CYBER SECURITY AND HUMAN RIGHTS CONSIDERING THE METAVERSE

Prof. Doina BANCIU, PhD
Academy of Romanian Scientists
banciu.doina@gmail.com

Assoc. Prof. Daniel FODOREAN, PhD
Baptist Theological Institute of Bucharest
danielfodorean@gmail.com

Carmen Elena CIRNU, PhD
National Institute for Research & Development in Informatics - ICI Bucharest
carmen.cirnu@gmail.com

Abstract:
The concept of metaverse brought into discussion these days in the context of rebrands of the social network Facebook under the name Meta, raises questions on several levels, both in terms of cybersecurity and in terms of human rights.
This term metaverse first appears in 1992 in the novel Snow Crash by Neil Stephenson, an American writer of speculative fiction, and it describes the virtual reality that exists alongside physical reality, a parallel coexistence. This meta, originally from the Greek language („with",„after",„next",„above" and„beyond") expresses a reality„from beyond" leading to the idea of metamorphosis, a change of place or state . Mark Zuckerberg, the Facebook company's CEO, imagines his metaverse as a virtual space that uses digital tools to offer a sense of physical presence to all over the world people. If Zuckerberg's prediction will become a reality, it is clear that the cyber security protection will need to increase accordingly. The metaverse will enter and will penetrate our private life and it will dramatically impact our human rights. This intersection between metaverse and cybersecurity, on the one hand, and human rights, on the other, will be examined in this article.

Keywords: *human rights, metaverse, cyber security, data protection.*

Facebook changed its name to "Meta", to highlight an evolution from the position of a giant of social networks to the development of a "metaverse", a digital world that could be the next internet generation.

Mark Zuckerberg, the company's CEO, imagines his metaverse as a virtual space that uses digital tools to offer a sense of physical presence to all over the world people.

"From now on, we will first be metaverse, not Facebook," Mark Zuckerberg said on Thursday, October 28th. One week after announcing the change, Zuckerberg made the announcement in a speech on Facebook Connect, into the company's annual internal conference. Zuckerberg, 37 years old, has spent much of the past year talking about the change. He mentioned that people are expected to consider in the near future Facebook as the company that created this "metaverse" and not just the social network.

Zuckerberg describes the metaverse as a virtual environment that will allow people to be present in digital spaces with each other in digital spaces.

"In metaverse, you will be able to spend your time, play with friends, work, create, and much more.""Basically, you'll be able to do everything you can on the internet today, as well as some things that don't make sense on the internet today, like dancing."

In his speech, Zuckerberg also described developments in Horizon Homes, an application designed to provide users with a digital space at home, where they can store their digital goods, spend time with their friends' avatars, and teleport to other spaces and worlds.

However, all this requires skills and knowledge to use information technology. The all European Action Plans for 2000-2005 (e Europe, e Europe +) included tasks to develop citizens' computer skills. All European policies and strategies have taken into account the increase of citizens' competence for ICT use, from 2005 until now.

In March 2021, the European Commissioner Ursula von der Leyen launched the EU's digitalization strategy entitled "A Europe ready for the digital age". The 2030 Strategic Policy actually includes four main pillars:

- skills → 80% citizens with ICT skills
- infrastructure → a large connectivity
- business environment → 90% SME has to use basic ICT and ¾ from large companies, cloud services

- e-governance → Public administration has to implement the ICT procedures and rules in all structures.

According to the mentioned documents, the transition to the digital transformation of Europe by 2030 will be supported by a budget of EUR 120 billion.

Skills development means education at all levels of existence. However, it is found that society has been divided as a whole into three categories of citizens, according to the generation they belong to:

- analog generation → over 65 years
- digital generation → 4-25 years
- functional digital generation that has gone through digitization and participates actively in digital transformation.
- Digital literacy → means to write, to read, to count by computer aid
- The education and political will have to work together to avoid the "digital divide".

The pandemic led to the development of computer skills, the spread of digital information in various forms of presentation and communication: websites, Twitter, Facebook, etc. Large collections of digital data, both in the literal, scientific, economic but also personal data, personal data such as unique identification code, medical record, personal address, etc. they need to be stored and protected from unwanted cyber-attacks. If we add to this data on national security or transnational strategies, it is obvious that the protection of digital collections must be ensured accordingly.

But digital transformation means more, a matter of managerial vision.

