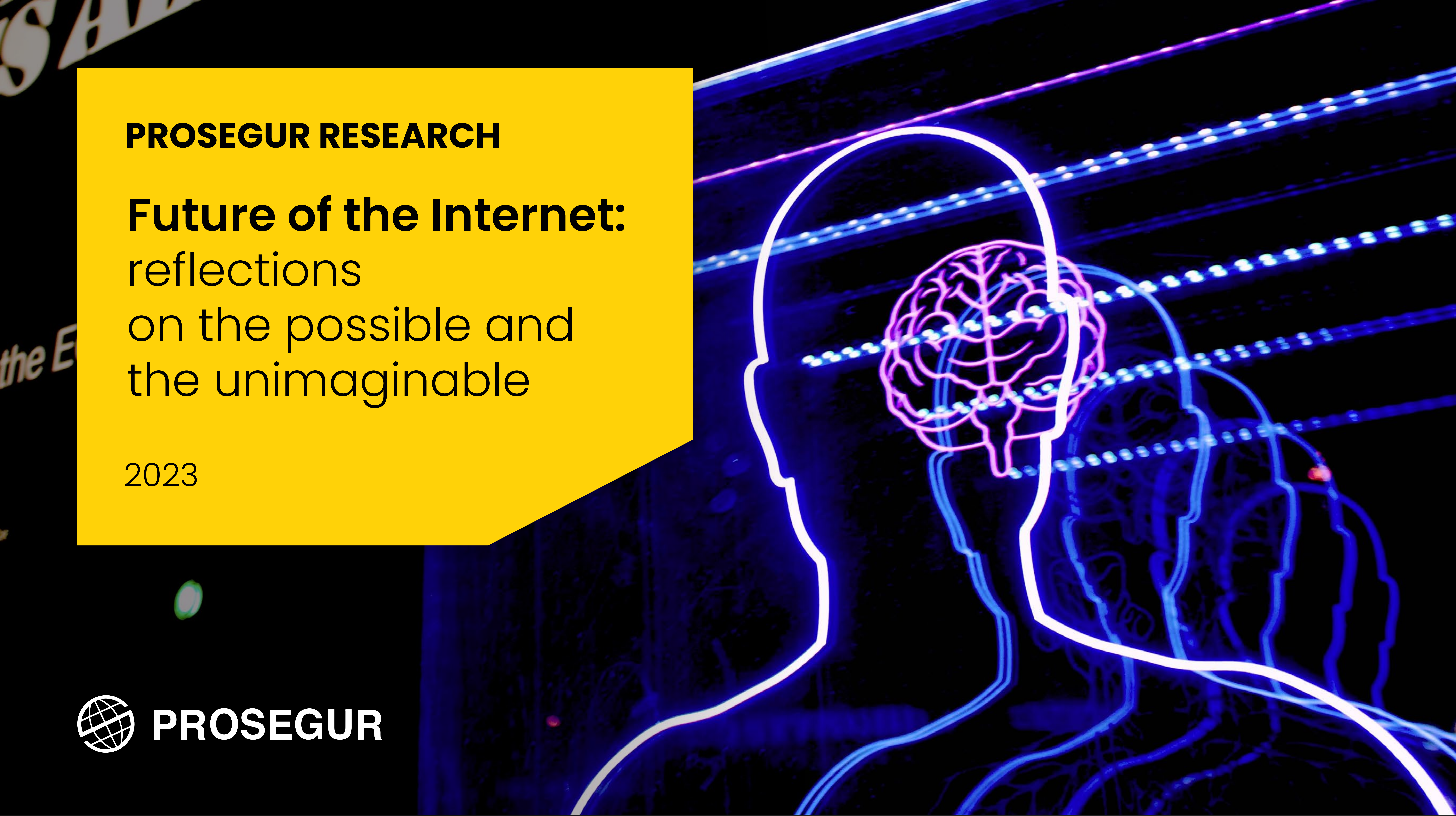


PROSEGUR RESEARCH

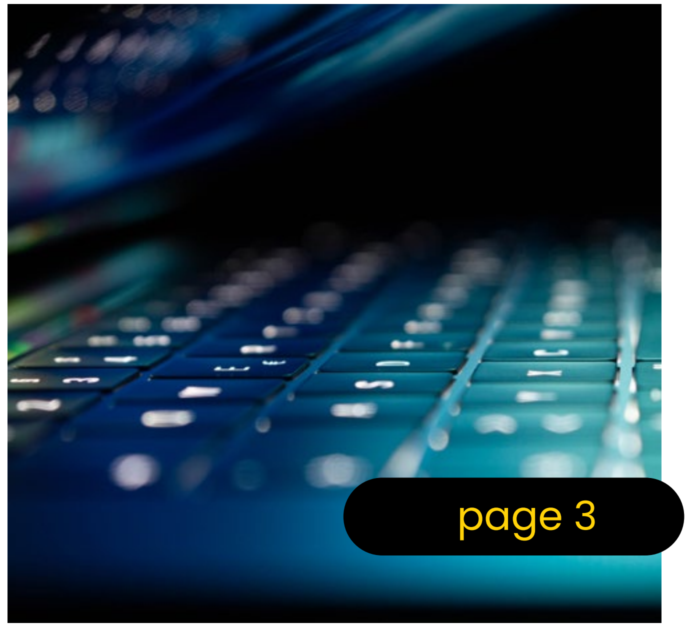
# Future of the Internet: reflections on the possible and the unimaginable

