PROSEGUR RESEARCH

Lights and shadows of the metaverse

2022

PROSEGUR

Limitless society

Digital economies

Business opportunity

Job creation

Opportunities

Threats

Violent behavior

New economical space for crime

Perverse gamification

Criminal e-learning

This is an interactive document

> **The metaverse is an immersive virtual world in three dimensions with representations of the environment and accessible through virtual and augmented reality devices, as well as haptic technology or recognition systems that allow us to interact with all of its elements in real time.**

The concept of the metaverse is not developed as a videogame of great dimensions, rather it is founded on the base of virtual **socialization:** the objective is to interact with other people **(avatars)** through public spaces, cinemas, offices, leisure spaces, etc. Therefore, **the opportunities are virtually limitless,** as many as the ones the physical world presents us with, among which are working, collecting a salary, going to concerts, visiting museums to studying a degree.

The metaverse is one of the **great paradigms of technological convergence by integrating different technologies** that complement each other to offer the user a comprehensive experience.

Technologies linked to the metaverse

Virtual reality

Using devices such as virtual glasses, it is a technology that allows the immersion of the individual in a computer-generated graphic environment.

Augmented reality

It is a technology that overlaps graphic elements to the ones existing in the physical world. As an example, there are live broadcasts of La Liga of Professional Football in Spain. Along with virtual reality, the mix or hybrid reality is one that reaches a full immersion of the user in the alternative vision.

Haptic and biometric technology

Through the usage of tools such as gloves, goggles and suits, these technologies would be used with the objective to make interacting and recognition of the avatar to be based on the movement and biological information of the human body.

IoT (Internet of Things)

The level of interaction between the physical and digital environment in the metaverse will be intensified by the IoT due to the new interconnecting opportunities between different devices offered by this technology.

Quantum computing

Type of computing that allows a variety of algorithms exponentially superior that increases the capacity of calculation to considerable limits that are so far unreachable for conventional computers.

Blockchain

Blockchain technology, used for cryptocurrencies and NFT (Non-fungible tokens), could provide the metaverse with an approximation to the concept of economy and private property. NFT, characterized for being unique, indivisibles and private, could play an important role for their verification capability based on the chain of blocks.

Artificial intelligence

It is one of the pillars of the development of the metaverse which could be used as a method to analyze the behavior of avatars (such as movements and messages) to predict demeanors or make the environment more precise.

New generations of mobile connectivity (5G, 6G, …)

Due to increasing connection and lower response latency, it is expected that the metaverse, maximized by these technologies, will be capable of offering better experiences to the users (some examples include better graphics and frames per second than the ones available in current virtual and augmented reality).

The metaverse **is not a concept** within the collective imagination. In fact, it has been almost 30 years, in 1992, when the author Neal Stephenson coined the term in his piece Snow Crash, where the characters interacted with each other in a virtual world in 3D. This has not been the only precedent of the metaverse: for example, a year later, in 1993, Steven Jackson Games, launched to the market a virtual reality system which would allow simultaneous connection of different users. **During the last years we have seen approximations of extensive virtual worlds in the entertainment industry,** especially in videogames such as MMORPG like World of Warcraft or sandbox like Minecraft, or Pokemon GO, the first augmented reality videogame with global success that amassed 630 million downloads and more than 5 billion dollars in billing since it launched in 2016.

We must understand the metaverse as an ample futuristic idea, not restrictive nor dominated by a sole company. Even though Facebook seems to be the most thriving on the future of the metaverse with its rebranding as Meta, there are other companies like XRSPACE with Mova, Microsoft, Apple, Nvidia, Epic Games or Roblox that have also shown interest. In fact, Epic Games has been able to breach boundaries and possibilities with its popular videogame Fortnite by, for example, hosting real-time virtual concerts of Ariana Grande or Travis Scott that accumulated more than ten million of spectators. Others such as Coca-Cola have launched their own NFTs in the virtual reality platform Decentraland equipped with resources such as virtual personalized discos or the possibility of understanding among the avatars of the world.

