Vol. 25 No 55 (2026)

Article

Experience and Lessons from Human security in the cyber environment: Risks and key protection issues

Gerelchimeg Kaliinaa[1]
Doctor (Ph.D), Research and Development Specialist,
Mongolian National Defense University, Ulaanbaatar, Mongolia
kgerelchimegk@gmail.com, ORCID: 0009-0007-5210-4601

Ideshnorov Demberel[2]
Doctor (Ph.D), Chief of the Research and Innovation Division,
Mongolian National Defense University, Ulaanbaatar, Mongolia
ideshnorov1919@gmail.com

Tsogzolboo Otgonbayar[3]
Lecturer,
Mongolian National Defense University, Ulaanbaatar, Mongolia
Temuulenmgl3@gmail.com

Enkhbaatar Chinbat[4]
Senior lecturer,
Mongolian National Defense University, Ulaanbaatar, Mongolia
chinbatenhbaatar931@gmail.com

ARTICLE INFO:

RECEIVED: 06 October 2025
ACCEPTED:15 December 2025
PUBLISHED: 15 January 2026

CORRESPONDING AUTHOR:
Gerelchimeg Kaliinaa

ABSTRACT

Breakthroughs in digital innovation, including artificial intelligence (AI) and Internet of Things (IoT) devices, have opened numerous opportunities across various aspects of human life. However, these technological developments also entail significant risks, such as the collection of personal data, influence over individual thoughts, behaviors, and lifestyles, alongside constraints on individual liberties. Such dynamics facilitate the emergence of "digital enslavement," wherein human safety in cyberspace is compromised through mechanisms of surveillance, exploitation, and rights suppression. Furthermore, the complete control and automation of human life and social interactions via AI and interconnected devices could lead to highly detrimental outcomes. Given these developments, the

Vol. 25 No 55 (2026)
KEYWORDS: Digital environment, Internet of Things (IoT), Artificial Intelligence (AI), personal data, surveillance, manipulation, algorithm

Article

issue of human security in digital environments has transcended a purely technological domain, becoming a complex, multidisciplinary challenge that demands coordinated efforts from social, economic, psychological, legal, and educational sectors. Ensuring the security and reliability of cyberspace necessitates collaborative efforts among governments, technology firms, civil society, and individuals.

I. INTRODUCTION

Today, human daily life and social relations are directly dependent on technology, and the cyber environment has become an integral part of human life. As cyberspace expands[1], It has become difficult to maintain human dignity, freedom, and social status, and it has brought with it a variety of “risks.” The issue of human security in the cyber environment is a set of measures, principles, practices, and technological policies to “protect[2]” individuals and their information assets, reputation, and emotional state in the digital space[3].

Some aspects of human security in the cyber environment, its risks, and protection. Human safety in the cyber environment is a comprehensive concept that encompasses ensuring the physical and psychological well-being of individuals in digital environments, including the Internet, as well as the responsible use of technology. Protecting oneself from the excessive use of technology and its direct and indirect dependence is a crucial aspect of electronic environment security. This problem evolves with the development of technology and requires the joint efforts and policies of individuals, organizations, and governments.

Therefore, ensuring human security in the cyber environment is not only a technical solution, but also an important issue of social relations that requires multi-faceted joint measures such as education, psychology, awareness, knowledge, and legal regulation.

In today's digital era, the risks to human security in the cyber environment are increasing day by day, and their harm is increasing, and they are becoming more complex and integrated.

Here are the most common risks:

✓ Risks related to loss of personal information. Organizations and companies are exposed to the unauthorized collection of user data from big data, application platforms,

[1] About cyber security. Law of Mongolia. December 17, 2021. 4.1.2. Clause in "Cyberspace" means the physical and non-physical domain consisting of the Internet and other information and communication networks and the interdependent complex of information infrastructures that support their operation.

[2] “Dictionary of Communication and Information Technology Terms". SHUTIS, ХМТГ, Universal Duty Fund, MUIS, UB., 2021

[3] National baseline survey report on children's online safety. Telecommunications Regulatory Commission. EMMC LLC.07.09.2020.

and applications in the cyber environment, loss of data integrity, misuse of data, theft of "biometric information[4]" and theft of personal values.

✓ Risks from cyber-attacks. These include software attacks such as electronic device viruses[5], malware[6], ransomware[7], and backdoor attacks[8], and network attacks such as DDoS attacks, network espionage, and man-in-the-middle attacks[9].

✓ Risk of social engineering. In addition to fraud-related attacks, such as phishing and business email scams, designed to trick users into disclosing their personal information, and social manipulation tactics like trust fraud, blackmail, and phishing, there are also other forms of social manipulation.

✓ Social media risk. Cyberbullying includes social relational risks such as discrimination, defamation, and doxing, and psychological risks such as cyber addiction, psychological distress, and negative content effects.

✓ Risks related to fake information and content. It includes risks related to the quality of information, such as fake news[10], misinformation[11], and disinformation[12], and risks related to artificial intelligence technologies, such as fake content created by artificial intelligence, fake profiles, fake images, photos, audio, and video.

✓ Risks faced by children and adolescents. These include child safety risks such as cyber-grooming[13]exposure to pornographic and illegal content, disclosure of personal information, and social development risks such as online bullying, excessive screen dependence, and the negative effects of social media.

✓ Financial risk. It consists of e-fraud and fraud risks such as online shopping fraud, investment fraud and online gaming fraud, and settlement risks such as payment card fraud, online banking fraud, and third-party payment fraud.

✓ Risks related to surveillance in the cyber environment. Risks related to surveillance and espionage, such as big data collection, Internet monitoring, and

[4] About the protection of personal information. Law of Mongolia. December 17, 2021. Clause 4.1.1: non-overlapping physical data related to a person's body, such as fingerprints, iris, face, voice, and body movement characteristics that can be used to identify a person with the help of equipment, hardware, or software.

[5] See reference[4]. Viruses (self-replicating code and attacks that infect files by attaching themselves to clean files and spreading throughout the computer system);

[6] See reference[4]. Malware (malware is usually an easy money-making and political cyber-attack);

[7] See reference[4]. Ransomware (an attack aimed at extorting money from the user by extracting the user's files and data);

[8] See reference[4]. Back door (An attack in which an attacker uses a vulnerability in the network to access the necessary information to damage the server and other things through its users).

[9] See reference[4]. Man-in-the-Middle (a Cyber attack in which a cybercriminal infiltrates the communication between two users and steals information);

[10] See reference[4]. False news (deliberately disseminating completely false information about the relevant subjects and people in the form of official news and information by means of brainwashing or with abstract evidence for the purpose of misleading, concealing the truth, or creating a scandal);

[11] See reference[4]. Misinformation (the process of using true information for other purposes and leading to incorrect conclusions. In some cases, the failure of information integrity is caused by a misunderstanding without a clear intention or purpose.

[12] See reference[4]. Disinformation is false or misleading information deliberately spread to deceive people, or to secure economic or political gain and which may cause public harm.

[13] See reference 4. Cyber grooming is the process of 'befriending' a young person online to facilitate online sexual contact and/or a physical meeting with them to commit sexual abuse.

location tracking, as well as risks to personal freedom, such as profiling and filler bubbles[14].

✓ Technology infrastructure risk. Risks associated with Internet-connected devices include Internet outages, power outages, and vulnerabilities in DNS[15] systems and critical national infrastructure, and vulnerabilities in smart devices.

Because these risks are not mutually exclusive, each country needs to adopt integrated policy solutions to protect human security in the cyber environment.

Ways to protect human security in the cyber environment are defined as follows. It includes:

✓ Technological solutions (Technological development creates risks while opening many new security opportunities. Technologies such as step-by-step electronic authentication, password managers, and cryptographic encryption[16], and virtual private networks (VPNs) [17] will help protect people's personal information.)

✓ Education and knowledge (The most important data for the protection of human electronic security is e-literacy or e-education. When working in an online environment, a person must know how to recognize risks, distinguish harmful content, and protect themselves.)

✓ Personal responsibility (Individuals need to take responsibility for their own cybersecurity. Use secure passwords on electronic devices, regularly update software, and exercise controlled caution when sharing personal information in cyberspace.)

Defining ways to protect human security in the cyber environment will create policy needs and requirements. This is determined by the legal framework, international cooperation and the role of technology companies. Every country urgently needs to create a legal framework suitable for today's digital society. Internationally, the European Union's GDPR[18] has taken a big step towards protecting personal data, but other countries around the world need to adopt similar legislation.

As cybersecurity has become a global issue, transnational international cooperation is of utmost importance. It is necessary to cooperate at the international level in the fight against cybercrime, exchange of information, and the development of common standards through international cooperation. Also, technology companies are responsible for ensuring the security of their platforms and products. They need to take more proactive measures to protect online users' data, monitor harmful content, and detect and stop illegal activities.

---

[14] See reference[4]. Censorship Bubble (a state of intellectual isolation resulting from algorithmic processing in the online digital space that limits an individual's access to the full range of news and other information on the Internet);

[15] See reference[4]. Domain Name System (a hierarchical, decentralized naming system for distinguishing between computers and similar objects connected by Internet Protocol);

[16] See reference[4]. Cryptographic encryption (The process of encoding messages and information that can only be accessed by authorized parties. Encryption makes it impossible to decipher confidential information if you have a special key to keep it secret.