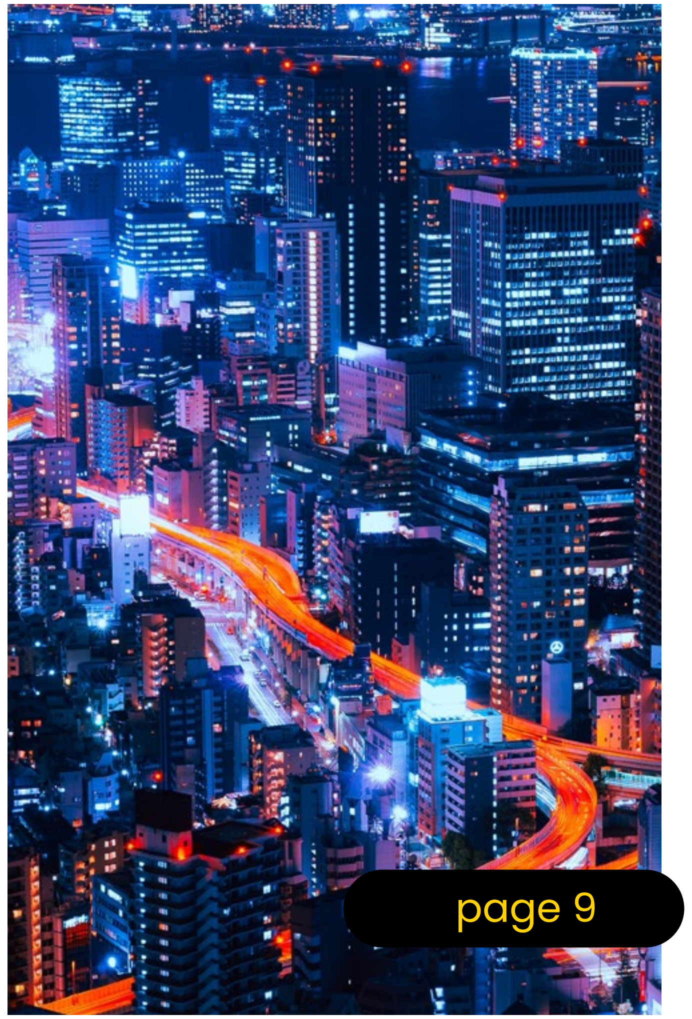
2023

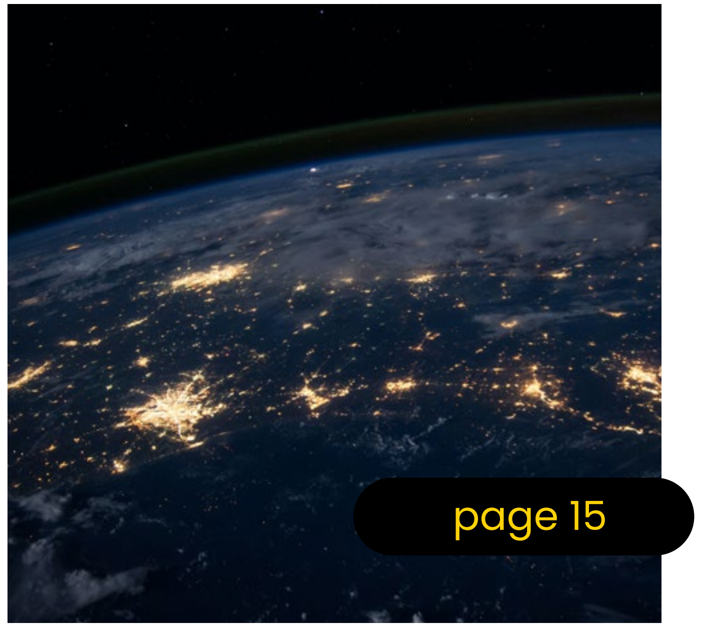
PROSEGUR

HOME

# INDEX







01

# Historical evolution: from arithmetic to influencers

HOME

# 01 HISTORICAL EVOLUTION: FROM ARITHMETIC TO INFLUENCERS

The development of the Internet has undergone **exponential growth** in terms of its capabilities and operability in recent decades since its **creation in the twentieth century,** which has revolutionized communication, access to information, business paradigms and, ultimately, the **democratization of content** around the world in a rapid, straightforward, and effective manner: the extensive features and applications found within a smartphone coupled with the conveniences and opportunities enabled by the Internet are just an example.

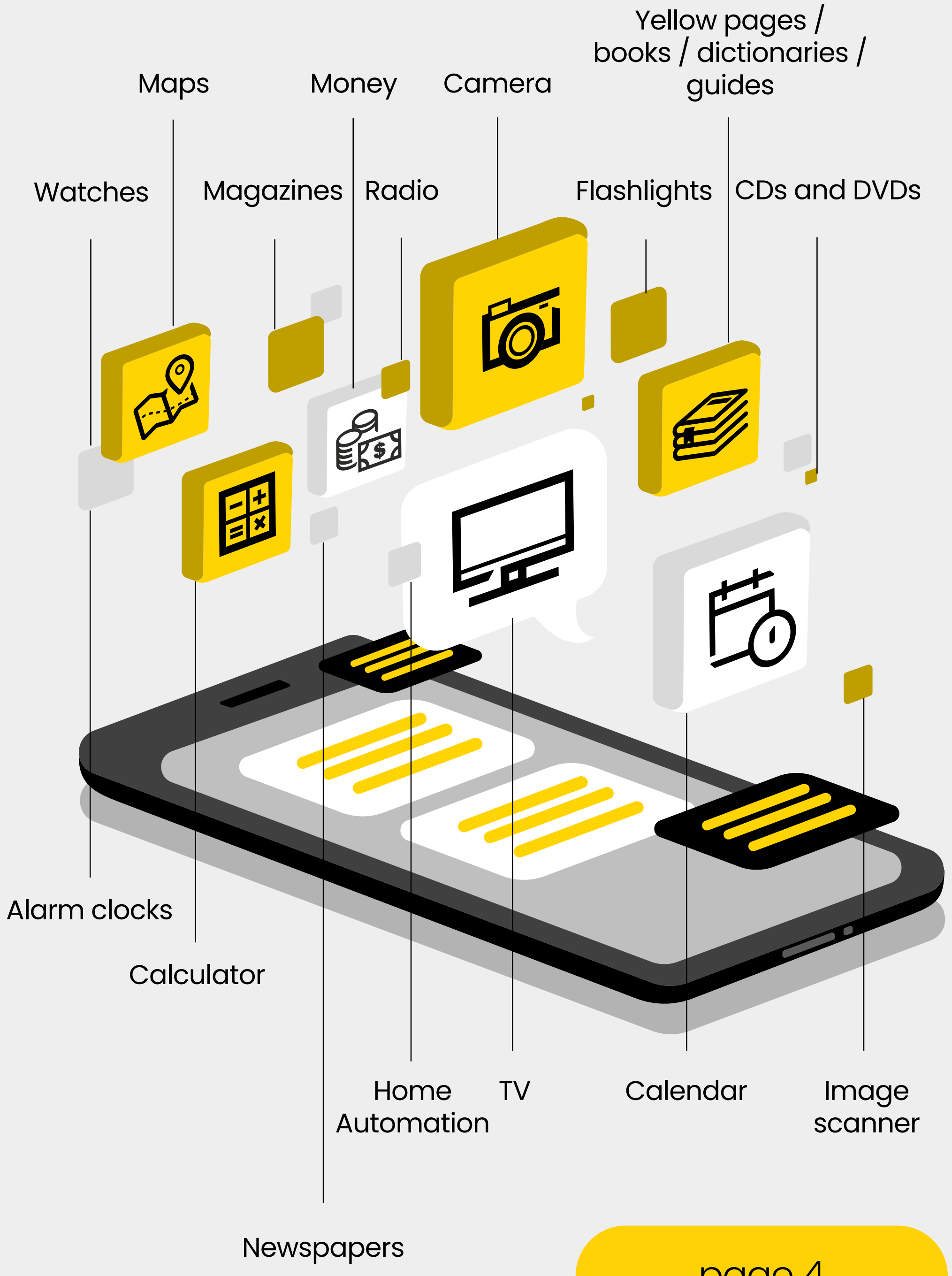
All these advancements have led to a genuine intertwining of the technology and the human being, giving rise to an entire stream of thought, literature and art known as the **human-machine binomial[1].**

According to the technologist Janet Abbate (2009), **the historical evolution of the Internet is driven by the necessity to forge a global network comprising interconnected networks** to satisfy human mathematical, military and later communication needs, developed eminently from the 1950s onwards by different authors, institutions and companies from different parts of the world. However, its rapid evolution and widespread acceptance among the general public, especially since the 2000s, as well as its potential capabilities, has given rise to technical challenges in recent decades. These challenges encompass domain scarcity, the **proliferation of illicit online activities** and the ensuing complexities associated with their identification, prevention and mitigation as can be seen in graphic 2.

[1] There are many publications on the relationship between human beings and technology and its various impacts on different spheres of human life, such as those by authors like the historian Yuval Harari *(Sapiens: from Animals into Gods),* the writer Edward Forster *(The Machine Stops),* the sociologist Manuel Castells *(The Information Age: The Network Society)* or the Wachowski film directors (Matrix).

Graphic 1
## The smartphone as a paradigm of the human-machine binomial

**Source:** Prosegur Research, 2023



HOME

## 1.1
## Historical background

Addressing the development of the Internet is a complex challenge, given the multitude of events and waves of innovation and technological progress that have shaped its trajectory and worldwide deployment.

**The origins of the Internet date back to the Second World War,** a period during which endeavors were made to develop **high-capacity arithmetic computers.** These early computers were not initially intended for a network interaction or communication with other users. An illustrative example of this era is the **Electronic Numerical Integrator and Computer** (ENIAC) project from the 1940s. This colossal apparatus spanned more than 12 meters in width and weighed more than 27 tons.

After the Second World War, in the context of the **Cold War,** the United States emerged as a technological powerhouse in this domain, creating in 1952 the Semi-Automatic Ground Environment (SAGE) project: a system capable of **detecting missiles from foreign nations through early warnings mechanisms.** Furthermore, in 1958, the AT&T Corporation launched the first **modems,** devices designed to convert digital computer data into analog signals from transmission over the telephone network.

