PROSEGUR RESEARCH

Hybrid Security Series

The dystopian wave of artificial intelligence: a framework of competencies

2024

PROSEGUR
SECURITY

This is an **interactive document**

HOME

01

A tsunami called **AI**

HOME

01
A tsunami
called AI

02
In the face of
concern, reflection

03
Empowerment
as a habit

04
AI in an expanded
business
ecosystem

01

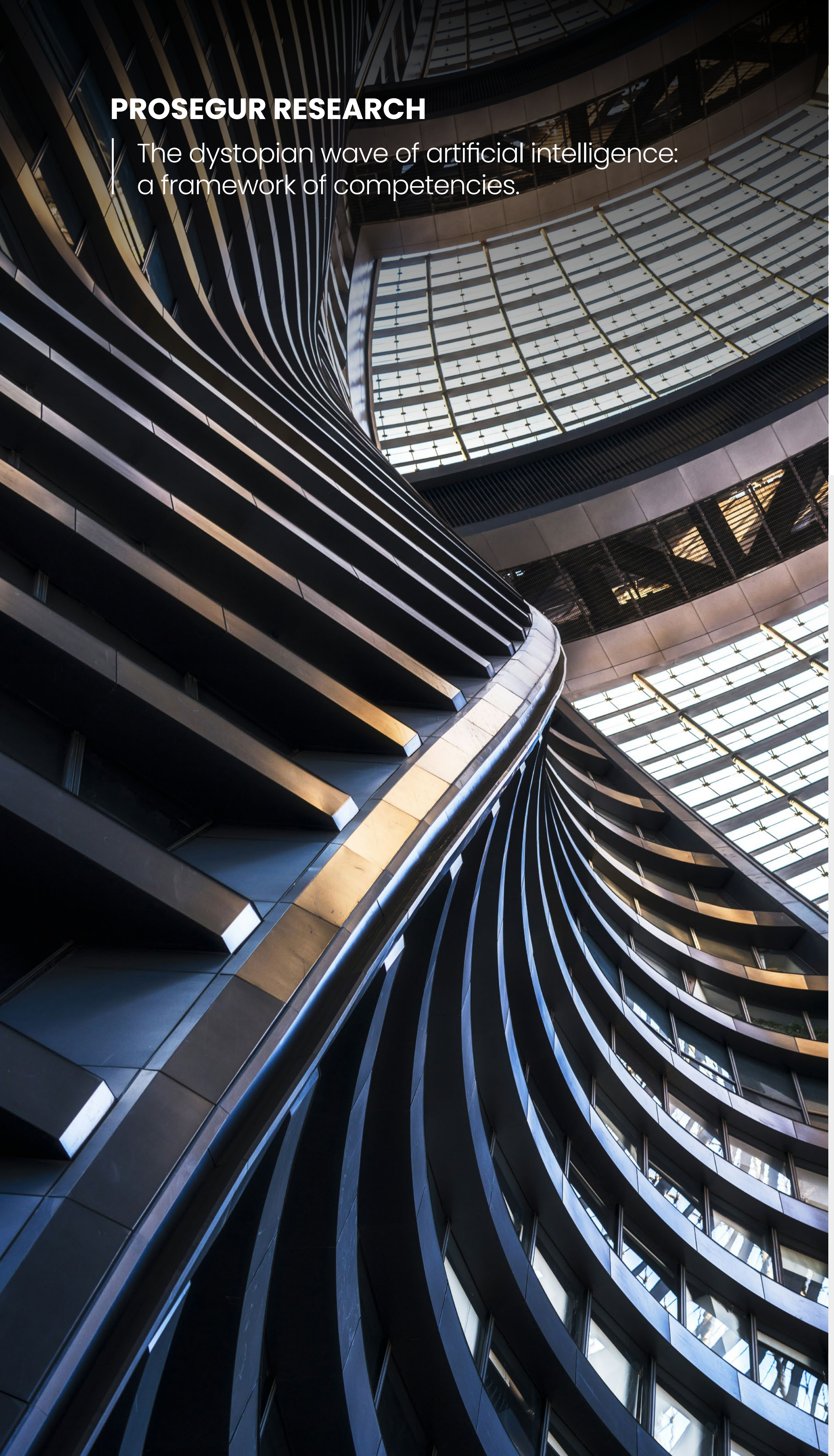
A TSUNAMI CALLED AI

Technology has been hand by hand with the human being since thousands of years ago, due to the human tendency to reinvent and seek solutions to complex problems. The first agricultural techniques, the wheel or gear systems are just a few examples. **Since the twentieth century, technological development** has lived with the internet an exponential growth that, as great wave of change, has gained great prominence given the opportunities and potentials arising from their convergence.

In this context, **artificial intelligence,** a concept as old as computation itself, and which was coined in the 1950s, has experienced **a great boom given the explosion of digital data and advances in computer processing capacity.** These waves of change contain important transformations for societies, and it is our present decisions on technological development the ones that will cause the impacts at multiple levels of tomorrow.