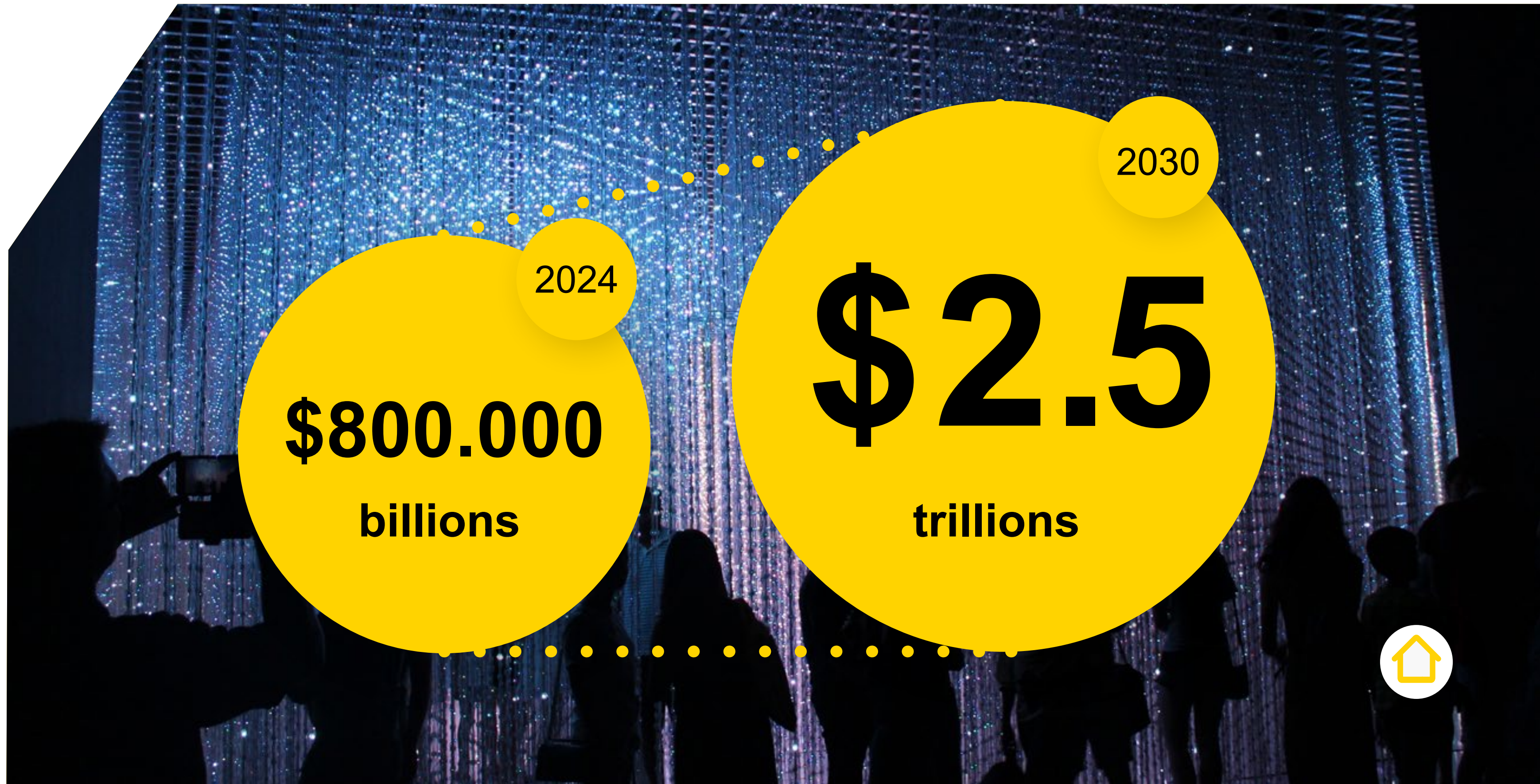
> All of this demonstrates that our way of interacting with reality is gradually being modified.