In the 1960s, **time-sharing operating systems** gained widespread popularity, enabling multiple users to concurrently operate different programs on a single computer. In this context, **increasing globalization** led to the large-scale creation of **commercial networks** available to users. Hence, in 1964, American Airlines and IBM completed the **SABRE project,** an online reservation system connecting as many as 2,000 terminals throughout the United States to a central computer.

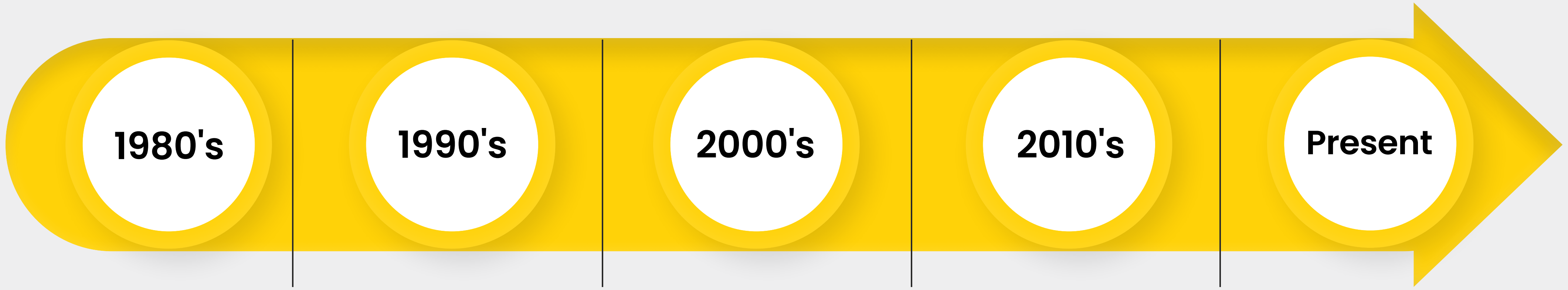
As a result, new research networks with increasing complexity emerged, enabling the interconnection of numerous computers, and paving the way for the popularization of the technique known as packet switching. In this regard, **projects such as ARPAnet (1969) for military purposes in the United States, NPL Mark 1 (1969) in the United Kingdom and CYCLADES (1972) in France, the latter two connected in 1976 to the European Computer Network, stand out.** In addition, 1973 saw the popularization of **Ethernet** by Robert Metcalfe, a LAN system that introduced the concept of random access, facilitating the sharing of communication channels among multiple users.

Later, in the 1980s, the implementation of the standard X.25 packet switching protocol, known for establishing **virtual circuits,** gained significance, owing to earlier projects such as Canada's Datapac network (1977) or Japan's DXX (1979), among others. Likewise, in 1985 the **Domain Name System** (DNS) was created, allowing the search for domains on servers.

Graphic 2

**Evolution of cybercrime on the internet in last decades**

**Source:** Prosegur Research, 2023 based on Insofec Institute



Ian Murphy was sentenced in 1981 as the first hacker in American history, while Morris Worm (1988) marked the emergence of the first self-replicating malware.

Malicious code boom, trojans and sophisticated worms.

Creation of botnets, SQL attacks, attacks dns. Progressive sophistication.

Social engineering boom, ransomware attacks, identity theft. Exponential growth of cybercrimes.

HOME

It was during this decade that the imperative emerged **to develop a new system that would ensure a reliable connection,** ultimately culminating in the renowned **Internet Project.**

## The **Internet Project,** led by Vinton Cerf and Robert Kahn, formulated its architectural framework based on **two fundamental principles:**

**A**

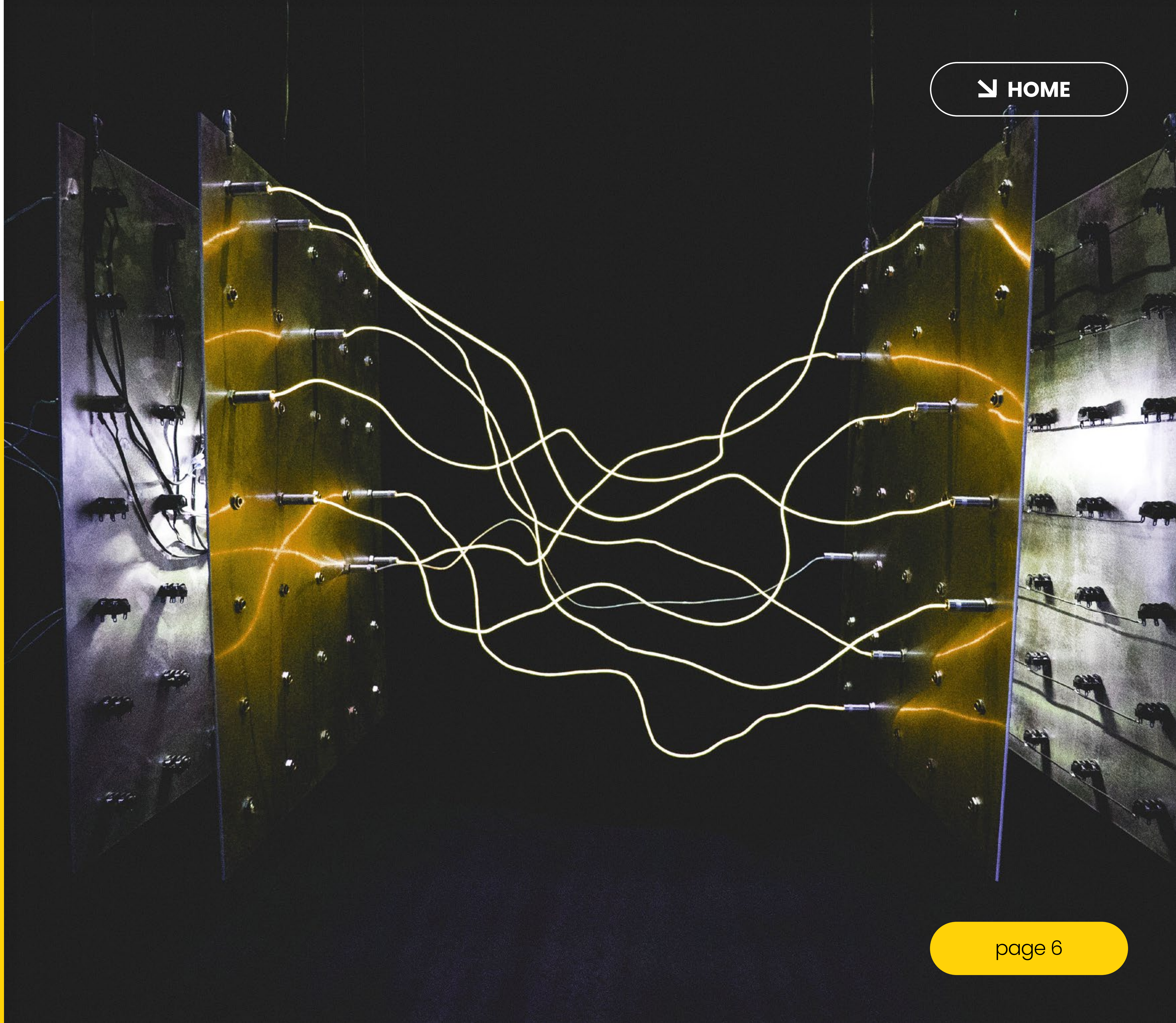
### TCP/IP protocols

Capable of establishing and maintaining connections between two host computer systems within a network.

**B**

### Gateways

Today known as routers, they determine the route that information packets must follow between networks.