[17] See reference[4]. Virtual Private Network (a technology that creates a secure and encrypted connection over a less secure network, such as the Internet.

[18] See reference[4]. The General Data Protection Regulation (GDPR) defines personal data as any information that identifies a person directly (e.g., name, ID) or indirectly (e.g., location data, online identifier). Data that seems anonymous can be personal if it can be re-identified with other information);

Vol. 25 No 55 (2026) Article

Today's hyper-concentration of social media, uncontrolled widespread use of information networks, false news and forms of manipulation through it are the means of "cyber-slavery" of social communication.

Cyber-slavery is the process of using digital technology to control, exploit, or limit a person's freedom by violating their security. Features of Electronic Slavery:

1. Insensitive service (in the cyber environment, people do not feel that they are losing their personal freedom, space, and time tremendously);

2. Dependence on technology (human life, interpersonal relationships, and daily life decisions are directly dependent on technology, information systems, applications, and the Internet);

3. Data mining (unauthorized collection and use of personal data in the cyber environment);

4. Behavioral control (constantly monitoring people's personal lives and communications with algorithms, restricting their freedom, directly influencing decision-making and habits, and controlling social psychology with fake news).

In modern society, electronic slavery is a violation of human rights through the use of technology and the Internet (restricting personal information and personal space, influencing choices, confusing them and violating rights), establishing social injustice (the excessive concentration of technology and information abuse deepens the gap between social classes, economic and cultural divisions), causing psychological pressure (monitoring people through the Internet, revealing their psychology and thoughts and manipulating them is psychological pressure creating and creating many harmful consequences and risks such as excessive control of social media and electronic platforms negatively affecting the user's self-esteem).

Ending cyber-slavery is a major issue that requires a concerted effort from many countries. For this, it is necessary to implement multifaceted measures such as electronic security, data protection, international cooperation, and legal regulation. Also, citizens' information education, psychological education, ability to use technology, and responsibility will play an important role in stopping electronic slavery.

Research section: In recent years, a significant change has been observed in the social psychology of Mongolia, and the main area for citizens to receive information and express their opinions has become the "cyber environment". The most obvious example of this is the growth in the use of the Facebook platform.

According to data from Meta's advertising tool, as of January 2025, the number of active Facebook users in Mongolia is estimated to be ~2.6 million, which is equivalent to ~74.4% of the total population. In some studies, this number has even reached 3 million. However, according to the data of the National Statistics Committee of Mongolia, the population over 18 years of age is approximately 2.23 million by 2025, which is only 63.5% of the total population. In other words, you see that the number of Facebook users exceeds the number of actual adults. This shows:

- ✓ 18-24 years old ~28.3%;
- ✓ 25–34 years old ~27.6%;
- ✓ 35–44 years old ~19.9%;

- ✓ About 12% of 55-year-olds;
- ✓ Almost no users aged 13–17 (<1,000)

According to the 55 age group, the Facebook platform is the "environment" that most strongly directs the information and opinions of the young people of Mongolia. It can be seen from this that electronic technology platforms are no longer just communication tools, but have turned into information manipulation systems that directly or indirectly affect citizens' opinions, emotions, decision-making, and trust in the government.

In the current state of Mongolia's society, how human security is violated in the cyber environment, and the impact of the risk on people's psychology, opinions, and trust in the government, and the issue of "electronic slavery" have been studied, limited to the space of artificial intelligence and Internet-connected devices.

II. IOT (INTERNET OF THINGS) – IMPACTING HUMAN PERSONAL SPACE

IoT devices are smart devices that can connect to the Internet and exchange information with each other. For example: smart watches, smart refrigerators, cameras, etc. These devices can record and transmit a person's daily behavior, location, and habits.

1. How do Internet-connected devices limit human freedom? Internet-connected devices appear to benefit people's lives, but are actually part of a larger system that limits people's freedom and personal space every day. Smartphones, smart watches, home cameras, smart refrigerators, door locks, and even your car, which people use every day, collect very detailed information about that person. For example, A smart home camera will record who entered and exited when. The smart thermometer "learns" to suggest a mode that matches the rhythm of the home. But that also means he'll learn when there's no one in the house. The smartwatch will also track a person's heart rate, steps, sleep quality, and how they breathe when stressed. All that information is a mirror of the person's body, mind and behavior. This personal data and information are stored on the Internet without the person's knowledge, and in some cases, it is used by third parties, advertising agencies, and government agencies.

Today, people's personal space and way of life are actually under the influence of technological surveillance and control. People may think that they are using technologies "only for their own convenience", but in reality, "people are gradually coming under the control of a comprehensive control system that can collect, store, and monitor all the information of a person's life, and then influence their behavior and important decisions. This is the simplest and most silent way for a person to lose their freedom and become too dependent on it. Smart devices seem to serve people, but in fact, they have become the main means of controlling and controlling people.

2. Hacking and third-party use: The most serious "risk" is that Internet-connected devices become surveillance and spying tools for hackers. These devices are often not well protected. Hackers can easily gain access to devices because users themselves are not knowledgeable enough to change passwords and configure settings. For example, Ring Doorbell, a smart door camera system, was hacked by many users in 2020. According to some users, the hackers were able to view the camera footage, talk to the

children through the microphone, make threats, and listen to the internal affairs of the family. In addition, many Internet-connected device manufacturers sell human data to third parties and use it for advertising. Users agree, but no one reads the terms and conditions. In this way, information about a person's home, habits, health, and location is turned into a business weapon and used.

III. Artificial Intelligence – Impact On Human Psychology:

Artificial intelligence is a system that mimics the human mind and is capable of self-learning and decision-making. It can analyze data using artificial intelligence algorithms, make human-like predictions, make recommendations, and influence psychology. Examples: Facebook News Feed, YouTube Video Recommendations, ChatGPT, etc.

Psychological Algorithms:

Artificial intelligence is a powerful algorithm that affects not only the actions of people on the Internet, but also their emotions, thoughts, beliefs, and decision-making processes. This effect takes place very quietly and imperceptibly, and is controlled by a person without his knowledge. Platforms like Facebook, TikTok, YouTube, and Instagram that people use every day use artificial intelligence algorithms to select the information to be displayed in front of them. A person may think that they are selecting and considering this information themselves, but in reality, artificial intelligence is doing the decision-making and thinking on behalf of the person. Artificial intelligence models psychology and behavior by studying content that people have previously been interested in, likes, comments, keywords, and things that have been viewed longer on the screen. Based on this, it offers you the most engaging and attention-grabbing content.

So what are the results for that person?

- ✓ Chances of one's opinion becoming one-sided;
- ✓ The opportunity to access balanced information of opposite opinions and facts will decrease.
- ✓ Even if a person thinks that he is making a choice, that choice has already been made by artificial intelligence.

1. Deepfake technology: Deepfake technology is blurring the lines between truth and falsehood. Deepfake is a technology that uses artificial intelligence to create fake videos, audio, and images that mimic human faces and voices. Everyone can get an artificial persona with a deepfake. The use of this technology for political, criminal, and personal reputation attacks is on the rise, and it is becoming increasingly challenging to distinguish between truth and falsehood. The result of this:

- ✓ Dissemination of fake recordings and voices will affect public confidence.
- ✓ Slander, intimidate, or mislead the public for political or business purposes;

2. Emotional analysis: Modern artificial intelligence systems can understand not only what the person is watching, but also what emotions they are feeling at that moment. For example, TikTok and Instagram Reels analyze the types of videos people spend more time on and the content they watch at specific times. Artificial intelligence

suggests content that resonates more with people when they're lonely, sad, or stressed. Repeatedly, people face the risk of becoming addicted to the platform, information overload, low self-confidence, and poor psychological health. The result of this:

✓ Humans feel as if they are in control, but in reality, artificial intelligence is guiding the human mind;

✓ Feelings of depression, loneliness, and self-blame increase tremendously;

3. Choice Manipulation: From shopping, travel planning, political choices, and even who to be friends with, AI predicts human decisions and shows the most likely choices closer to humans.

IV. RESULT

AI (Artificial Intelligence) IoT(Internet of Things) = Society in Glass. "Society in Glass" allows the state, government organizations, the private sector, and individuals to control all aspects of human freedom, personal space, psychology, and thoughts. Our lives may appear to be "free" in the traditional sense, but in fact, we are slowly moving into "life under a glass" (dependent on someone else).

Social Credit System (China) – a real example of IoT AI combined control: China's "Social Credit System" is a system that uses internet-connected devices, surveillance cameras, and artificial intelligence to give points to the actions and maturity of citizens and evaluate social freedom. More than 20 million cameras combined with artificial intelligence deployed throughout the city record citizens' movements, interactions, purchases, payments, and electronic communications and send them to a central server. AI then analyzes this data to determine if it is a good citizen or a "suspicious person." The following measures are taken by measuring them with points. It includes:

✓ Points will be deducted for littering in public places.

✓ In case of violations of the law, the right to travel abroad will be restricted;

✓ If you have a bad social score, you will not be able to send your child to a good school or get a job;

Cambridge Analytica – used AI to manipulate psychology and change elections. Cambridge Analytica is a real-life case where Facebook collected the personal data of 50 million users without their consent, used artificial intelligence to model their psychological types, and directly influenced the results of political elections.

The company classified each user into psychological types such as "trusting", "timid", "angry", "vulnerable", etc., and sent political ads, information and content tailored to each of them. As a result, a lot of people voted not based on their own thoughts and beliefs, but based on AI-adjusted content.