The fact that more than a company is interested in the creation of a metaverse calls into question whether the **principle of full interoperability** will be achieved: the possibility of codes to flow and share data, enabling the exchange of information between different systems. Today, the metaverse as it has been proposed is closer to a purpose than a reality: experts have indicated the **great barriers** that slow its development such as insufficient precision or **design of virtual reality technological** devices, in terms of the **necessary infrastructure** that would require this alternative universe (from skyscrapers to streets, supermarkets or traffic lights). Thus, the interoperability capacity seems utopic: how can connection between users that use “business metaverses” be achieved? Will companies be willing to share users’ information’s in order to accomplish an authentic connection between virtual worlds?

The economic potential of the metaverse is immense. Already in 2021, the last data of Bloomberg Intelligence valued the metaverse at 500 billion dollars. Moreover, they also point to the market opportunity Will reach approximately **800 billion dollars in 2024 and 2.5 trillion dollars in 2030**[1]. Moreover, Bank of America named the metaverse as one of the fourteen disruptive technologies that will transform our lives.

These optimistic economical expectations are due to the infinite possibilities, as we previously briefly mentioned, and its capability to modify the **labor market and the development of videogames, programing, and social media**[2]**.** In fact, the Longterm Spanish National Strategy 2050 has pointed out the growth of the metaverse and virtual reality as vectors of technological development, with its consequent creation of jobs such as data scientists, robot operators or the controversial Minecraft gardeners or avatar trainers.

However, the metaverse will also involve a **series of challenges for security** that companies and users must consider.



[1] On the other hand, Grayscale estimates the incomes of videogames ´virtual worlds to 180 000 million dollars which would amount to 400 000 million in 2025. Grayscale estimated revenues from video game virtual worlds at $180 billion in 2020, which could rise to $400 billion by 2025.

[2] For example, Meta has already announced its plan to employ 10 000 people from European Union during the following years that will exclusively dedicated to the development of the metaverse.

Challenges for security

The progress in the development of the metaverse implies the emergence of new risks and challenges, forcing the security guarantors to anticipate the imagination and the limitless or ethical and legal conditions that want to employ the metaverse for malicious purposes.

In this regard, the **hyperindividualism** of the **contents and services,** the economical exploitation of the metaverse, the anonymity and the transfer of social common dilemmas to the cyberspace such as discrimination of all sorts or the social polarization that encourages the rise of criminal behavior.

Next, potential criminal uses or malicious applications that can be exploited during the development of the metaverse and its associated technologies will be displayed.

Transfer of social conduct into the metaverse

Just as it happened with Internet and the named as "primitive metaverse" of ***Second Life,*** it is probable that a great deal of the activity developed in upcoming metaverses will be oriented towards the consumption of adult content, hence presenting significant challenges for the protection of people as it will be reviewed below.

Violent behavior

The transfer of social interaction into the virtual framework implies the transfer of violent behaviors such as bullying, abuse and coercion. In this regard, it is likely that interactions between avatars will involve an increasing number of situations that will have a tangible impact in the real world in a similar way that it has happened with abuse and coercion in social media and that these will develop in a sphere of impunity by taking advantage of the latency with which the **legal system** adapts to the innovative criminal behavior.

Recruitment and radicalization

The enormous digital offer as well as the absence of register of communications which may happen avoiding chat (both orally and by making use of the physical spaces of the games, such as writing messages with the outline of steps or weapons), and the underlining anonymity sensation to the majority of gaming platforms, facilitates the development of “sensitive interactions” to recruit the youth in criminal and terrorist organizations. In addition, the immersion into the metaverse favors the systematic desensitization in the process of radicalization through exposure of violent content in virtual reality.