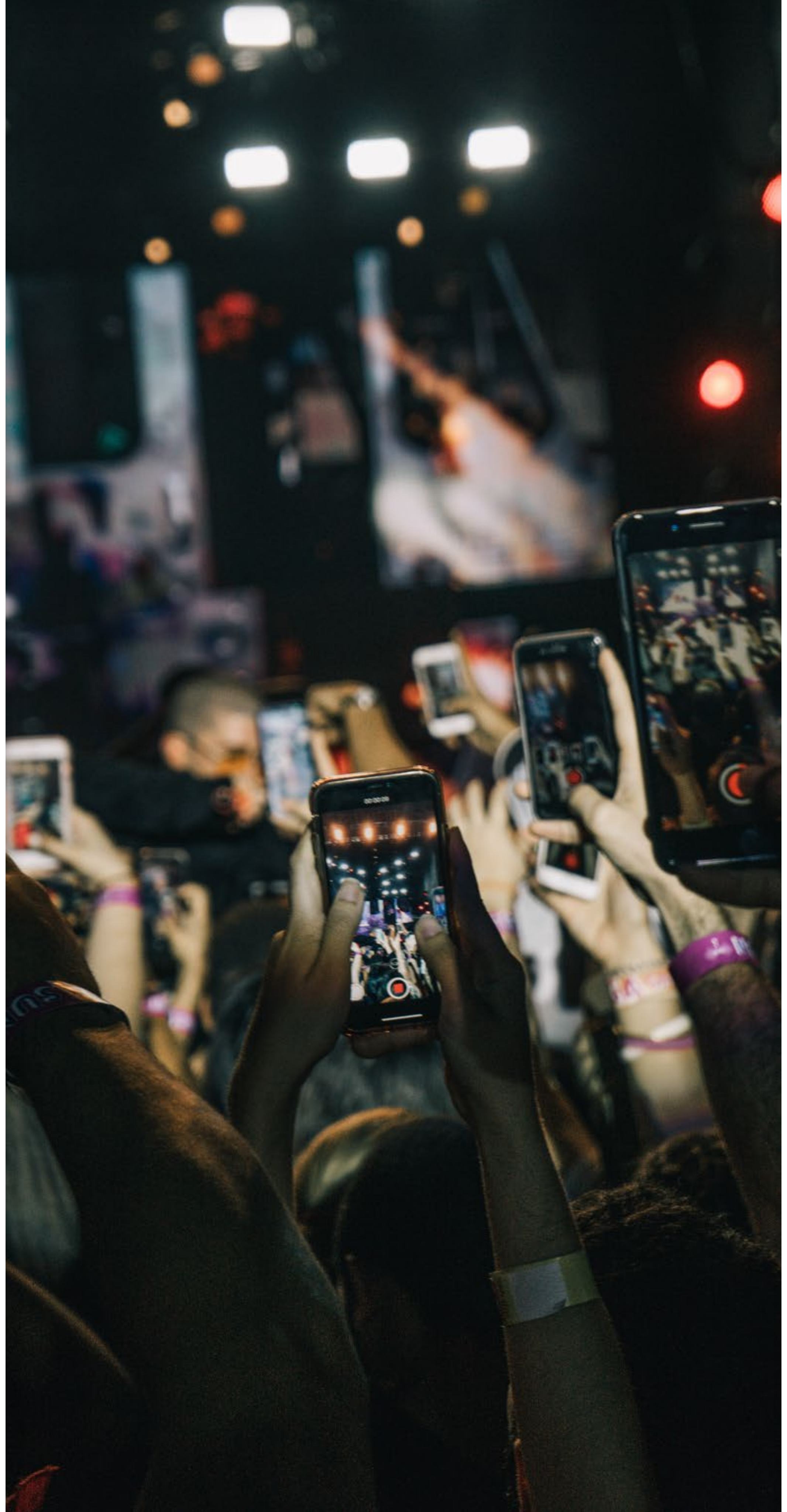
↘ HOME

## 1.2
## The World Wide Web: turning point and Web 1.0

All of these advancements culminated in a **turning point in the 1990s:** the creation of the **World Wide Web** (WWW) at the International Physics Laboratory in Geneva, with scientists such as Tim Berners-Lee, under the premise of a **collaborative space that would allow information** of all kinds to be shared.

Consequently, it was in the 1990s when the Internet experienced significant growth, as it transitioned into an **accessible tool for the general public.** This evolution was driven by the advent of user-friendly web browsers such as **Netscape Navigator and Internet Explorer,** which simplified web page browsing and facilitated the access to online information.

> Thus, the well-known **Web 1.0** came into existence, covering the period from 1990 to the early 2000s, **characterized by the creation of static, unidirectional web pages, with low connection speed and limited user interaction.**



## 1.3
## Web 2.0: active network users

It was few years later, during the 2000s, when broadband access saw widespread adoption, facilitating a **swifter and more stable Internet connection.** This expansion significantly boosted the growth of the Internet, enabling individuals to **access and share multimedia content in a more efficient and active manner.**

> **Web 2.0,** which came to fruition in the mid-2000s, is distinguished by the **active engagement of users in the network, promoting the creation of user-generated content, enhanced interactivity on websites and content personalization.**

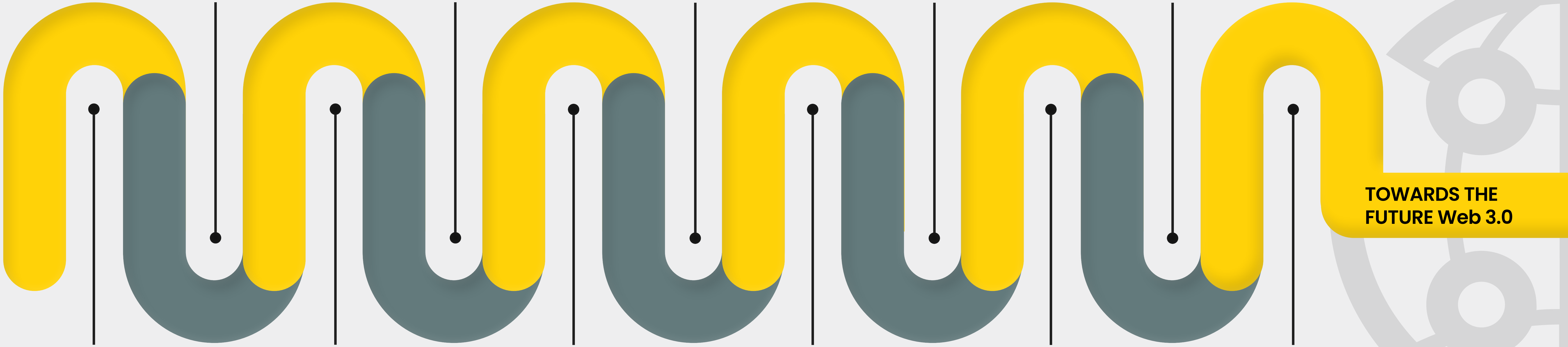
Moreover, this period witnessed the birth of globally renowned **social networks and platforms** worldwide like Facebook and Twitter. Additionally, the figure of **youtubers and influencers** in the digital realm gained prominence, although there were earlier precedents, such as the creation of Sixdegrees in 1997, regarded as the first-ever social network in history.