It is also the clearest example of how human opinions and choices can be controlled based on artificial intelligence algorithms and information dissemination. This is an issue that affects the independence and national security of the respective countries.

CONCLUSION

As advanced technologies such as artificial intelligence and Internet-connected devices are used as social control and information manipulation tools, human rights, freedom, national sovereignty, and national security are facing a new generation of challenges. Examples such as China and Cambridge Analytica show that the misuse of this technology can have a profound impact not only on the country itself, but also on democratic values, international relations and trust in the world.

The above study shows that the concept of "electronic slavery" has turned into a new type of social control system of the 21st century with the rapid development of artificial intelligence and Internet-connected devices. The main feature is that it is based on "human natural data and subconsciousness" and not on coercion or violence.

Considering the electronic use of the entire population of Mongolia, the excessive dependence on electronic technology and the one-flow state of information have a great impact on the public opinion, and it seems that they have a huge database, but in reality, citizens are guided by uncontrolled information and turn into a "conscious automatic response" unit, which is a manifestation of psychological dependence.

Let's say the AI knows what you watch, and the AI knows what you do.

So one question is very important. Who controls what we think? Who needs it and why? *Opinions, beliefs, feelings, decisions* — these should be the most important and highest level of freedom of the individual, but today they are used as data and become the "key" of the system.

In today's Mongolian society, public trust in the government has decreased dramatically, and mistrust prevails. It is not enough to link this phenomenon only to political decisions and economic crisis. Today, when the main space for determining people's thoughts, opinions, and psychology has turned into the cyber environment, the underlying cause of this attitude is the problem of inseparably connecting with the system of "electronic slavery" based on "artificial intelligence" and "things connected to the Internet".

Citizens of Mongolia today are not under the shadow of the government, but under the shadow of the electronic control system, and are losing their psychological freedom day by day. Therefore, although the government and administration of the country may have made real mistakes in the problems faced by the country, the above research shows that the reason for the great frustration of the citizens may be the flow of negative information created by artificial intelligence and electronic platforms, and the psychological manipulation of society.

It is important to develop legal regulations and policies that protect human rights and security at the level of society and the country.

REFERENCES

[1] Protection of personal information. Law of Mongolia. December 17, 2021. Clause 4.1.11. Clause 4.1.1

[2] About cyber security. Law of Mongolia. December 17, 2021. Clause 4.1.3

[3] National Statistics Committee. (2024). Number and structure of the population of Mongolia (estimated in 2025). http://www.nso.mn

[4] Meta Ads Manager (2024). Mongolia Audience Insights – Facebook Ads Reach Data. https://adsmanager.faceb List of sources and research papers citedook.com

[5] Erdenetsogt, S. (2024). Issues of legal regulation in the cyber environment of Mongolia. Rule of Law, 38(1), 22-37

[6] Galbadrakh, L. & Naranbaatar, M. (2023). A study of the legal environment of cybersecurity in Mongolia. Legal Studies, 25(3), 112-127

[7] Jargalsaikhan, D. & Munkhbat, O. (2024). Security challenges in the era of digital transition. Bulletin of the Mongolian Academy of Sciences, 62(1), 45-57

[8] Sodnomdarjaa, T. (2024). Technological solutions for personal information protection in the cyber environment. Mongolian Journal of Information Technology, 16(1), 88-102

[9] Erdenebayar, B. (2022). Ways to protect personal information in the cyber environment. Proceedings of the Days of the Academy of Sciences, Mongolian University of Science and Technology, 345-358

[10] "Dictionary of communication and information technology terms". Mongolian Academy of Sciences, baseline research report. Telecommunications Regulatory Commission. MMCG LLC. 2020.07.09

[11] Galbadrakh, L. & Naranbaatar, M. (2023). Mongol ulsyn tsakhim ayuulgüi baidlyn erkh züin orchny sudalgaa. Khuuli züin sudlal, 25(3),

[12] Galbadrakh, L. & Naranbaatar, M. (2023). A study of the legal environment of cybersecurity in Mongolia. Legal Studies, 25(3), 112-127

[13] Gerelchimeg. K. (2024). The negative impact of electronic information on society and ways to reduce it" doctoral dissertation. 33 pages.

[14] Jargalsaikhan, D. & Munkhbat, O. (2024). Security challenges in the era of digital transition. Bulletin of the Mongolian Academy of Sciences, 62(1), 45-57

[15] Sodnomdarjaa, T. (2024). Technological solutions for personal information protection in the cyber environment. Mongolian Journal of Information Technology, 16(1), 88-102

[16] Erdenebayar, B. (2022). Ways to protect personal information in the electronic environment. Proceedings of the Academy of Sciences Employee Days, National University of Mongolia, 345-358

[17] "Dictionary of communication and information technology terms". National University of Mongolia, National University of Mongolia, 2021

[18] National baseline survey report on child safety in cyberspace. Telecommunications Regulatory Commission. MMCG LLC. 2020.07.09

[19] Cambridge Dictionary. (n.d.). Manipulation. In the Cambridge English Dictionary. Cambridge University.
Press. https://dictionary.cambridge.org/us/dictionary/english/manipulation

[20] Zuboff, Shoshana. (2019). The Age of Surveillance Capitalism. Public Affairs Publishing. "Surveillance capitalism, AI + data governance, and the impact on human freedom"

[21] Wired Magazine. (2023). "Tesla remotely disables features of cars without the owner's consent". https://www.wired.com

[22] 2 MIT Technology Review. (2022). "Deepfakes and the threat to reality". https://www.technologyreview.com
[23] Netflix Documentary. (2020). "The Social Dilemma"
[24] European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape Report 2023*. Luxembourg: Publications Office of the European Union.
[25] International Telecommunication Union (ITU). (2023). *Global Cybersecurity Index 2023*. Geneva: ITU Publications
[26] Pew Research Center. (2023). *Digital Privacy Concerns and Attitudes: A Global Survey*. Washington, DC: Pew Research Center
[27] United Nations Office on Drugs and Crime (UNODC). (2023). *Global Report on Cybercrime 2023*. Vienna: United Nations Publications

ЦАХИМ ОРЧИН ДАХЬ ХҮНИЙ АЮУЛГҮЙ БАЙДАЛ: ЭРСДЭЛ, ХАМГААЛАЛТ, БОДЛОГЫН ХЭРЭГЦЭЭ

Калийнаа Гэрэлчимэг[1]
Доктор (Ph.D), Судалгаа хөгжүүлэлтийн мэргэжилтэн,
Үндэсний Батлан Хамгаалахын Их Сургууль, Монгол Улс
kgerelchimegk@gmail.com, ORCID: 0009-0007-5210-4601

Дэмбэрэл Идэшноров[2]
Доктор (Ph.D), Эрдэм шинжилээ, инновацын хэлтсийн дарга,
Үндэсний Батлан Хамгаалахын Их Сургууль, Монгол Улс
ideshnorov1919@gmail.com

Отгонбаяр Цогзолбоо[3]
Багш,
Үндэсний Батлан Хамгаалахын Их Сургууль, Монгол Улс
Temuulenmgl3@gmail.com

Чинбат Энхбаатар[4]
Ахлах багш,
Цэргийн нэгдсэн сургууль,
Үндэсний Батлан Хамгаалахын Их Сургууль, Монгол Улс
chinbatenhbaatar931@gmail.com

Хураангуй: Хүн төрөлхтний амьдралд техник, технологийн дэвшил хиймэл оюун (AI), интернетэд холбогдсон төхөөрөмжүүд (IoT) олон сайхан боломжийг бий болгож байгаа ч, бодит байдал дээр технологиор дамжуулан "хүний хувийн мэдээлэл[19]"-ийг цуглуулж, тэдний бодол, үйлдэл, амьдралын хэв маягт нөлөөлөн,

[19] Хүний хувийн мэдээлэл хамгаалах тухай. Монгол Улсын хууль. 2021 оны 12 дугаар сарын 17-ны өдөр. 4.1.11 дэх заалт. "хүний хувийн мэдээлэл" гэж хүний эмзэг мэдээлэл болон хүний эцэг /эх/-ийн нэр, өөрийн нэр, төрсөн он, сар, өдөр, төрсөн газар, оршин суугаа газрын хаяг, байршил, иргэний бүртгэлийн дугаар, хөрөнгө, боловсрол, гишүүнчлэл, цахим тодорхойлогч, хүнийг шууд болон шууд бусаар тодорхойлох, эсхүл тодорхойлох боломжтой бусад мэдээллийг;

Vol. 25 No 55 (2026) Article

эрх чөлөөг хязгаарлаж, шүүмжлэлтэй сэтгэх чадварыг алдагдуулах эрсдэлийг дагуулж байна. Энэ нь технологи ашиг лан цахим орчинд хүний аюулгүй байдалд халдаж, түүнийг хяналтандаа авах, мөлжих, эрх чөлөөг нь хязгаарлах үйл явц “цахим боолчлол”-ыг бий болгож байна. Цаашлаад хүний амьдрах болон нийгмийн харилцааны бүхий л үйл явц хиймэл оюун, интернетэд холбогдсон төхөөрөмжүүдийн хяналтын системээр удирдагдах маш хортой үр дагаварт хүрч болзошгүй байна.