> **Artificial intelligence** (AI) is a "technology that applies advanced analysis and logic-based techniques, mainly machine learning, to interpret events, support and automate decisions".
>
> Within AI there's generative AI, a tool that along with other practices that define this technology -optimization, heuristics, machine learning, simulation-, offers the capacity to create creative and original content, simulating the behavior and reasoning that human beings follow in non-computer tasks.
>
> ***MIT***

HOME

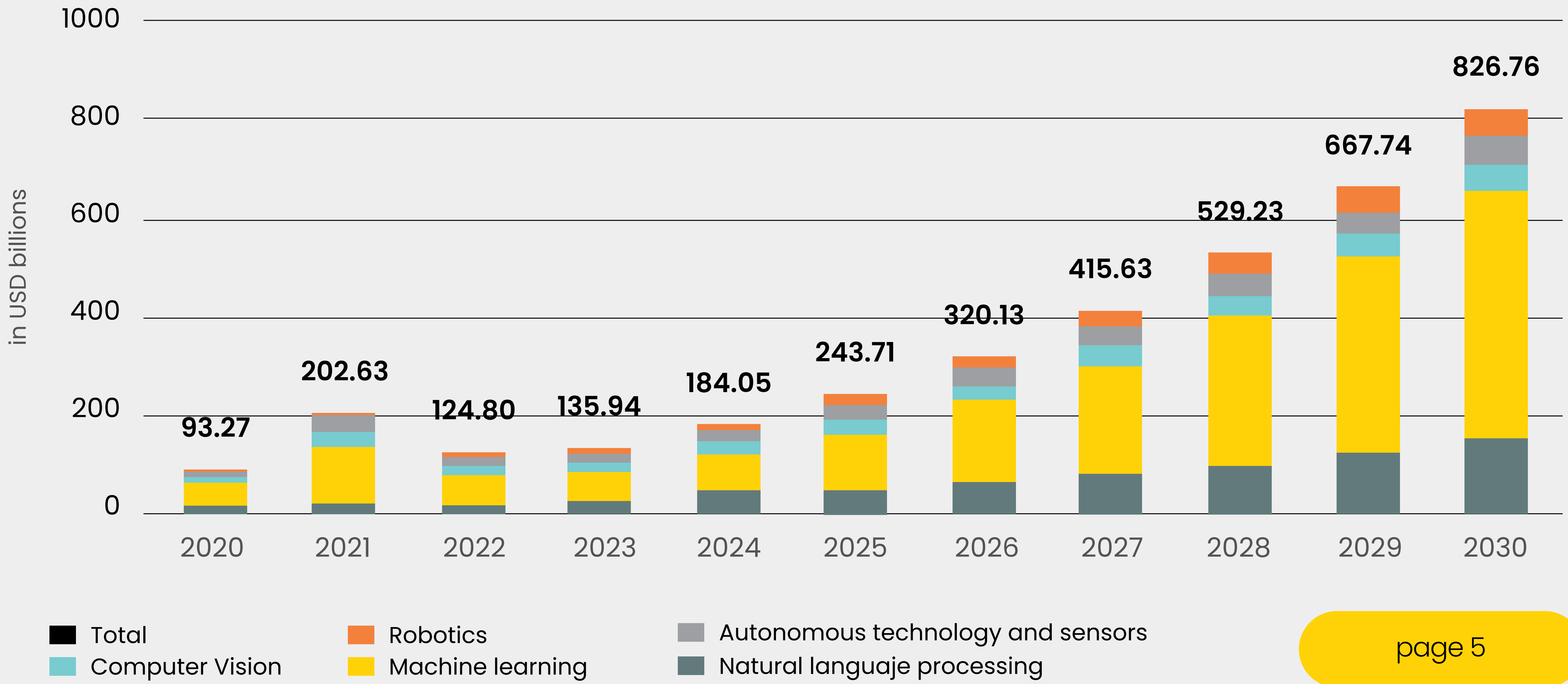


After decades of development, AI's role in the world market is expected to **record growth average annual rate of 28.46%,** up from €184 billion from 2024 to €826 billion in 2030. In this context, within the different modalities that AI integrates, it is estimated that those related to the machine learning and Natural Language Processing (NLP), represent the largest market volume.