HOME

Graphic 3

## Key historical landmarks in the evolution of the Internet

**Source:** Prosegur Research, 2023



1943
**Electronic Numerical Integrator and Computer** (ENIAC)

1952
Semi-Automatic Ground Environment (SAGE):

1958
Modems

1964
**SABRE**

1969
**ARPAnet and NPL Mark 1**

1972
CYCLADES

1973
Ethernet

1980s
**INTERNET PROJECT**

1985
Domain Name System

1990s
**World Wide Web and Web 1.0**

2000s
**Web 2.0**

**TOWARDS THE FUTURE Web 3.0**

# 02

# The Internet of the future or the future of the Internet? Towards Web 3.0

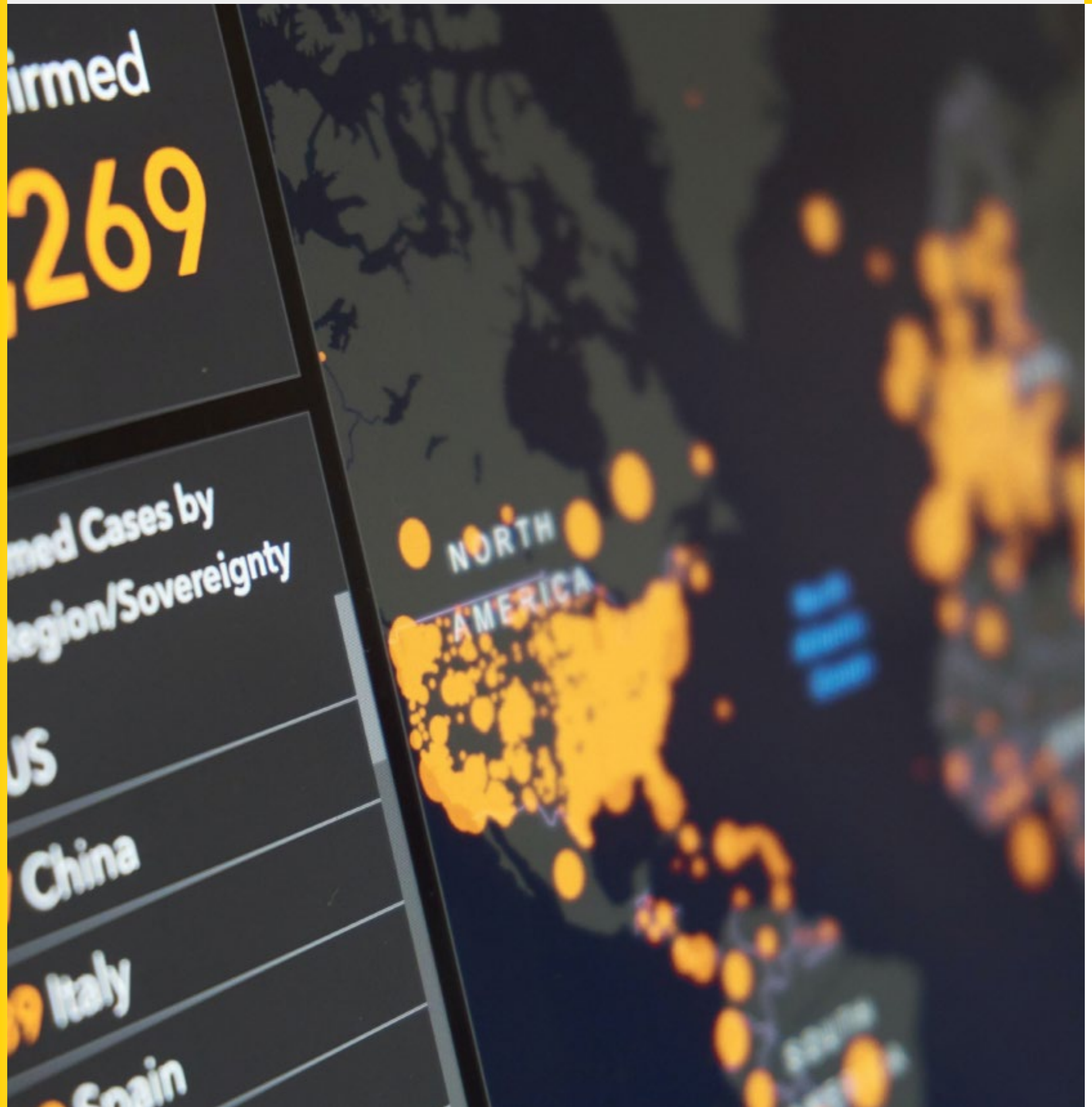
HOME

HOME

02

# THE INTERNET OF THE FUTURE OR THE FUTURE OF THE INTERNET? TOWARDS WEB 3.0

> The world has never gone this fast... and it will never be this slow again
>
> ***Martin Lindstrom,***
> CEO of Lindstrom Group



Analyzing the future of the Internet, or what the Internet of the future might become if it continues to evolve in its current conceptualization, demands a thoughtful and, to some extent, retrospective analysis. Therefore, a potential initial approach could involve **revisiting past notions regarding the internet´s future state** - its anticipated evolution - and assessing the extent to which these notions have been realized.

Regarding this matter, the Pew Research Center has been conducting diverse studies, consultations and surveys on the Internet´s evolution for decades. These efforts have engaged experts in the field, along with private organizations and public institutions:

Ⓐ

In 2004, over 1,000 individuals revealed that 66% of respondents consulted expected a massive and devastating attack on the country's information infrastructure or power grid within the next 10 years. Furthermore, 57% believed that virtual education would become more popular worldwide within formal education, with students being organized into classrooms based on their interests and skills rather than age. Additionally, an impressive 32% foresaw secure online voting to be implemented worldwide by 2014[2].

Ⓑ

In 2010, 76% of the 895 people surveyed believed that the use of the Internet by 2020 would have increased human intelligence, due to greater access to information. However, 32% believed that the ability to read, write and interpret information would be impaired[3].

Ⓒ

In 2014, in a study on digital life in 2025 garnered insights from over 2,000 respondents. Among the most prevalent predictions were those pertaining to the impact of artificial intelligence on human life and big data, envisioning increased awareness of the world around us and our own behavior. In this sense, political awareness and social action would be facilitated, with peaceful currents of change emerging as new Arab Springs[4].

[2] See the study of Pew Research Center (2005).
[3] See the study of Pew Research Center (2010).
[4] See the study of Pew Research Center (2014).

Has there been a devastating mass attack across the planet in the last decade? Has online voting gained widespread popularity? Has human intelligence increased or decreased? Similar to every facet and realm of human existence, the response and interpretations that can be ascribed to the events of recent years are characterized by ambivalence and, to some degree, contradiction.

As noted in the previous section, **cybercrime has increased exponentially in the last decade.** At present, the world witnesses a **staggering 90 million cyberattacks daily.** Some of them have been known for their **global reach, such as WannaCry, although their effects have not been totally devastating** as forecasted in 2004. Likewise, in-person voting remains the predominant method for citizens to exercise their **democratic right to participate in elections,** with some exceptions in limited countries such as Switzerland or Australia, among others. Ultimately, the debate surrounding the **Internet´s impact on human intelligence and capabilities** continues to be an ongoing subject of deliberation and contention. While some reports point to limited effects[5] and a lack of substantial correlations in cross-sectional studies, there have been indications of a decline in specific skills such as verbal intelligence, as well as a slight increase in the brain volume of gray matter and white matter.

In short, the evolution of the Internet has sometimes been characterized by **excessive expectations,** although it has undoubtedly revolutionized the lives of countless individuals and has transformed societies in various facets.

The wake of Internet development persists along this journey of transformation at all levels, leading to what is now commonly referred to as **Web 3.0:** an evolution of the current landscape encompasses the **searching and interpretation of the meaning embedded within online content.** Hence, it is often labeled as the semantic web. Ultimately, what Web 3.0 pursues is **decentralization and interoperability between systems and platforms,** so that data would never depend on a central platform and would always be accessible from different systems and applications, based on **peer-to-peer (P2P) protocols** and allowing users to manage and monetize their own data and digital assets. Likewise, the integration and convergence of technologies are set to become more prominent by jointly using developments such as mixed reality, artificial intelligence, or data mining.