Иймд өнөөгийн нийгэмд цахим орчин дахь хүний аюулгүй байдлын асуудал нь зөвхөн технологиос хамааралтай асуудал биш, нийгэм, эдийн засаг, сэтгэл зүй, хууль эрх зүй, боловсрол зэрэг олон талын хүчин чармайлтыг шаардах цогц асуудал болсон. Цахим орчныг илүү аюулгүй, найдвартай болгохын тулд улс орны засгийн газар, технологийн компаниуд, иргэний нийгэм болон хувь хүмүүс хамтран ажиллах зайлшгүй шаардлагатай байна.

Түлхүүр үг: Цахим орчин, IoT (интернетэд холбогдсон төхөөрөмж), AI (хиймэл оюун), хүний хувийн мэдээлэл, хяналт, манипуляц, алгоритм, цахим боолчлол, шилэн доторх нийгэм.

I. Үндсэн хэсэг

Хүн төрөлхтний өдөр тутмын амьдрал, нийгмийн харилцааны асуудал технологиос шууд хамааралтай болж, цахим орчин хүний амьдралын салшгүй нэг хэсэг болжээ. Цахим орчин хөгжихийн хэрээр хүний нэр төр, эрх чөлөө, нийгмийн байр суурийг хадгалах асуудалд хүндрэл үүсэж олон төрлийн “эрсдэл[20]”-ийг дагуулж байна. Цахим орчин дахь хүний аюулгүй байдал нь дижитал орчинд хувь хүн болон түүний мэдээлэл, хөрөнгө, нэр хүнд, сэтгэл санааны байдлыг хамгаалах арга хэмжээ, зарчим, дадал, технологи болон бодлогын цогц арга хэмжээ юм[21].

Цахим орчин дахь хүний аюулгүй байдал: эрсдэл, хамгаалалт, бодлогын хэрэгцээ**.** Цахим орчин дахь хүний аюулгүй байдал гэдэг нь дижитал орчин, интернет болон технологийн хэрэглээнд хүний биеийн болон сэтгэл зүйн аюулгүй байдлыг хангахтай холбоотой цогц ойлголт юм. Хүн өөрөө өөрийгөө технологийн хэт их хэрэглээ, түүний шууд болон шууд бус хамааралд автахаас хамгаалах нь цахим орчны аюулгүй байдлын хамгийн чухал хэсэг бөгөөд энэхүү асуудал нь технологийн хөгжилтэй хамт хувьсан өөрчлөгдөж, хувь хүн, байгууллага, төр засгаас тэдний хамтын хүчин чармайлт, бодлогын хэрэгцээг шаардаж байна.

Иймд цахим орчин дахь хүний аюулгүй байдлыг хангах нь зөвхөн техникийн шийдэл төдийгүй боловсрол, сэтгэл зүй, ухамсар, мэдлэг, хууль эрх зүйн нэгдсэн зохицуулалт зэрэг олон талт-хамтын арга хэмжээг шаардах нийгмийн харилцааны чухал асуудал болсон байна.

Өнөөгийн дижитал эрин үед цахим орчин дахь хүний аюулгүй байдалд учрах эрсдэл өдрөөс өдөрт улам бүр нэмэгдэж, хор уршиг нь ихсэж, нарийн, нэгдсэн

[20] “Харилцаа холбоо, мэдээллийн технологийн нэр томъёоны толь бичиг”. ШУТИС, ХХМТГ, Бүх нийтийн үүргийн сан, МУИС, УБ., 2021

[21] Цахим орчин дахь хүүхдийн аюулгүй байдлын талаар үндэсний суурь судалгааны тайлан. Харилцаа холбооны зохицуулах хороо. Эм Эм Си Жи ХХК. 2020.07.09;

зохион байгуулалттай болж байна. Үүнээс хамгийн түгээмэл илэрч буй эрсдэлүүдийг авч үзвэл:

Хүний хувийн мэдээллийн алдагдалтай холбоотой эрсдэл. Байгууллага, компаниуд цахим орчин дахь их өгөгдөл, хэрэглээний платформ, аппликейшнүүдээс хэрэглэгчийн мэдээллийг зөвшөөрөлгүй цуглуулах, өгөгдлийн бүрэн бүтэн байдлыг алдагдах, мэдээллийг буруу зориулалтаар ашиглах зэрэг хэлбэрээр илэрч, “биометрик мэдээлэл[22]”-ийн хулгай болон хувийн үнэт зүйлсийн хулгайд хүргэж байна.

Кибер халдлагаас үүдэлтэй эрсдэл. Цахим төхөөрөмжийн virus[23], malware[24], ransomware[25], backdoor[26] халдлага зэрэг программ хангамжийн халдлагууд болон DDoS халдлага, сүлжээний тагнуул, man-in-the-middle[27] халдлага зэрэг сүлжээний халдлагууд багтана.

Сошиал инженерчлэлийн эрсдэл. Цахим орчинд хэрэглэгчдийг хуурч мэхлэн тэдний хувийн мэдээллийг олж авах зорилготой фишинг халдлага, хууран мэхлэх, бизнесийн е-мэйлийн луйвар зэрэг хууран мэхлэлттэй холбоотой халдлагуудаас гадна итгэл олж аван залилах, шантаажлах, таамаглалд суурилсан халдлага зэрэг нийгмийн манипуляциуд багтана.

Нийгмийн сүлжээний эрсдэл. Цахим орчны дээрэлхэлт гадуурхал, хүний нэр хүндэд халдах, доксинг зэрэг нийгмийн харилцааны эрсдэлүүд болон цахим донтолт, сэтгэл зүйн дарамт, контентын сөрөг нөлөө зэрэг сэтгэл зүйн эрсдэлийг агуулна.

Хуурамч мэдээлэл, контенттой холбоотой эрсдэл. Fake news [28], misinformation[29], disinformation[30] зэрэг мэдээллийн чанартай холбоотой эрсдэлүүд болон хиймэл оюунаар үүсгэсэн хуурамч контент, хуурамч профайл, хуурамч дүрс, зураг, аудио, видео зэрэг хиймэл оюуны технологитой холбоотой эрсдэлүүд багтаана.

---

[22] Хүний хувийн мэдээлэл хамгаалах тухай. Монгол Улсын хууль. 2021 оны 12 дугаар сарын 17-ны өдөр. 4.1.1 дэх заалт: тоног төхөөрөмж, техник хэрэгсэл, программ хангамжийн тусламжтайгаар хүнийг тодорхойлох боломжтой гарын хурууны хээ, нүдний солонгон бүрхэвч, нүүр царай, дуу хоолой, биеийн хөдөлгөөний онцлог шинж зэрэг хүний бие махбодтой холбоотой биеийн давхцахгүй өгөгдлийг;

[23] Эш[4] үз. Вирус (өөрийгөө хувилдаг код ба цэвэрхэн файл дээр наалдаж улмаар компьютер систем даяар тархаж файл хордуулдаг халдлага);

[24] Эш[4] үз. Майлвэр (хортой программ нь ихэвчлэн амархан мөнгө олох болон улс төрийн чанартай кибер халдлага);

[25] Эш[4] үз. Рансомвэр (Хэрэглэгчийн файл болон мэдээлэл тусгаарлаж хэрэглэгчээс мөнгө нэхэх зорилготой халдлага);

[26] Эш[4] үз. Арын хаалга (Халдагч этгээд сүлжээний эмзэг байдлийг ашиглан түүний хэрэглэгчдээр дамжуулан сервер болон бусад зүйлсийг бусниулах хэрэгтэй мэдээлэлдээ хандаж хэрэгтэй мэдээллээ олж авах халдлага);

[27] Эш[4] үз. Дундын хүн (Кибер гэмт хэрэгтэн хоёр хэрэглэгчийн харилцаанд нэвтрэж мэдээлэл хулгайлах кибер халдлага);

[28] Эш[4] үз. Худал мэдээ (Холбогдох субьект, хүмүүсийн талаар огт худал зүйлийг хуурч төөрөгдүүлэн, үнэнийг нуун дарагдуулах, дуулиан тарих зорилгоор “тархи угаалт”-ын аргаар буюу хийсвэр нотолгоотойгоор боловсруулж, албан ёсны мэдээ, мэдээлэл хэлбэрээр зориудаар тараах);

[29] Эш[4] үз. Ташаа мэдээлэл (Үнэн мэдээллийг өөр зорилгоор ашиглаж, буруу дүгнэлтэд хүргэх үйл явц. Зарим тохиолдолд тодорхой санаа, зорилгогүйгээр эндүүрч ташаарснаас үүдсэн мэдээллийн бүрэн бүтэн байдлын доголдол);

[30] Эш[4] үз. Хуурамч мэдээлэл (Санаатайгаар, бусдыг хууран мэхлэх зорилготойгоор үүсгэсэн хуурамч мэдээлэл);

Vol. 25 No 55 (2026) Article

Хүүхэд, өсвөр насныханд тулгарах эрсдэл. Цахим үс засалт[31], садар самуун, хууль бус +18 агуулгатай контентод өртөх, хувийн мэдээллийн ил тод байдал зэрэг хүүхдийн аюулгүй байдлын эрсдэлүүд болон онлайн дээрэлхэлт, хэт их дэлгэцийн хамаарал, нийгэм цахим мэдээллийн үзүүлэх сөрөг нөлөө[32] зэрэг нийгмийн хөгжлийн эрсдэлүүд орно.