Extorsion

The employment of avatars by delinquents- through the recording of conversations and interactions- allows the extorsion of consumers of content by threatening them with the publication of personal information

Exposure of minors

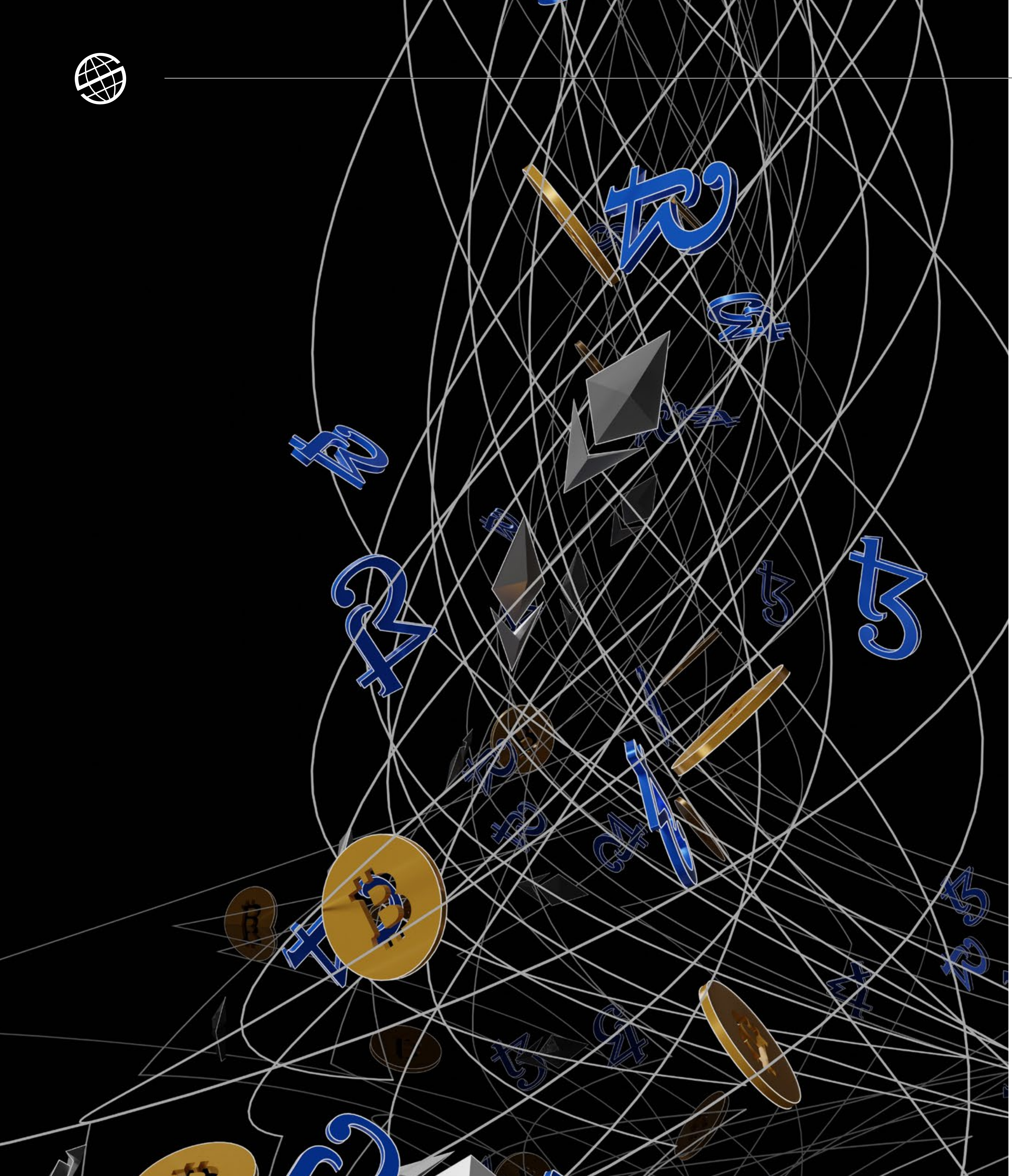
Even though the virtual expression of a user (the avatar) lacks physical presence as such, the fact that the interactions among users are real and can develop without supervision heightens the chances of certain circumstances such as the anonymity that allows minors with curiosity to be exposed to the mentioned threats.