The economic function is changing, the economic paradigm is changing, the digitization of products in the economy has become necessary to adjust the way of economic growth, so far based on consumption.

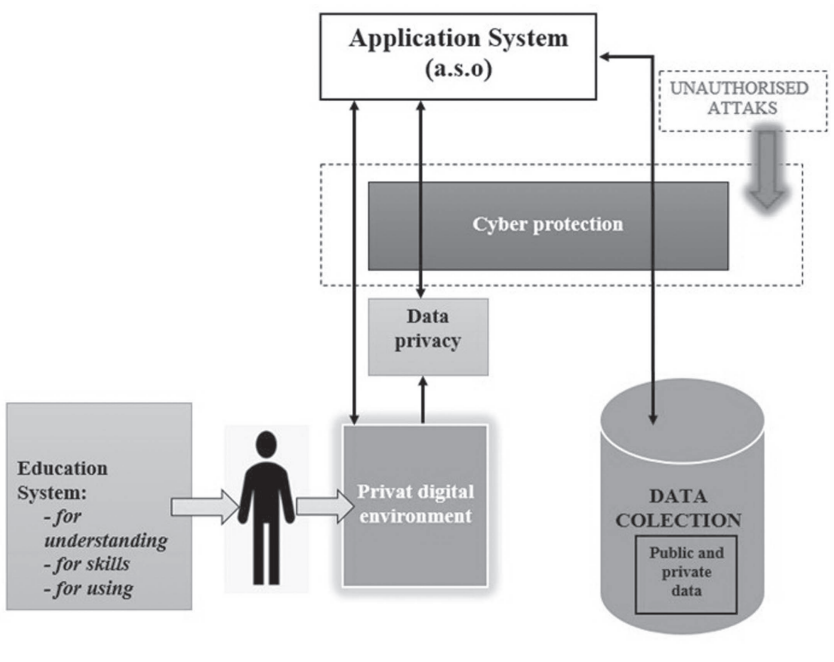
Solving the two aspects: education and cyber protection requires a new social pact through which authorities, the decision-makers, ICT producers and citizens, act in the same direction that respects the human condition and human rights.

At the level of ICT systems are many rules for protection but this kind of protection function also as an auto-protection given by the types of equipment and other kinds of protection systems, like as, Firewall. Normally this protection is provided by companies vendors ICT.

Cyber protection has to be oriented on two components:

- keeping data privacy
- stopping the unauthorized attack

This fact could be understood better from the following chart about Protection Layer in the Metaverse.



The cyber protection regarding data protection and unauthorized attacks has to be given by the special procedures and implemented by special bodies. These authorized bodies could managed by state authoritiesand they has to act according to the legal framework. Our oppinion is that in this manner the freedom of the citizens and private data could be garantated.

In light of the rapid acceleration of the application of the "Metaverse" concept, there are different possible intersections between cyber security and human rights that call our attention:

- The application of cyber security-associated norms and policies can protect human rights and fundamental freedoms;
- In a similar manner, the application of the aforementioned norms/policies can also negatively affect rights and fundamental freedoms;
- There may be noticed similarities between cybersecurity and cybercrime-related measures in protecting human freedoms/rights

- The need to keep the balance between the protection of human rights and freedoms and the cyber security recommendations.

The specific situation of the COVID-19 pandemic makes this discussion more urgent than ever. The vast majority of affected societies had to adjust to living and working remotely from home/online, which makes free and uninterrupted access to information and communication technology (ICT) more important now than ever. Evidently, this shift has led to concerns and questions related to, but not limited to the privacy and security of such communications. The acceleration of the "Metaverse" brings even more pressure on the evaluation of the associated risks and benefits. Could the metaverse be considered a fairly safe place? Experts are worried about the high level of attractivity this new paradigm may bear to cybercriminals. For example, considering the recent launch of the important auction house Sotheby's metaverse digital art platform, Cisco Talos Head of Outreach Nick Biasini expressed his concerns as follows:

> *Because [the metaverse] is tied to this largely unregulated, quasi new era of cryptocurrency, there's a huge potential for scams. It's something where some organizations are spending a huge amount of resources, so there's the potential for this to become a very big part of the internet. You have a place with low regulation and low legal recourse for victims — it's extremely attractive to criminals*[1].

Biasini also warns that some cyberthreats are particular to the metaverse and the technologies that make it functional, especially blockchain, cryptocurrencies, and NFTs (Non-Fungible Tokens). He notes that "*one of the challenges (…) coming up is going to be related to defending your intellectual property and branding*"[2], which are aspects intimately tied to personal human rights.