Санхүүгийн эрсдэл. Онлайн худалдааны залилан, хөрөнгө оруулалтын луйвар, онлайн тоглоомын залилан зэрэг цахим залилан, луйварын эрсдэлүүд болон төлбөрийн картын залилан, онлайн банкны залилан, гуравдагч талын төлбөрийн залилан зэрэг төлбөр тооцооны эрсдэлүүдээс бүрддэг.

Цахим орчин дахь хяналттай холбоотой эрсдэл. Их өгөгдөл цуглуулалт, интернэт хяналт, байршил тагнах зэрэг хяналт, тагнуултай холбоотой эрсдэлүүд мөн профайлинг, filler bubble[33] зэрэг хүний хувийн орон зайн эрх чөлөөний эрсдэлүүд орно.

Технологийн дэд бүтцийн эрсдэл. Интернэт тасалдал, цахилгаан тасралт, DNS[34] системийн болон улс орны чухал дэд бүтцийн эмзэг байдал, ухаалаг төхөөрөмжийн эмзэг байдал зэргийн хяналтыг алдагдуулах интернетэд холбогдсон төхөөрөмжүүдтэй холбоотой эрсдэлүүд багтана.

Эдгээр эрсдэлүүд нь дангаараа бус харилцан бие биенээсээ хамааралтай байдаг тул цахим орчин дахь хүний аюулгүй байдлыг хамгаалахад улс орон бүр бодлогын нэгдсэн шийдлүүдийг авч хэрэгжүүлэх шаардлагатай байна.

Цахим орчин дахь хүний аюулгүй байдлыг хамгаалалтын арга замуудыг дараах байдлаар тодорхойлно. Үүнд:

- ✓ Технологийн шийдлүүд (Технологийн хөгжил эрсдэлийг бий болгохын зэрэгцээ хамгаалалтын олон шинэ боломжуудыг нээж байна. Цахим технологийн үе шаттай баталгаажуулалт, нууц үгийн менежер, криптограф шифрлэлт[35], хувийн виртуал сүлжээ[36] (VPN) зэрэг технологи нь хүний хувийн мэдээллийг хамгаалахад тусална.)

---

[31] Эш[4] үз. Цахим үс засалт (Цахим орчинд насанд хүрсэн этгээд хүүхдийн итгэлийн олж аван улмаар түүнтэй найз, нөхдийн дотно харилцааг бий болгосны дараа хүүхдийг садар самуун үйл хэрэгт ашиглах зорилго агуулсан үйлдэл);

[32] Гэрэлчимэг. К. (2024). Нийгэмд цахим мэдээллийн үзүүлэх сөрөг нөлөө, түүнийг бууруулах арга зам” докторын диссертацын ажил. х33. Тодорхойлолт: Нийгэмд цахим мэдээллийн үзүүлэх сөрөг нөлөө нь үндэсний эв нэгдэл, нийгмийн тогтвортой байдлыг хангахад нийгмийн субъект (хувь хүн, гэр бүл, хамт олон, улс төрийн байгууллагууд, нийгмийн бүлэг)-ын эрх, эрх чөлөө, хууль ёсны ашиг сонирхолд харилцаа холбоо, мэдээллийн технологийн хэрэгслийг ашиглан хэм хэмжээг зөрчих, нөлөөлөх, ашиглах, хамгаалалтыг алдагдуулахад чиглэсэн үйлдэл.

[33] Эш[4] үз. Шүүлтийн бөмбөлөг (Хувь хүний интернет дэх мэдээ болон бусад мэдээллийг бүрэн хэмжээгээр авах боломжийг хязгаарласан онлайн дижитал орон зайд алгоритмын боловсруулалтын үр дүнд бий болсон оюуны тусгаарлагдсан төлөв);

[34] Эш[4] үз. Домэйн нэрийн систем (Интернэт протоколоор холбоотой байгаа компьютер болон түүнтэй адилтгах зүйлсийг хооронд нь ялгах зориулалттай, шаталсан, төвлөрсөн бус нэрийн систем);

[35] Эш[4] үз. Криптографийн шифрлэлт (Зөвхөн эрх бүхий талуудад хандах боломжтой мессеж, мэдээллийг кодлох үйл явц. Шифрлэлт нь мэдээллийг нууцлах тусгай түлхүүртэй бол нууц мэдээллийг задлах боломжгүй болгодог).

[36] Эш[4] үз. Виртуал хувийн сүлжээ (Интернет гэх мэт хамгаалалт багатай сүлжээгээр аюулгүй, шифрлэгдсэн холболт үүсгэдэг технологи;

- ✓ Боловсрол ба мэдлэг (Хүний цахим аюулгүй байдлын хамгаалалтын хамгийн чухал өгөгдөл бол цахим бичиг үсгийн боловсрол буюу цахим боловсрол юм. Хүн цахим орчинд ажиллахдаа эрсдэлийг таних, хортой контентыг ялгах, өөрсдийгөө хамгаалах арга замуудыг зайлшгүй мэддэг байх шаардлагатай.)
- ✓ Хувийн хариуцлага (Хувь хүн өөрийн цахим аюулгүй байдлаа хангахад хариуцлагатай хандах шаардлагатай. Цахим хэрэгсэлдээ аюулгүй нууц үг хэрэглэх, программ хангамжийг тогтмол шинэчлэх, цахим орчинд хувийн мэдээллээ хуваалцахдаа хяналттай болгоомжтой хандах хэрэгтэй.)

Цахим орчин дахь хүний аюулгүй байдлыг хамгаалалтын арга замыг тодорхойлсоноор бодлогын хэрэгцээ, шаардлага бий болно. Үүнийг хууль эрх зүйн орчин, олон улсын хамтын ажиллагаа, технологийн компаниудын гүйцэтгэх үүргээр тодорхойлдог. Улс орон бүр өнөөгийн дижитал нийгэмд тохирсон хууль эрх зүйн орчинг нэн даруй бүрдүүлэх шаардлагатай байна. Олон улсад Европын холбоо GDPR[37] нь хүний хувийн мэдээллийг хамгаалах чиглэлээр томоохон алхам хийсэн боловч үүнтэй адил хууль тогтоомжийг дэлхийн бусад улс орнууд баталж хэрэгжүүлэх шаардлагатай байгаа юм.

Цахим аюулгүй байдал нь дэлхий нийтийн асуудал болсон тул үндэстэн дамнасан олон улсын хамтын ажиллагаа хамгийн чухал байр суурийг эзэлж байна. Олон улсын хамтын ажиллагаагаар кибер гэмт хэрэгтэй тэмцэх, мэдээлэл солилцох, нэгдсэн стандарт боловсруулах чиглэлээр олон улсын түвшинд хамтран ажиллах хэрэгтэй юм. Мөн технологийн компаниуд өөрсдийн платформ, бүтээгдэхүүний аюулгүй байдлыг хангаж ажиллах үүрэгтэй. Тэд цахим хэрэглэгчдийн мэдээллийг хамгаалах, хортой контентыг хянах, хууль бус үйл ажиллагааг илрүүлэх, таслан зогсоох зэрэг чиглэлээр илүү идэвхтэй арга хэмжээ авах шаардлагатай байна.

Өнөөгийн нийгмийн мэдээллийн хэт төвлөрөл, мэдээллийн сүлжээний хяналтгүй өргөн хэрэглээ, түүгээр дамжих худал мэдээ болон манипуляцийн хэлбэрүүд нь нийгмийн харилцааны “цахим боолчлол”-ын арга хэрэгсэл юм.

Цахим боолчлол гэдэг нь дижитал технологи ашиглан хүний аюулгүй байдлыг зөрчин хяналтдаа авах, мөлжих, эрх чөлөөг нь хязгаарлах үйл явц юм.

Цахим боолчлолын онцлог:

1. Мэдрэхгүй үйлчлэл (цахим орчинд хүмүүс өөрсдийн хувийн эрх чөлөө, орон зай, цаг хугацаагаа асар ихээр алдаж байгаагаа мэдрэхгүй байх);
2. Технологийн хамаарал (хүний амьдрал, хоорондын харилцаа, өдөр тутмын амьдралын шийдвэр гаргалт техник технологи, мэдээллийн систем, аппликейшн, интернэтээс шууд хамааралтай болох);
3. Өгөгдлийн олборлолт (цахим орчинд хүний хувийн өгөгдлийг зөвшөөрөлгүйгээр цуглуулж, ашиглах);

[37] Эш[4] үз. Өгөгдөл хамгааллын ерөнхий журам (General Data Protection Regulation нь хувийн мэдээллийг тухайн хүнийг шууд (нэр, ID) эсвэл шууд бусаар (байршлын өгөгдөл, онлайн танигч) тодорхойлох аливаа мэдээлэл гэж тодорхойлдог. Нэргүй мэт санагдах өгөгдөл нь бусад мэдээлэлтэй дахин танигдаж чадвал хувийн шинж чанартай байж болно);

4. Зан үйлийн хяналт (хүмүүсийн хувийн амьдрал, харилцаа холбоог алгоритмаар байнга хянаж, эрх чөлөөг нь хязгаарлах, шийдвэр гаргалт, дадал зуршилд шууд нөлөөлөх, хуурамч мэдээгээр нийгмийн сэтгэл зүйг удирдах) зэрэг юм.