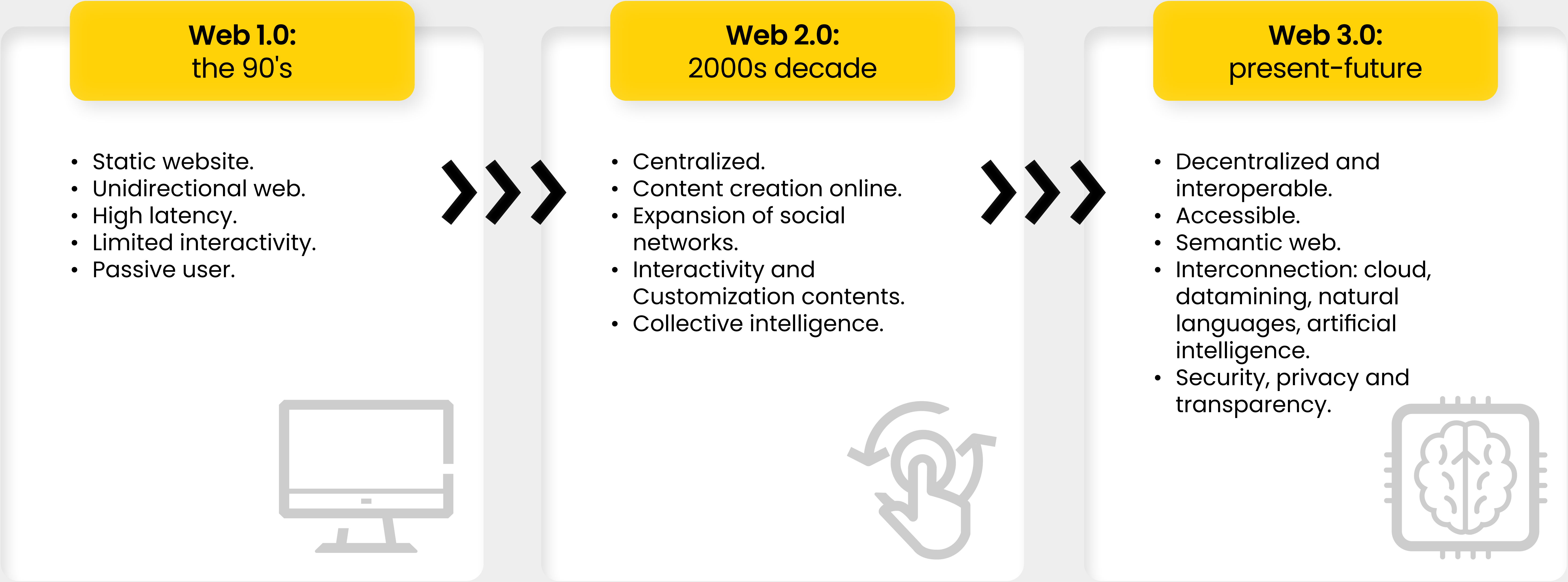
[5] See **Human Brain Mapping.**

HOME

HOME

Graphic 4

## Evolution of the Internet and World Wide Web



**Web 1.0:**
the 90's

- Static website.
- Unidirectional web.
- High latency.
- Limited interactivity.
- Passive user.

**Web 2.0:**
2000s decade

- Centralized.
- Content creation online.
- Expansion of social networks.
- Interactivity and Customization contents.
- Collective intelligence.

**Web 3.0:**
present-future

- Decentralized and interoperable.
- Accessible.
- Semantic web.
- Interconnection: cloud, datamining, natural languages, artificial intelligence.
- Security, privacy and transparency.

**Source:** Prosegur Research, 2023

Following the ingenious **Crypto Guide of The New York Times,** the Web 3.0 - sometimes differentiated from web3 by some technologists - would be owned by the users in the future the Internet, facilitated by **blockchain technology** and taking diverse forms such as the creation of decentralized social networks or 'play-to-earn' video games. This paradigm shift would give rise to a **new digital economy free from intermediaries or gatekeepers.** For this reason, the development of the Internet towards the web3 is related in popular culture to the **metaverse;** however, despite their obvious similarities, in terms of the integration and convergence of technologies, **web 3.0 is oriented towards the creation of an entire decentralized infrastructure that represents a new paradigm in the management of online content, while the metaverse refers to the creation of a virtual world in three dimensions that offers total immersion to the user.**

All of this could lead to a significant **revolution in the prevailing business models, cognitive and behavioral patterns, and operational methods across multiple industries, ultimately impacting societies at large.** Some of the **predictions for 2050** hint at outlandish innovations such as the introduction of nanobots in the brain for the retrieval of memories of loved ones potentially facilitating virtual reincarnation. Additional conjectures encompass the emergence of space tourism and the intriguing prospect of utilizing tree and plant photosynthesis for battery recharging, among others.

In fact, authors such as Carlos Oliva and Sara Gallego argue that the current pressing technological revolution is leading to a **"parallel sociological revolution"[6],** developing new business models and fostering innovative thinking, such as the possible trend of adoption of smart contracts based on blockchain technology[7].

Thus, advancements in Internet technology and new mobile connectivity networks, with 5G or 6G, collectively driving a **new industrial revolution[8]:**

> The first industrial revolution shattered energy barriers with the steam engine. The second skyrocketed productivity with the advent of mass production lines. The third improved sustainability and quality. The fourth, driven by the convergence of connectivity and data, is poised to eradicate knowledge constraints.
>
> ***Vicente Muñoz,***
> Global Chief IoT Officer de Telefónica

[6] See **Signo y Pensamiento.**
[7] See **IBM.**
[8] See *The fourth industrial revolution* by the founder of the World Economic Forum Klaus Schwab.

The incorporation of technologies in industries has led to the so-called **smart industries or smart factories, operating within the paradigm of Industry 4.0.** This endeavor aims to infuse new technologies including big data, into the sector, linking the physical realm, with machinery and products, to the digital realm, with computer systems and the cloud. As is common with technological trends, discussions regarding Industry 5.0 and even 6.0 have emerged, which redesign the collaboration between machines and humans, with special emphasis on intelligent spaces, the Internet of Things (IoT) and the metaverse.

However, as articulated by journalist and writer Esther Paniagua, **the technological development should not be only techno-solutionist,** which states that any problem has a computational solution. It is essential, therefore, to account for the psychosocial principles of people, **the value of culture and society and the broader economic,** political and social context of the historical era within which we find ourselves. Behind any **new technological innovation** process is a group of people, so that from the moment of its development to its implementation, **a good governance system must be guaranteed,** as far as possible, to ensure a dignified, equitable, secure, and private digitization.

Yet we must **look to the future with optimism,** courage, and positivity. An array of future challenges lies ahead, yet they are accompanied by **countless opportunities and possibilities for action,** to transform our lives from the personal to the professional sphere. In fact, certain studies claim that **digitalization** has the potential to create more than one million jobs in Spain alone in the forthcoming years[9], ushering in a profound **global shift in the paradigm of work:** according to the World Economic Forum (WEF), **the skills of up to 44% of global workforce are expected to change in the next five years**, prioritizing **strategic competences** such as creative thinking, analytical thinking, curiosity, resilience or flexibility.

[9] See the study of **Randstad Research.**

# 03

# **Internet and security:** present and future challenges across all spheres

HOME

HOME

# 03 INTERNET AND SECURITY: PRESENT AND FUTURE CHALLENGES ACROSS ALL SPHERES

While the new technologies discussed so far, such as the metaverse, web3, blockchain, artificial intelligence, mixed reality, or the Internet of Things, can help create a **prosperous Internet future,** it is imperative not to underestimate the **potential threats and security challenges of this common future,** one in which we will all have a stake.

## 3.1 Geopolitics and geoeconomics

### Ⓐ The Invisible Cables: The Undersea Iron Curtain

One of the main security threats is the **preservation of the physical infrastructure essentia**l for global data transmission. In this regard, counter to conventional expectations, **up to 97% of the world's telecommunications traffic is routed via undersea cables on the ocean floor.**

There is sometimes a tendency to overestimate threats in cyberspace to the detriment of the physical plane, with massive cyber-attacks or computer wars. However, some events in recent months, such as the **sabotage** of Nord Stream, have redirected attention to the protection of critical physical infrastructures. Hence, the c**onstruction and control over submarine cables have emerged as a key point of conflict,** accompanied by an escalating **geopolitical and geoeconomic** struggle projected to unfold in the coming years. This shift has been a**ccentuated by the growing global** sway of actors such as **China** in the last decade or the existing geopolitical confrontation around the **Arctic;** as underscore by Foreign Policy, we find ourselves in the era of the **Undersea Iron Curtain.**

In addition, the actions of **non-state armed actors** represent another potential threat in this domain, particularly with the rise of unmanned **underwater vehicles.** This evolution may pose a risk of **disruptions to the global telecommunications network in the event of attacks or sabotage.**

### Ⓑ Splinternet: hurdles in the cyberspace

One of the greatest challenges in crafting and nurturing the future Internet is interoperability and fostering open, unfettered access to data from anywhere in the world. In this sense, **international tensions** in recent years have been orienting actions in the opposite direction, with increased r**estrictions on Internet access** and **content filtering,** a phenomenon known as **balkanization or splinternet**. This trend, as highlighted by publications such as The Economist, have been regarded as a virtual counterrevolution.

