimed at protecting digital spaces from cyber threats and ensuring data security. The diversity of such legislative provisions demonstrates the general increase in attention to cybersecurity and the need to regulate digital spaces to ensure security and protect human rights in the online environment. [4, p.1, 4, 36]

Cybersecurity remains a global priority as digital technologies continue to impact countries and citizens around the world. This requires not only the development of effective legislative provisions to protect against cyber threats, but also improved international cooperation in this area. The application of strict cybersecurity measures should be fair and transparent, ensuring the protection of human rights and privacy in the digital space at the international level.

REFERENCES

1. Megan Roberts. International cooperation on digital and tech: outlook for the rest of 2021. August 30, 2021 URL: https://unfoundation.org/blog/post/international-cooperation-on-digital-and-tech-outlook-for-the-rest-of-2021/.

2. User Privacy or Cyber Sovereignty? 2020 URL: https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty.

3. Загальна декларація прав людини прийнята Генеральною Асамблеєю ООН 10 грудня 1948 року URL: https://don.kyivcity.gov.ua/files/2014/11/24/deklaracia.pdf.

4. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу США, Канади та інших URL: https://infocenter.rada.gov.ua/uploads/documents/28982.pdf.