Identity fraud

People could become victims of data theft, whether they are personal or biometric, that subsequently could be marketed or used in an illicit manner in the metaverse or the physical world. That is why identity fraud, also known as spoofing, is one of the most worrisome subjects in the development of the new digital universe.

Social polarization

The truth is that there is a high risk of political and social polarization in the development of the metaverse. The combination of augmented reality, virtual reality and artificial intelligence technologies could suppose a vision of the world unique for each user, thus certain visual or audio content could be block for not being in line with each person´s ideals or likings. In addition to the usage of collected biometric information, there has been speculation about the possibility of including individualized advertising which would open the door to the monetization of the metaverse.



Emergence of a new space for economic delinquency

We will review the possibilities of economic exploitation of infinite of developments that were not considered in its origins. The rapid flow of transactions and the fact that **neither the metaverse nor the crypto-economic spaces are yet sufficiently regulated** has provoked this scenario to become an attractive element for scammers and cyber criminals.

In this new environment the lack of knowledge surrounding the metaverse´s transaction system by users and businesses could facilitate the success of scammers through, for example, **intelligent contracts** that do not comply with what they promise, rather they offer access to the victim´s crypto actives or personal information.

Other common risks currently present in Internet must not be disregarded in the metaverse. For example, **Distributed Denial of Service (DDoS)** which try to collapse servers by receiving more petitions that the system can process could be used in the metaverse in order to interrupt its operations. Moreover, the crypto-based economy, supported by blockchain technology and NFT, could imply the trading of precious digital actives, such as artwork or digital terrains, which could potentially become objective of **ransomware** attacks, which try to hold hostage data stored while requesting an economic ransom to decipher said information.

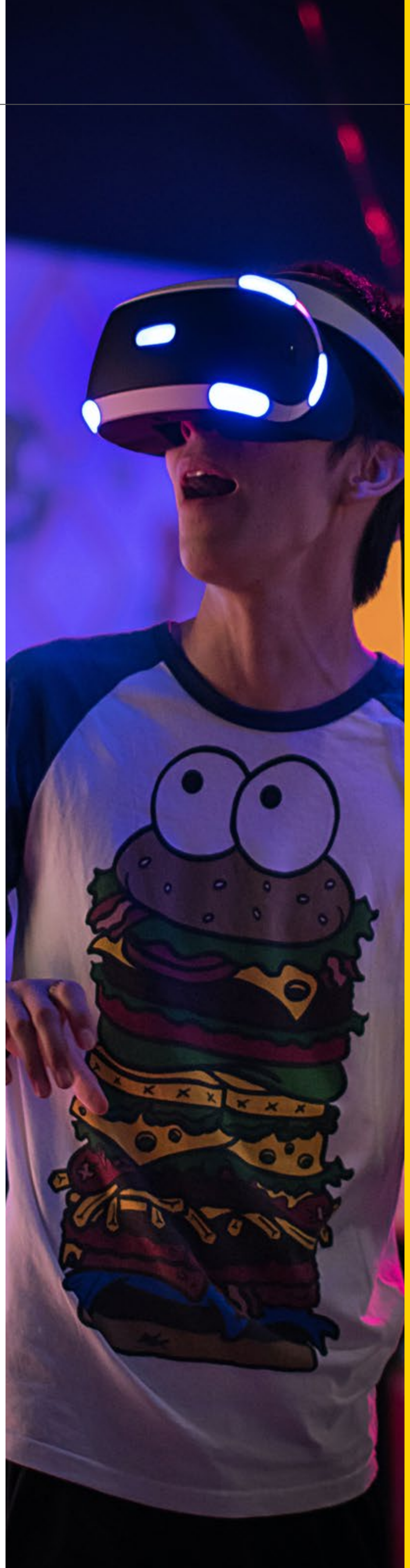
Perverse gamification

The usage of augmented reality devices in a reckless or careless manner could derive significant challenges for security **by taking on risky behaviors or placing certain people, without a criminal intention, in compromising situations.** In this regard, the large number of violation of perimeters and access to restricted areas cases occurred at the global level due to the Pokémon GO phenomenon. This situation has led to the United States Marine Corps to **publish recommendations** for players to avoid accessing restricted areas while playing.