Consequently, **various states are trying to bolster their dominance** in the IT field, prioritizing the construction of their own **"digital territories"** in partnership with large technology companies. Their overarching objective is to **assert their regulatory, ethical and privacy frameworks** for the future Internet.

Moreover, techno-regionalization can yield diverse consequences in geopolitical and geoeconomic terms, such as the imposition of fees, industrial **espionage, intelligence-gathering activities,** the **deterioration of trade relations among nations,** or the **prohibition of access to certain software or online plataforms,** as has been observed with Google, Facebook or TikTok, among others.

## Ⓒ Rare elements: another technological race

This apparent trend towards **technological deglobalization,** albeit partial, is intensifying the quest for supply **chain control** and dominance in the trade of some critical elements for technological development. As an illustrative instance, in 2021 China announced a slowdown in the export of rare earths, where it is estimated to hold an 80% market share and possess over 35% of global reserves, although new deposits are appearing in other regions such as Sweden or Turkey, potentially reshaping the market dynamics.

According to a prospective study prepared in 2020 by the European Commission, industries such as **renewable energy, mobility** or **defense** and **space** are some of the most prone to **disruptions in the supply chain of rare elements**, especially light and heavy **rare earths.**

Thus, the **crisis in semiconductors,** the **struggle for control of rare earths** and **commercial disputes** within this realm emerged as the most pivotal variables shaping technological evolution in the coming years. These factors hold the potential **to impede the progress** of new products and services in this field, while also contributing to pronounced **regional disparities** and **global inequalities across the globe.**

# 3.2
# Terrorism and organized crime

## A Uncontrolled criminal empowerment

**Organized crime has evolved over the decades,** and continues to do so, adapting to the economic, political, social, and even physical changes in the environment within which it operates. Technological development is facilitating and but also engendering novel criminal modus operandi that until recently were unimaginable, exemplified by the utilization of **deepfake technology** for identity theft or disinformation, among other uses. Therefore, certain are highlighting the **advancements** of artificial intelligence and machine learning as enhancers of criminal organizations identifying emerging **focal points of conflict** for the coming years, such as **'hackable' autonomous vehicles,** which could potentially be utilized in terrorist incidents, reminiscent of the tragic event on La Rambla in Barcelona (Spain) in 2017. Furthermore, there is a growing concern surrounding the so-called concept of data poisoning, where malicious actors manipulate machine learning algorithms to create X-ray machines insensitive to weapons at airports, for instance, or the prospect of **robots engineered to carry out thefts** in secure facilities arduous for humans to breach, among others. In fact, some **forecasts** by The Future Laboratory suggest that **by 2040 computers will commit more criminal acts than people.**

Moreover, Europol points out different **trends of change** for organized crime in the forthcoming decades, highlighting the use of **robotics** and **nanotechnology** as new criminal markets. Additionally, Europol anticipates that certain criminal activities will be carried out for **political motivations** rather than financial gain, potentially blurring the **delineation of power** between state and non-state actors, as suggested in various **studies** by Prosegur Research.

## B Radicalization, metaverses and virtual immersions

**Immersive virtual environments** offer myriad opportunities and benefits, such as the creation of virtual economies, innovations in medical and therapeutic applications or in the field of entertainment. Nevertheless, as in any technological advance, there are lights and shadows to be taken into consideration.

The latest **Terrorism Situation and Trend Report** (TE-SAT) has outlined **trends in the virtual ecosystem and emerging technologies** that may be poised to shape the evolution of terrorism in the coming years. Notably, the TE-SAT highlights that **boundaries between terrorist groups are blurring,** with motivations and narratives converging between different organizations across the ideological spectrum - from anarchism, extreme left or extreme right to jihadism.

Thus, the Internet can serve as a facilitating driver for **recruitment and propaganda** efforts, providing unfettered **access to violent content** on multiple communication channels over time. According to Europol, all these groups are increasing their operations and interest in the **metaverse and decentralized platforms.** These environments can be a source of recruitment and **online radicalization actions,** especially for young people. Additionally, they offer **prospects for training and simulation,** aided by the development of graphic engines and **hyperrealism** in recent years, notably within industries such as military simulation (MilSim) in video games.

These developments are giving rise to a flourishing ecosystem of **privacy technologies** and countermeasures against false or manipulated information, with the aim of preventing or mitigating these actions. Notably, significant strides have been made in areas like biometric signals, phoneme-viseme discordance or convolutional neural networks in computer vision.

## 3.3
## Cybercrime

### A The era of (cyber-in)security

**Technology has been a *game changer*** for criminal activities worldwide, opening up possibilities for action at all levels. As previously highlighted in various Prosegur Research **studies,** the boom in the use of the Internet in African countries, which are sometimes logistical hubs for wildlife trafficking, has amplified this illicit activity on the **Deep and Dark Web.** Similarly, there has been an surge in ***high-tech crime,*** with offenses such as **denial of service attacks, ransomware** or **remote access** trojans, among others.

Due to advances in the convergence and integration of technologies, it is foreseeable that there will be an increase in the use of what is referred to as **'cyberpower,'** representing yet another facet of dispersed power among both **state and non-state actors.** In fact, the United Nations University predicts that cybercrime in 2050 will be even **more fluid and flexible** than it is today, thereby enabling its **expansion into various sectors of society.**

### B Beyond the encryption

In the sphere of communication and the activities of terrorist and organized crime entities, **the encryption of messages and channels constitutes a key area.** A notable case in point is the **EncroChat operation** in Europe, which resulted in the arrest of more than 6,500 people and the seizure of 740 million euros in cash, in addition to 154 million euros in assets and bank accounts.

Hence, criminal organizations are prioritizing the search for new secure communication and financing methods to continue operating in criminal markets, beyond advanced encryption and encoding systems. In this regard, there has been recent interest exhibited by entities such as the **Islamic State** in **Non-Fungible Tokens** (NFT) and **Ethereum cryptoassets,** as highlighted by the Global Network on Extremism & Technology (GNET). These digital assets may serve dual purposes, enabling both **propaganda dissemination** and profit generation for potential attacks, all while possessing limited traceability. Furthermore, the use of **decentralized platforms** and the impact of Web3, as indicated by GNET, could make it **difficult to detect** their activities due to heightened data privacy.

HOME

### Ⓒ Data: weapons of math destruction

In alignment with author Cathy O'Neil's analogy of war, data has been aptly described as "weapons of mathematical destruction"[10]. **The safeguarding and responsible utilization of data,** encompassing personal, financial, commercial, and medical categories, represent paramount challenges for any organization. In this regard, Gartner has pointed out that in 2023 up to 65% of the world's population will benefit from the protection of their personal data under various **regulatory** frameworks, compared to the **10% coverage observed in 2020.**

According to the World Economic Forum (WEF), cyber-attacks are becoming progressively more aggressive and indiscriminate. Concurrently, ***crime-as-a-service*** is consolidating, with entities offering professional-level activities such as triple or quadruple **extortion, data and computer system hijacking, data breaches or denial-of-service attacks,** among others.

Moreover**, data is a self-contained market,** with everything from bank accounts to complete identity documents can be obtained on the Dark Web for prices ranging from **$20 to thousands of dollars.** This underscores the imperative of formulating robust data protection protocols, as well as greater data awareness. An exemplification of the latter pertains to the sheer time investment necessitated for parsing the privacy terms of major applications—a task demanding several days of continuous reading.