Орчин үеийн нийгэмд цахим боолчлол технологи, интернетийн хэрэглээгээр дамжуулан хүний эрхийн зөрчих (хувь хүний мэдээлэл, хувийн орон зайг хязгаарлан, сонголтонд нөлөөлж, тэднийг төөрөгдөлд оруулж, эрхийг зөрчиж байна), нийгэмд шударга бус байдал тогтоох (технологийн хэт төвлөрөл, мэдээллийн хүчирхийлэл нь нийгмийн давхаргын хоорондын ялгааг улам нэмэгдүүлж, эдийн засгийн болон соёлын хуваагдлыг гүнзгийрүүлж байна), хүнд сэтгэлзүйн дарамт учруулах (хүмүүсийг цахим орчинд хянах замаар тэдний сэтгэлзүй, бодол санааг илрүүлж, манипуляц хийх нь сэтгэлзүйн дарамт үүсгэж, сошиал медиа, цахим платформын хэт хяналт хэрэглэгч өөрийгөө үнэлэх чадварт сөргөөр нөлөөлж байна) зэрэг олон хортой үр дагавар, эрсдэлийг бий болгож байна.

Цахим боолчлолыг зогсоох нь улс орны хувьд олон талын нэгдсэн хүчин чармайлт шаардах томоохон асуудал юм. Үүний тулд цахим аюулгүй байдал, мэдээллийн хамгаалалт, олон улсын хамтын ажиллагаа, хуулийн зохицуулалт зэрэг олон талт арга хэмжээг хэрэгжүүлэх шаардлагатай байна. Мөн иргэдийн мэдээллийн боловсрол, сэтгэлзүйн боловсрол, технологи ашиглах чадвар, хариуцлагатай байдал зэрэг нь цахим боолчлолыг зогсооход чухал үүрэг гүйцэтгэнэ.

II. СУДАЛГААНЫ ХЭСЭГ

Сүүлийн жилүүдэд Монгол Улсын нийгмийн сэтгэл зүйд мэдэгдэхүйц өөрчлөлт ажиглагдаж байгаа бөгөөд иргэдийн мэдээлэл хүлээн авах, үзэл бодол илэрхийлэх гол тал_бар нь “цахим орчин” болсон. Үүнийг илтгэх хамгийн тод жишээ бол Facebook платформын хэрэглээний өсөлт юм.

Мета (Meta) компанийн зар сурталчилгааны хэрэгслийн мэдээллээр 2025 оны 1-р сарын байдлаар Монгол Улсад Facebook-ийн идэвхтэй хэрэглэгчийн тоо ~2.6 сая хэмээн тооцоологдсон нь нийт хүн амын ~74.4%-тай тэнцэж байгаа юм. Зарим судалгаанд энэхүү тоо бүр 3 саяд хүрсэн гэх үзүүлэлт ч байгаа юм. Гэтэл Монгол Улсын Үндэсний статистикийн хорооны мэдээллээр 2025 оны байдлаар 18-аас дээш насны хүн ам ойролцоогоор ~2.23 сая бөгөөд энэ нь нийт хүн амын ~63.5%-ийг л бүрдүүлж байна. Өөрөөр хэлбэл, Facebook хэрэглэгчдийн тоо бодит насанд хүрэгчдийн тооноос давж гарч байгааг та харж байна. Үүнийг харуулбал:

- ✓ 18–24 насныхан ~28.3%;
- ✓ 25–34 насныхан ~27.6%;
- ✓ 35–44 насныхан ~19.9%;
- ✓ Харин 55+ насныхан нийлээд ~12% орчим;
- ✓ 13–17 насны хэрэглэгч бараг байхгүй (<1,000)

55+ насны ангилалаас үзвэл Facebook платформ Монгол Улсын нийгмийн залуу үеийн мэдээлэл, үзэл бодлыг хамгийн хүчтэй чиглүүлж буй “орчин” гэдгийг илтгэж байна. Эндээс харахад цахим технологийн платформууд зөвхөн харилцаа

холбооны хэрэгсэл байхаа больж, иргэдийн үзэл бодол, сэтгэл хөдлөл, шийдвэр гаргалт, төрд итгэх хандлагад шууд болон шууд бусаар нөлөөлж буй мэдээллийн манипуляцийн систем болон хувирсан байж болзошгүй нөхцөл байдал үүсээд байна.

Өнөөгийн Монгол Улсын нийгмийн өнөөгийн байдалд цахим орчин дахь хүний аюулгүй байдал хэрхэн зөрчигдөж, түүнээс учрах эрсдэл ард иргэдийн сэтгэл зүй, үзэл бодол, төрд итгэх итгэлд ямар их нөлөө үзүүлж “цахим боолчлол”-д орж байгаа асуудлыг хиймэл оюун, интернетэд холбогдсон төхөөрөмжийн орон зайн хүрээгээр хязгаарлан авч үзэж судаллаа.

III. IOT (ИНТЕРНЕТЭД ХОЛБОГДСОН ЗҮЙЛС) – ХҮНИЙ ХУВИЙН ОРОН ЗАЙД НӨЛӨӨЛӨХ НЬ

IoT нь интернетээр холбогдож, өөр хоорондоо мэдээлэл солилцох чадвартай ухаалаг төхөөрөмжүүд юм. Жишээлбэл: ухаалаг цаг, ухаалаг хөргөгч, камерууд гэх мэт. Эдгээр төхөөрөмжүүд хүний өдөр тутмын зан үйл, байршил, зуршлыг бүртгэж, дамжуулж чаддаг.

1. Интернетэд холбогдсон төхөөрөмжүүд хүний эрх чөлөөг хэрхэн хязгаарладаг вэ? Интернетэд холбогдсон төхөөрөмжүүд хүний амьдралд ашиг тусаа өгч байгаа мэт харагддаг ч үнэн хэрэгтээ хүний эрх чөлөө, хувийн орон зайг өдөр бүр хязгаарлаж байдаг маш том системийн нэг хэсэг юм. Хүний өдөр тутмын хэрэглэдэг ухаалаг утас, ухаалаг цаг, гэрийн камерууд, ухаалаг хөргөгч, хаалганы түгжээ, тэр ч байтугай автомашин чинь хүртэл тухайн хүний талаар маш нарийн мэдээлэл цуглуулж байдаг. Жишээ нь: Ухаалаг гэрийн камер хэзээ хэн орж, гарч байсныг тэмдэглэнэ. Ухаалаг температур хэмжигч тухайн гэрийн хэмнэлд тохирсон горимыг санал болгож "сурна". Гэхдээ энэ нь тэр гэрт хэзээ хүн байхгүйг бас сурна гэсэн үг. Ухаалаг цаг тухайн хүний зүрхний цохилт, алхам, нойрны чанар, стресстэй үед хэрхэн амьсгалж байгааг ч бүртгэнэ. Тэр бүх мэдээлэл бол тухайн хүний биеийн, сэтгэлийн, зан үйлийн толь. Энэхүү хувийн өгөгдөл, мэдээлэл тухайн хүнд мэдэлгүйгээр интернэтэд хадгалагдаж, зарим тохиолдолд гуравдагч этгээд, сурталчилгааны агентлаг, төрийн байгууллагад дамжин ашиглагддаг байна.

Өнөөдөр хүний эрх чөлөөтэй амьдрах хувийн орон зай, амьдралын хэв маяг нь бодитоор технологийн ажиглалт, хяналтын нөлөөнд орсон байна. Хүн технологиудыг “зөвхөн өөрийн тав тухын төлөө” ашиглаж байна гэж бодож болох ч бодит байдал дээр тухайн хүний амьдралын бүхий мэдээллийг цуглуулж, хадгалж, хянаж, улмаар зан төлөв, чухал шийдвэрт нь нөлөөлж чадах бүрэн цогц хяналтын системийн мэдэлд “хүн”-ийг өөрийн мэдэлгүй алхам алхмаар орж байна. Энэ бол хүн эрх чөлөөгөө алдах, түүнээс хэт хараат болох хамгийн энгийн, чимээгүй хэлбэр юм. Ухаалаг төхөөрөмжүүд хүнд үйлчилж байгаа мэт боловч үнэндээ хүнийг хянах, удирдах үндсэн хэрэгсэл болоод байна.

2. Өдөр тутмын зуршлыг хянах: Интернетэд холбогдсон төхөөрөмжүүд хүний амьдралын хэмнэл, зуршил, шийдвэр гаргах арга барилыг маш өндөр нарийвчлалтайгаар хянаж чаддаг. Жишээлбэл: Тухайн гэрийн ухаалаг гэрэл хэдэн

цагт асаж унтардагийг мэдэж байгаа бол энэ нь гэрийн эзний өглөө сэрдэг, орой унтдаг цагийг мэдэж байна гэсэн үг. Мөн ухаалаг хөргөгч өдөр бүр тогтмол 21:00 цагт онгойдог бол гэрийн хэн нэгэн магадгүй оройн амттандаа дуртай хүн гэдгийг, эсвэл гэр бүлийн хооллолтын давтамж, зуршлыг ойлгож чадна.