Moreover, the immersion of users into the metaverse increases the chances of dissociation from reality during the participation of perversive games, such as it happened with the **Blue Whale** case, a challenge that results with the inducement to suicide of its participants. In this regard, the elements of virtual reality and augmented reality increases its captivating capability as well as the ease of certain **coercion and manipulation schemes** to have a greater impact upon their victims implying a real physical and tangible risk for their physical integrity.

Additionally, in an immersive context, **the gamification facilitates tools of an unprecedented power to carry out manipulative actions** it alters the vector of influence of the victims shifting from external (the victim is convinced) to internal (the progress itself). In this scenario, it is likely that the development of this technologies will derive in the emergence of spaces and groups dedicated to extracting benefits from manipulation of users in the metaverse, configuring as sects or clans that carry an economical exploitation.

Furthermore, as the World Economic Forum points out the effects of long-lasting effects such as loss of visual coordination, we cannot underestimate **physical risks for the user** like dizziness, falls or "cyber-diseases".



Under the spotlight. Milsim and defense leaks in the metaverse.

The development of increasingly powerful graphics and logic engines (derived from the evolution of computational capacity) allows **increasingly realistic digital approaches** with simulation environments, often replicating scenarios, physics, materials, procedures and actions very similar to the reality. Nevertheless, professional armies in countries such as the U.S. already use military simulation systems (Milsim) and virtual reality devices to carry out training.

In this context, the Milsim video game genre stands out as a **potential source of defense information** leaks that can pose a security risk. This is due to the confluence of the perceived low-risk nature of gaming environments and the usually high presence of military personnel with access to restricted information.
In this context, the efforts to represent military infrastructure, equipment, weaponry, tactics or procedures without a malicious intent, it is a potential risk for such knowledge to leak into criminals´ or terrorists´ hands.