## 3.4 Society and culture

### Ⓐ Digital human rights: the power of disinformation

It is currently unthinkable to visualize and carry out foresight exercises without acknowledging the profound ramifications of the Internet across every sphere of contemporary life. Consequently, diligent progress is warranted in the sphere of **safeguarding human rights within the digital realm,** which is gaining special prominence as 2023 marks the 75th anniversary of the Universal Declaration of Human Rights. Thus, the European Declaration of Digital Principles and Rights has emphasized the need **to place the individual at the center of technological development,** as well as to ensure **sustainability, security, privacy, participation, inclusion,** and **freedom of choice.**

In this regard, the **proliferation of disinformation** in recent years on the Internet and social networks has led to a general **decline in trust in institutions and the media outlets.** Consequently, this erosion has resulted in **increased social polarization and civil unrest.** Furthermore, the emergence of **generative artificial intelligence and deepfake** capabilities holds the potential to magnify the effects and impacts of disinformation, as has already been experienced in recent years with the **impersonation** of world leaders and the well-known ***Frankenstein IDs*** in the field of cybercrime and **digital fraud.** According to Europol, the use of **deepfake technology** can facilitate the perpetration of acts such as **discrimination, humiliation,** or **pornographic extortion,** as well as produce **disruptions in financial markets, fuel document fraud or manipulation of information** that may harm **police and judicial investigations.**

Furthermore, some reports, such as the **Digital News Report 2023** point to the **fragmentation of communication services** embraced by users on the network. Platforms like TikTok and influencers have gained special relevance over traditional media and journalists. This transformation requires a review of policies, protocols and social campaigns against disinformation. The pernicious influence of disinformation on contemporary **democracy** and **socio-political stability** underscores the urgency of these efforts. Accordingly, some experts advocate for the concept of **'meta-ideological awareness'** to navigate this evolving terrain.

[10] See *Weapons of Mathematical Destruction:* How *Big Data increases inequality and threatens democracy.*

## B Deliriums in times of algorithms

The **hyperconnected society** in which we reside has ushered in a fundamental shift in the way we relate to each other, particularly in the younger demographic, with thousands of contacts at our fingertips.

The **metaverse,** this three-dimensional realm poised to connect the physical and the virtual dimensions, harbors the promise of an equally significant change in society. Nevertheless, as we are seeing, its evolution follows the **cycle of technological hype,** in which its capabilities and short-term expectations have been overestimated. The adoption of new technologies in **mixed and extended reality** raises potential concerns for the future: if we are able to build an avatar with the characteristics and the life we dream of, what compels us to disconnect from that parallel life?

Some authors are considering the possible sources of conflict associated with these advancements, including the concept of **persuasive computing** or the **dissociation of reality.** For instance, the possible increase of the **Proteus effect** is highlighted, whereby people who create avatars in digital environments (video games, among others) tend to assume specific traits of their avatars, leading to behavioral changes and other problems such as **body dysmorphia[11].**

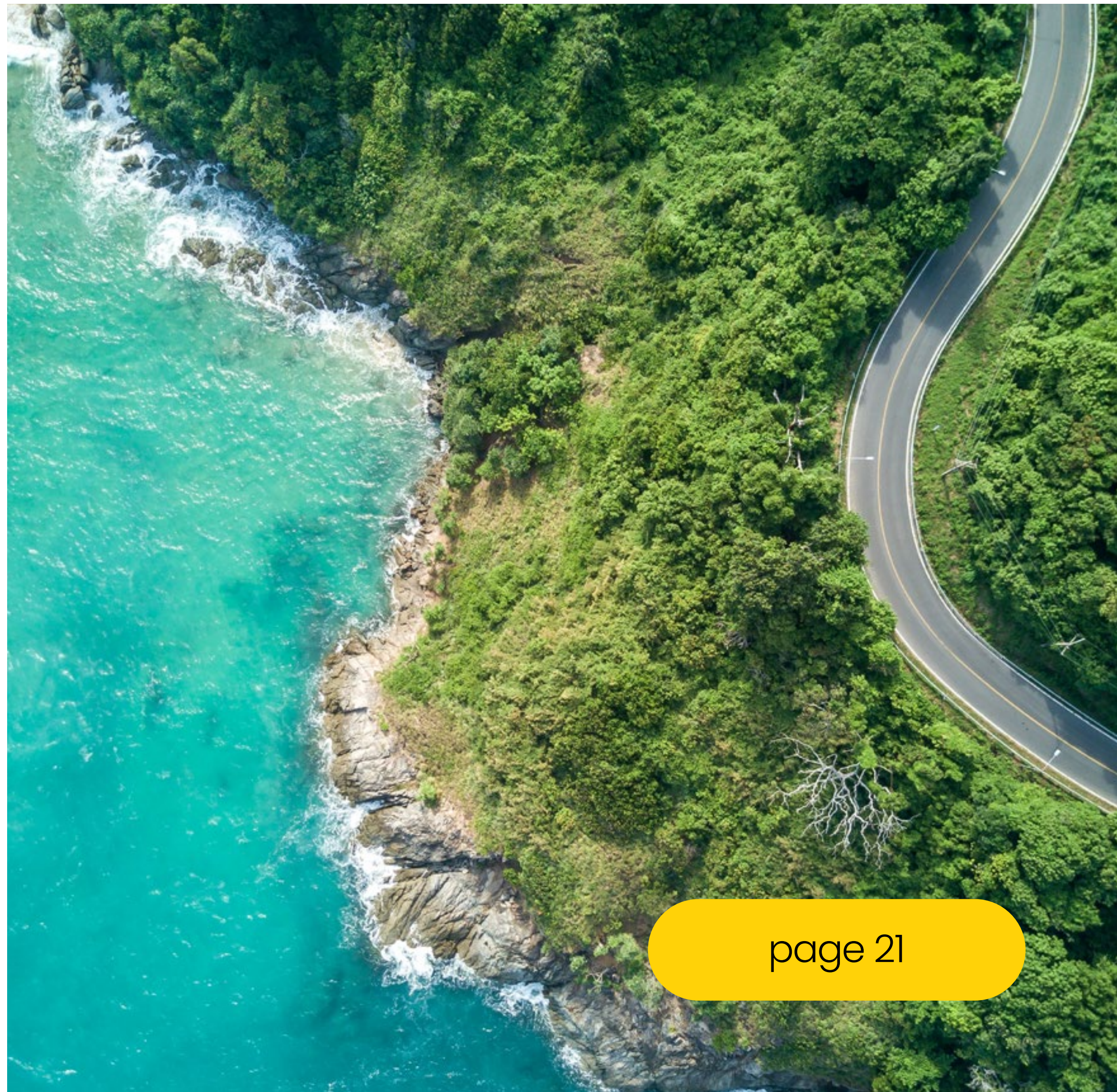
In essence, technological development towards the web3, the metaverse and generative artificial intelligence, among other innovations, has the potential to intensify the problems already existing in digital spaces as Paniagua points out, especially in terms of **addictions, discrimination, polarization and social fragmentation, and abuses.**

## C Green Internet: futuristic utopia?

Security permeates every aspect of our lives and, likewise, the environment around us. Thus, the **protection of ecosystems** must stand as one of **the main axes shaping the future** on which to base any technological development.

In this sense, we can find some apparently alarming data: for example, some studies claim that the artificial intelligence industry *(AI Industry)* has a larger **environmental footprint than the aviation sector;** or that bitcoin mining consumes **more annual energy than the equivalent of entire countries such as Argentina, Pakistan or Bangladesh;** or that a single data center consumes **more electricity than 50,000 households.**

The rise in **social awareness** and the relevance of **ESG criteria** in organizations will undeniably exert influence on the trajectory of technological development in the years ahead. While achieving a completely **eco-friendly Internet** with no environmental impact may seem utopian, we can, and indeed must, channel our endeavors toward the utmost preservation of the ecosystems that surround us.



PROSEGUR

We guarantee the safety of people, companies, and society as a whole

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com