3. Хакердах, гуравдагч этгээд ашиглах: Хамгийн ноцтой “эрсдэл” бол интернетэд холбогдсон төхөөрөмжүүд хакеруудын хувьд хяналт, тагнуулын хэрэгсэл нь юм. Эдгээр төхөөрөмжүүд ихэнх тохиолдолд сайн хамгаалалттай байдаггүй. Хэрэглэгчид өөрсдөө ч нууц үг солих, тохиргоо хийх тал дээр хангалттай мэдлэггүй байдгийн улмаас хакерууд төхөөрөмжүүд рүү амархан нэвтэрч чаддаг. Жишээ нь: Ring Doorbell гэх ухаалаг хаалганы камерын системийг 2020 онд олон хэрэглэгч хакердуулсан тохиолдол гарсан. Зарим хэрэглэгчдийн мэдээллээр бол хакерууд камерын дүрсийг үзэж, микрофоноор хүүхдүүдтэй ярих, айлган сүрдүүлэх, гэр бүлийн дотоод асуудлыг сонсох зэрэг үйлдлүүдийг хийж байсан. Үүнээс гадна олон интернетэд холбогдсон зүйлс үйлдвэрлэгчид хүний өгөгдлийг гуравдагч талд худалдаж, сурталчилгаанд ашигладаг. Хэрэглэгчид өөрсдөө зөвшөөрдөг гэхдээ тухайн нөхцөл, болзлыг хэн ч гүйцэт уншдаггүй. Ингэснээр тухайн хүний гэр орон, зуршил, эрүүл мэнд, байршлын талаарх мэдээлэл нь бизнесийн зэвсэг болон хувирч, ашиглагдаж байна.

IV. ХИЙМЭЛ ОЮУН – ХҮНИЙ СЭТГЭЛЗҮЙД ҮЗҮҮЛЭХ НӨЛӨӨЛӨЛ

Хиймэл оюун нь хүний оюун ухааныг дуурайсан, өөрөө суралцаж, шийдвэр гаргах чадвартай систем юм. Хиймэл оюун алгоритм ашиглан өгөгдөлд дүн шинжилгээ хийж, хүн шиг таамаглах, зөвлөмж гаргах, сэтгэл зүйд нөлөөлөх зэрэг чадвартай. Жишээ: Facebook-ийн мэдээний урсгал, YouTube-ийн санал болгох видео, ChatGPT гэх мэт.

1. Сэтгэл зүйн алгоритм: Хиймэл оюун нь хүний зөвхөн интернет дэх үйлдлийг биш, сэтгэл хөдлөл, бодол, итгэл үнэмшил, шийдвэр гаргах бүхий л процесст нөлөөлөх хүчтэй алгоримт юм. Энэ нөлөө маш чимээгүй, анзаарагдахгүй байдалтайгаар явагддаг бөгөөд хүн өөрийн мэдэлгүйгээр удирддаг. Хүмүүс өдөр тутам хэрэглэж буй Facebook, TikTok, YouTube, Instagram зэрэг платформууд өмнө харуулах мэдээллийг хиймэл оюун алгоритм ашиглан сонгож өгдөг. Хүн эдгээр мэдээллийг өөрөө сонгож авч үзэж байна гэж бодож болох ч бодит байдал дээр хиймэл оюун хүний өмнөөс шийдэл, бодолтыг хийж байгаа юм. Хиймэл хүний оюун өмнө нь сонирхож байсан контент, дарсан лайк, бичсэн сэтгэгдэл, хайсан түлхүүр үг, дэлгэц дээр илүү удаан харсан зүйлсийг судалж, сэтгэл зүй, зан төлөвийг загварчилдаг. Үүний үндсэн дээр таныг хамгийн ихээр оролцуулах, анхаарал татах контентыг санал болгодог.

Тэгвэл тухайн хүнд ямар үр дүн гарах вэ?

- ✓ Хүний үзэл бодол нэг талыг баримтлагч болох магадлал ихсэнэ;
- ✓ Эсрэг үзэл бодол, бодит байдлын тэнцвэртэй мэдээлэлд хүрэх боломж буурна;
- ✓ Хүн өөрөө сонголт хийж байна гэж бодсон ч, хиймэл оюун өмнөөс тэр сонголтыг хэдийнэ хийчихсэн байдаг байна.

Vol. 25 No 55 (2026) Article

2. Deepfake технологи: Deepfake технологи үнэн худлын ялгааг үгүй хийж байна. Deepfake нь хиймэл оюун ашиглан хүний царай, дуу хоолойг дуурайлган бодит мэт хуурамч видео, аудио, зураг үүсгэх технологи юм. Хүн болгон deepfake-ээр хиймэл дүртэй болчих боломжтой болсон. Энэ технологийг улс төр, гэмт хэрэг, хувийн нэр хүндэд халдах зорилгоор ашиглах нь ихэсч, үнэн худлыг ялгахад ихээхэн хүндрэлтэй асуудалтай тулгарч байна. Үүнээс гарах үр дүн:

- ✓ Хуурамч бичлэг, дуу хоолой тараагдсанаар олон нийтийн итгэл үнэмшилд нөлөөлнө;
- ✓ Хэн нэгнийг гүтгэх, айлган сүрдүүлэх, эсвэл улс төр, бизнесийн зорилгоор олон нийтийг төөрөгдүүлнэ;
- ✓ Хүн өөрийнхөө нүдээр харж байгаа зүйлдээ ч итгэж чадахаа больж эхэлнэ.

3. Сэтгэл хөдлөлийн анализ: Орчин үеийн хиймэл оюуны системүүд зөвхөн тухайн хүн юу үзэж байгааг биш, та яг тэр агшинд ямар сэтгэл хөдлөлтэй байгааг хүртэл ойлгож чаддаг болсон. Жишээ нь, TikTok, Instagram Reels хүний ямар төрлийн бичлэг дээр илүү удаан тогтож байгааг, ямар үед ямар төрлийн контент үзэж байгааг судалдаг. Хиймэл оюун хүний ганцаардсан, гунигтай, стресстэй үед илүү хүчтэй нөлөөлөх контент санал болгодог. Энэ нь олон удаа давтагдсанаар тухайн платформд хүн донтох, мэдээлэлд хэт автагдах, өөртөө итгэх итгэл буурах, сэтгэл зүйн эрүүл мэнд муудах зэрэг эрсдэлтэй тулгардаг байна. Үүнээс гарах үр дүн:

- ✓ Хүн өөрийгөө удирдаж байгаа мэт мэдрэмжтэй боловч үнэндээ хиймэл оюун хүний сэтгэлийг чиглүүлж байдаг;
- ✓ Сэтгэл гутрал, ганцаардал, өөрийгөө буруутгах мэдрэмж асар ихээр нэмэгддэг;

4. Сонголтын манипуляц: Худалдан авалт, аялал төлөвлөлт, улс төрийн сонголт, бүр хэнтэй найзлах хүртэл хиймэл оюун хүний шийдвэрийг урьдчилан тооцоолж, хамгийн өндөр магадлалтай сонголтыг хүнд илүү ойртуулан харуулдаг.

V. AI (Хиймэл оюун) + IoT (Интернетэд холбогдсон зүйлс) = Шилэн доторх нийгэм

“Шилэн доторх нийгэм” нь хүний эрх чөлөө, хувийн орон зай, сэтгэл зүй, бодол санаа гээд бүх л талыг хянах боломжийг төр, төрийн байгууллага, хувийн хэвшил болон хувь хүнд өгдөг. Бидний амьдрал уламжлалт утгаар бол “эрх чөлөөтэй” мэт харагдаж болох ч, үнэндээ “шилэн доторх амьдрал”-д (хөндлөнгийн хэн нэгнээс хараат байдалд) алгуурханаар шилжин орж байна.

Нийгмийн онооны систем (Хятад) – IoT + AI хосолсон хяналтын бодит жишээ: Хятадын “Social Credit System” бол интернетэд холбогдсон зүйлсийн төхөөрөмж, хяналтын камерууд, хиймэл оюун ухааныг ашиглан иргэдийн үйлдэл, төлөвшилд оноо өгч, нийгмийн эрх чөлөөг үнэлдэг систем юм. Хот даяар байршуулсан хиймэл оюунтай хосолсон 20 сая гаруй камер нь иргэдийн хөдөлгөөн, харилцаа, худалдан авалт, төлбөр тооцоо, цахим харилцаа зэргийг бүртгэж, төв серверт илгээдэг. Дараа нь хиймэл оюун эдгээр мэдээлэлд дүн

Vol. 25 No 55 (2026) Article

шинжилгээ хийж, сайн иргэн үү? эсвэл "сэжигтэй этгээд" үү? гэдгийг оноогоор хэмжиж дараах арга хэмжээг авдаг. Үүнд:

- ✓ Олон нийтийн газарт хог хаявал оноо хасна;
- ✓ Хуулийн зөрчил гаргавал гадагшаа аялах эрхийг хязгаарлана;
- ✓ Нийгмийн оноо муутай бол хүүхдээ сайн сургуульд оруулж чадахгүй, ажилд орох боломжгүй болно;

Cambridge Analytica – AI ашиглан сэтгэл зүйг удирдаж, сонгуулийг өөрчилсөн. Cambridge Analytica нь Facebook-ээс 50+ сая хэрэглэгчийн хувийн мэдээллийг зөвшөөрөлгүйгээр цуглуулж, Хиймэл оюун ашиглан тэдний сэтгэл зүйн төрлийг загварчилж, улс төрийн сонгуулийн үр дүнд шууд нөлөөлсөн бодит кейс юм. Тус компани хэрэглэгч бүрийг “итгэмтгий”, “аймхай”, “ууртай”, “эмзэг” гэх мэт сэтгэл зүйн төрлөөр ангилж, тус бүрд нь тохирсон улс төрийн сурталчилгаа, мэдээлэл, контент илгээж байсан. Үүний үр дүнд маш олон хүн өөрсдийн бодол, үнэмшил дээр биш, харин хиймэл оюунын тохируулсан контент дээр үндэслэн санал өгсөн. Мөн хүний үзэл бодол, сонголт хиймэл оюуны алгоритм, мэдээллийн тархалт дээр тулгуурлан хянагдаж болдгийг харуулсан хамгийн тод жишээ юм. Энэ нь тухайн улс орнуудын тусгаар тогтнол, үндэсний аюулгүй байдалд ч нөлөөлөх асуудал юм.