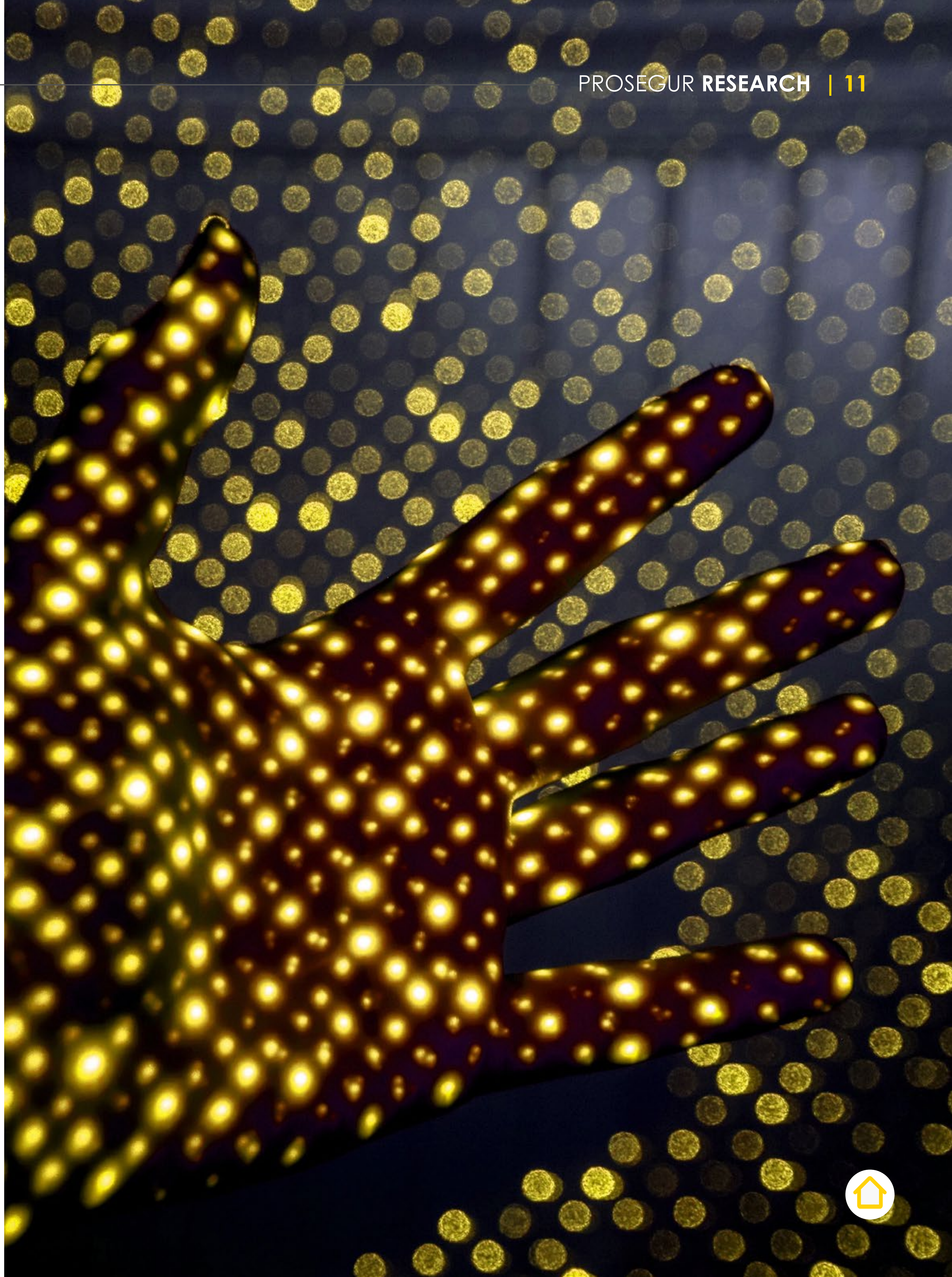
The metaverse as a criminal e-learning

In a context in which conventional communications are easily traceable by the authorities in charge of controlling the terrorist threat, **the metaverse is configured as an ideal scenario for the increase of activities of communication transmission and planification of operations for criminal or terrorist organizations.** This is due to the following factors:

- Metaverses based on the Sandbox principle would allow **scenarios of future attacks to be replicate**d with relative accuracy, improving the planning and future performance of terrorist assets. As an example of sandbox planning, it is noted that three of the 9/11 terrorists trained to **fly large aircraft** on a flight simulator, which probably had far less graphics power than any conventional civilian aviation simulator currently in use.

- It is very likely that the **progressive development of Artificial Intelligence** applied to NPCs (Non-Playable Characters) will make it possible to simulate an increasingly realistic response by security forces, emergency services or civilians, also contributing to the quality of asset training in the metaverse.

This criminal e-learning service is extensible to any group or individual with an interest in learning and intent to commit crime; and will facilitate communication, learning and strategy development more than ever before, challenging law enforcement agencies.



In addition to all these threats, the **legal challenge** posed by the metaverse must be considered.

The decentralization of the internet and the lack of adaptation of the legal system to this new reality greatly limits the possibilities for specific regulation of many criminal behaviors of users, as well as their prosecution and prevention. Additionally, the protection of privacy and intellectual property are two important issues raised by the theoretical and practical development of the metaverse.

Technology is a medium and the metaverse is presented as an **engine of change,** innovation and convergence. For this reason, we must not forget that it is the **human factor** that really generates the risks and has the ability to anticipate them and build a safe environment, in keeping with the technological development in which we find ourselves.

> In short, we are facing an exciting future, albeit not without significant challenges, on which to build a multidimensional interactive environment with great transformative potential.

PROSEGUR

We ensure the security of people,
businesses, and society as a whole.