Amelia Kallman, the futurist, is also highlighting the cyber risks implied by the metaverse. Even if it brings numerous advantages that make us think we soon might be living in a sci-fi movie, such as holoportation, teleoperations, and new e-commerce opportunities, at the same time the metaverse offers "*fresh possibilities for unforeseen threats to the security of the*

1 https://www.sdxcentral.com/articles/news/why-cisco-calls-the-metaverse-cybersecuritys-wild-west/2021/11/

2 *Ibidem*.

consumer, commercial, and corporate markets"[3]. Underlining the fine line between cyber security and real human rights violation, A. Kallman affirms that *"it is just a matter of time before virtual breaches become real world court cases".*[4]

Although there is a somewhat limited but yet expanding body of regulation, research and case law concerning human rights safeguards and guarantees applicable to fight against cybercrime and use of electronic evidence in criminal cases – due to cybercrime being a criminal justice matter in the first place - cybersecurity and relevant human rights guarantees remain an area less addressed and discussed in a balanced manner. Too often, the debate on the subject matter is bringing together highly polarized views in the manner of "security vs freedom" rather than seeking balance in recognizing potential positive and negative effects of strengthening cybersecurity for individual rights and freedoms.

The cyber-attacks increased dramatically in the last years and the pandemic and the upscaling use of digital, also increased the need for digital data transfer and the development of big digital data collection, not only for public entities but also for the private.

The damage on the private data (like that of the cyber-attacks on banks) represents one of the concerns over the need of considering cyber defense. To exemplify this phenomenon, the present paper discusses the example of the cyber attacks on top-level domains. The analysis below shows the increasing data attacks.

Also, at the national level, the supervising authority declares an increasing number of attacks, most of them blocked through special procedures.

If Zuckerberg's prediction will become a reality, it is clear that the cyber security protection will need to increase accordingly. The metaverse will enter and will penetrate our private life and it will dramatically impact our human rights.

The focus of current discussions and debates should be to look beyond more established subjects of criminal justice response and related human rights safeguards, by focusing on rapidly developing area of cybersecurity regulations and compliance, and to evaluate the rights and freedoms at stake that could be both protected and/or affected by cybersecurity

3 https://www.ibc.org/blog-cyber-security-and-the-metaverse/2904.article

4 *Ibidem*.

measures. However, finding possible common ground on the subject matter between cybercrime and cybersecurity domains is equally important. Viewed from this perspective, the COVID-19 pandemic has not brought along particularly new questions, but rather amplified both positive and negative aspects of the interaction between cybersecurity/cybercrime and applicable human rights. Finding appropriate balance in this new reality is an ever-shifting but nevertheless still an important goal.

Metaverse has real implications for the notion of humanity because, in fact, it proposes a dehumanization, a metamorphosis. Michael Taylor believes that „The key transformation from meatverse to metaverse (besides the movement of one letter) can be captured by the concept of dematerialization. Future production of goods and services need not be physical. They will be largely digital. We will increasingly live our whole lives in this digital world"[5]. But metaverse may have implications for cybersecurity and respect for human rights. The process of embracing the metaverse must be viewed with caution.

Bibliography:

- Joanna, Kulesza and Roy Balleste, Cybersecurity and Human Rights in the Age of Cyberveillance, Rowman & Littlefield Publishers, Inc., 2015.
- Pavlova, P., „Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups", Peace Human Rights Governance, 4(3), 2020, 391-418
- https://www.ibc.org/blog-cyber-security-and-the-metaverse/2904.article
- https://news.artnet.com/market/sothebys-wades-deeper-digital-art-game-new-custom-nft-marketplace-called-metaverse-2021205
- https://www.sdxcentral.com/articles/news/why-cisco-calls-the-metaverse-cybersecuritys-wild-west/2021/11/
- https://rm.coe.int/katrin-cybersecurity-and-human-rights/1680a0c1f8
- https://blog.malwarebytes.com/privacy-2/2021/11/zuckerbergs-metaverse-and-the-possible-privacy-and-security-concerns/
- https://www.bbc.com/future/article/20211112-facebook-and-the-true-meaning-of-meta

5 https://www.expressnews.com/business/business_columnists/michael_taylor/article/Taylor-Metaverse-Smart-Money-16623685.php