VI. Дүгнэлт

Дэлхий нийтэд хиймэл оюун, интернетд холбогдсон төхөөрөмж зэрэг дэвшилтэт технологиуд нийгмийн хяналт, мэдээллийн манипуляцийн хэрэгсэл болон ашиглагдаж эхэлснээр хүний эрх, эрх чөлөө, улс орны тусгаар тогтнол, үндэсний аюулгүй байдалд шинэ үеийн сорилтууд тулгарч байна. Хятад, Cambridge Analytica зэрэг жишээнээс харахад, энэхүү технологийн буруу хэрэглээ зөвхөн тухайн улс оронд бус, дэлхийн ардчиллын үнэт зүйл, олон улсын харилцаа, итгэлцэлд ч гүнзгий нөлөө үзүүлж болзошгүйг илтгэн харуулж байна.

“Цахим боолчлол” хэмээх ойлголт нь хиймэл оюун болон интернетэд холбогдсон төхөөрөмжийн хурдацтай хөгжсөн XXI зууны нийгмийн шинэ хэлбэрийн дотоод хяналтын тогтолцоо болон хувирсан байгааг дээрх судалгаанаас харагдаж байна. Гол онцлог нь албадлага, хүчирхийллээр бус “хүний байгалийн өгөгдөл, далд ухамсар” дээр суурилж байгаа юм.

Монгол Улсын нийт хүн амын цахим хэрэглээг авч үзвэл цахим технологийн хэт хамаарал, мэдээллийн нэг урсгалтай байдал зэрэг нь олон нийтийн үзэл бодолд ихээхэн нөлөө үзүүлж, асар их өгөгдлийн сантай мэт харагдавч, бодит байдал дээр иргэд хяналтгүй мэдээллээр дамжуулан удирдуулж, “ухамсартай автомат хариу үйлдэл үзүүлэгч” нэгж болон хувирч буй нь сэтгэл зүйн хараат байдлын илрэл юм.

Хиймэл оюун таны юу үзэхийг, хиймэл оюун таны юу хийж байгааг мэдэж байгаа гэж үзье.

Тэгвэл нэг асуулт маш чухал. Бидний юу бодохыг хэн хянаад байгаа вэ? Хэнд, юунд хэрэгтэй вэ? **Үзэл бодол, үнэмшил, мэдрэмж, шийдвэр** — эдгээр нь хувь хүний хамгийн чухал бөгөөд дээд түвшний эрх чөлөө байх ёстой гэтэл

өнөөдөр тэдгээр нь өгөгдөл болон ашиглагдаж, системийн “түлхүүр” болж эхэлсэн байна.

Өнөөгийн Монголын нийгэмд төр, засагт итгэх олон нийтийн хандлага эрс буурч, үл итгэх байдал давамгайлж байна. Энэ үзэгдлийг зөвхөн улс төрийн шийдвэр, эдийн засгийн хямралтай холбох нь хангалтгүй. Хүмүүсийн бодол санаа, үзэл бодол, сэтгэл зүйг тодорхойлох гол орон зай нь цахим орчин болж хувирсан өнөө цагт энэ хандлагын суурь шалтгааныг “хиймэл оюун” болон “интернетэд холбогдсон зүйлс”-д суурилсан "цахим боолчлол”-ын тогтолцоотой салшгүй холбох шаардлагатай асуудал юм.

Монгол Улсын иргэд өнөөдөр төрдөө бус, цахим хяналтын системийн сүүдэрт автан, ухаалаг хяналттай, далд манипуляцид суурилсан “цахим боолчлол” буюу мэдээллийн орон зайн хамаарал хязгаарлалтанд өөрсдөө ч мэдэлгүйгээр хэлбэршиж, сэтгэл зүйн эрх чөлөөгөө өдрөөс өдөрт алдаж байна. Иймд тухайн улс орны төр, засаг тулгарч буй асуудалд бодит алдаа гаргасан байж болох ч, иргэдийн бухимдлын асар их байгаа шалтгаан нь хиймэл оюун, цахим платформуудын бий болгож буй сөрөг мэдээллийн урсгал, нийгмийн сэтгэл зүйн манипуляци байх боломжтойг дээрх судалгаа харуулж байна.

Нийгэм, улс орны хэмжээнд хүний эрх, аюулгүй байдлыг хамгаалсан хууль эрх зүйн зохицуулалт, бодлого боловсруулах нь чухал юм.

Цахим орчин дахь хүний аюулгүй байдал нь тасралтгүй хувьсан өөрчлөгдөж байгаа салбар бөгөөд технологийн шинэ дэвшил бүрийн хамт шинэ эрсдэл, боломжууд бий болсоор байна. Хүний аюулгүй байдлыг хангахын тулд дээрх бүх хүчин зүйлсийг харгалзан үзэж, цогц арга хэмжээ авах шаардлагатай байна.

ЭШ ТАТСАН СУРВАЛЖ, СУДАЛГААНЫ БҮТЭЭЛИЙН ЖАГСААЛТ

[1] Хүний хувийн мэдээлэл хамгаалах тухай. Монгол Улсын хууль. 2021 оны 12 дугаар сарын 17-ны өдөр. 4.1.11 дэх заалт. 4.1.1 дэх заалт

[2] Кибер аюулгүй байдлын тухай. Монгол Улсын хууль. 2021 оны 12 дугаар сарын 17-ны өдөр. 4.1.3 дахь заалт

[3] Үндэсний статистикийн хороо. (2024). Монгол Улсын хүн амын тоо, бүтэц (2025 оны төсөөлөл). http://www.nso.mn

[4] Meta Ads Manager (2024). Mongolia Audience Insights – Facebook Ads Reach Data. https://adsmanager.facebook.com

[5] Эрдэнэцогт, С. (2024). Монгол улсын цахим орчин дахь хууль эрх зүйн зохицуулалтын асуудлууд. *Хууль дээдлэх ёс*, 38(1), 22-37

[6] Галбадрах, Л. & Наранбаатар, М. (2023). Монгол улсын цахим аюулгүй байдлын эрх зүйн орчны судалгаа. *Хууль зүйн судлал*, 25(3), 112-127

[7] Гэрэлчимэг. К. (2024). Нийгэмд цахим мэдээллийн үзүүлэх сөрөг нөлөө, түүнийг бууруулах арга зам” докторын диссертацын ажил. 33 тал.

[8] Жаргалсайхан, Д. & Мөнхбат, О. (2024). Дижитал шилжилтийн эрин үеийн аюулгүй байдлын сорилтууд. *МУ-ын ШУА-ийн мэдээ*, 62(1), 45-57

[9] Содномдаржаа, Т. (2024). Цахим орчин дахь хувийн мэдээллийн хамгаалалтын технологийн шийдлүүд. *Монголын мэдээллийн технологийн сэтгүүл*, 16(1), 88-102

[10] Эрдэнэбаяр, Б. (2022). Цахим орчинд хувийн мэдээллээ хамгаалах арга зам. *ШУ-ны ажилтны өдрүүдийн эмхэтгэл*, МУИС, 345-358

Vol. 25 No 55 (2026)

[11] “Харилцаа холбоо, мэдээллийн технологийн нэр томъёоны толь бичиг”. ШУТИС, ХХМТГ, Бүх нийтийн үүргийн сан, МУИС, УБ., 2021

[12] Цахим орчин дахь хүүхдийн аюулгүй байдлын талаар үндэсний суурь судалгааны тайлан. Харилцаа холбооны зохицуулах хороо. Эм Эм Си Жи ХХК. 2020.07.09

[13] Cambridge Dictionary. (n.d.). Manipulation. In Cambridge English Dictionary. Cambridge University

[14] Press. https://dictionary.cambridge.org/us/dictionary/english/manipulation

[15] Zuboff, Shoshana. (2019). The Age of Surveillance Capitalism. Public Affairs Publishing. “Surveillance capitalism, AI + data governance, and the impact on human freedom”

[16] Wired Magazine. (2023). “Tesla remotely disables features of cars without owner's consent”. https://www.wired.com

[17] MIT Technology Review. (2022). “Deepfakes and the threat to reality”. https://www.technologyreview.com

[18] Netflix Documentary. (2020). “The Social Dilemma”

[19] European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape Report 2023*. Luxembourg: Publications Office of the European Union.

[20] International Telecommunication Union (ITU). (2023). *Global Cybersecurity Index 2023*. Geneva: ITU Publications

[21] Pew Research Center. (2023). *Digital Privacy Concerns and Attitudes: A Global Survey*. Washington, DC: Pew Research Center

[22] United Nations Office on Drugs and Crime (UNODC). (2023). *Global Report on Cybercrime 2023*. Vienna: United Nations Publications