Graphic 1

Volume of the AI market

Source: Prosegur Research, 2024 based on Statista Market Insight

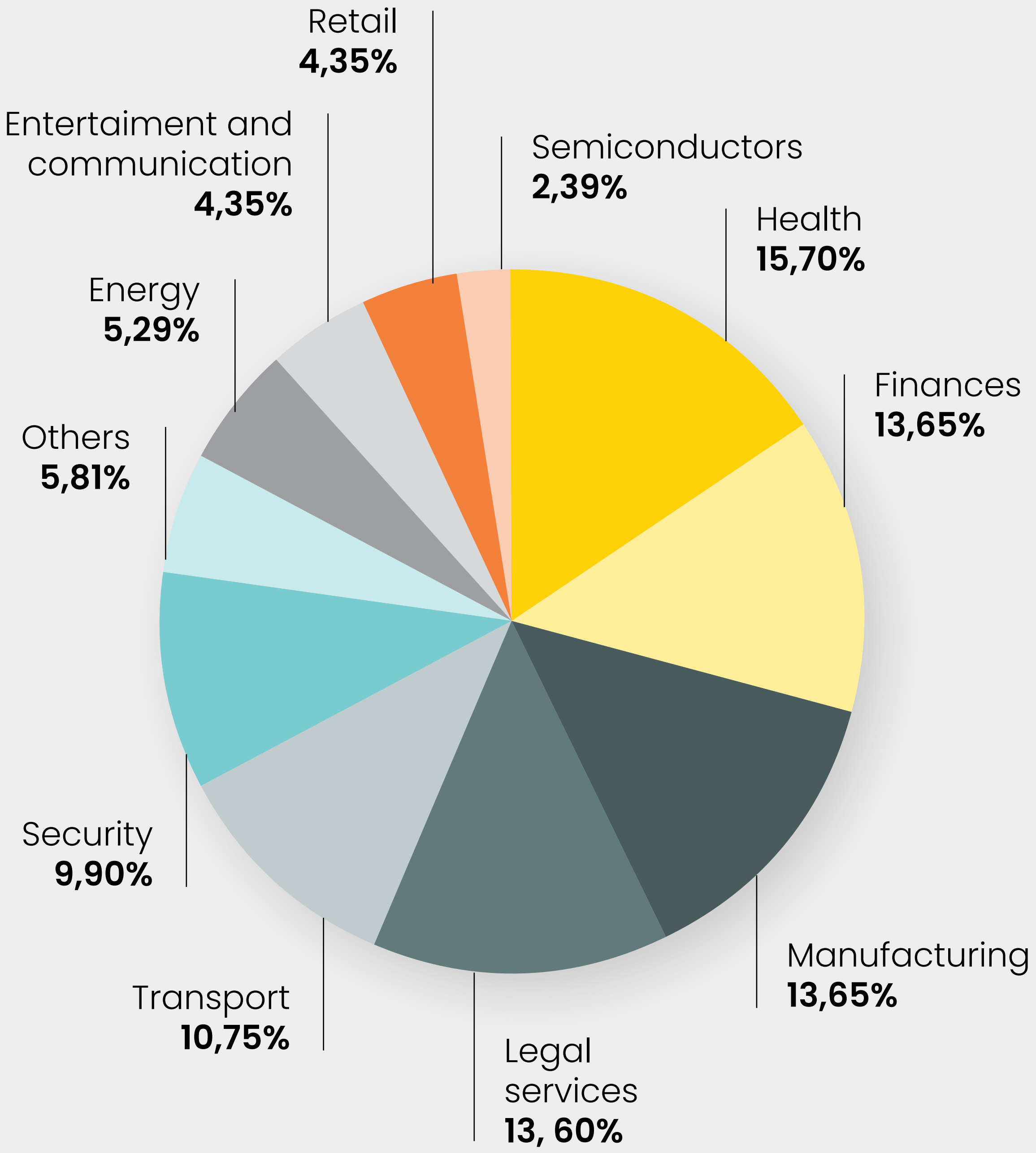


The democratization that presents the access of this type of technology has led to its inclusion in a wide range of fields, offering models that allow the classification or autonomous recognition tasks, and even the generation of original content. These new skills are expected to have high impact on the labor market. According to the IMF and **Standford, affecting 40% of jobs worldwide,** generating a transformation of the labor market by modifying technical needs for the workforce and enhancing computer skills, such as handling programming languages and data analysis.

The implementation of AI among the tools of organizations proves to be a disruptive factor, redefining the way traditional industrial sectors are conceived. According to the **Artificial Intelligence Index Report,** considering the volume of private investment in 2023, **it is expected that the areas related to governance/research, customer service, processing and management of data, medicine or Fintech have a greater impact and transformation by the use of AI.**

Graphic 2

Market volume by industry



Source: Prosegur Research, 2024
based on Statista Market Insight

↘ HOME

According to Gartner, every technology goes through a life cycle with a certain level of homogeneity, from its conception to its massive adoption and stabilization in the markets. The graph analyses the expected projection of AI, in its different types and aspects. *(See Glossary)*

Overall, AI would be suffering a **vertiginous ascent in a reduced amount of time.** Firstly, the peak of expectations, a phase of great expectation and enthusiasm within the conception of future implications, would be headed by Generative AI, followed by Responsible AI and General AI as outstanding technologies.

By not being able to comply immediately expectations and future tasks, usually little realistic, the AI would enter the valley of the disillusionment, decreasing the degree of attention media around it, as well as the emphases on its development.

After overcoming problems and limitations in the design, AI will suffer a sustained rise and moderated in time, **with a focus on the effective production of practical benefits.**

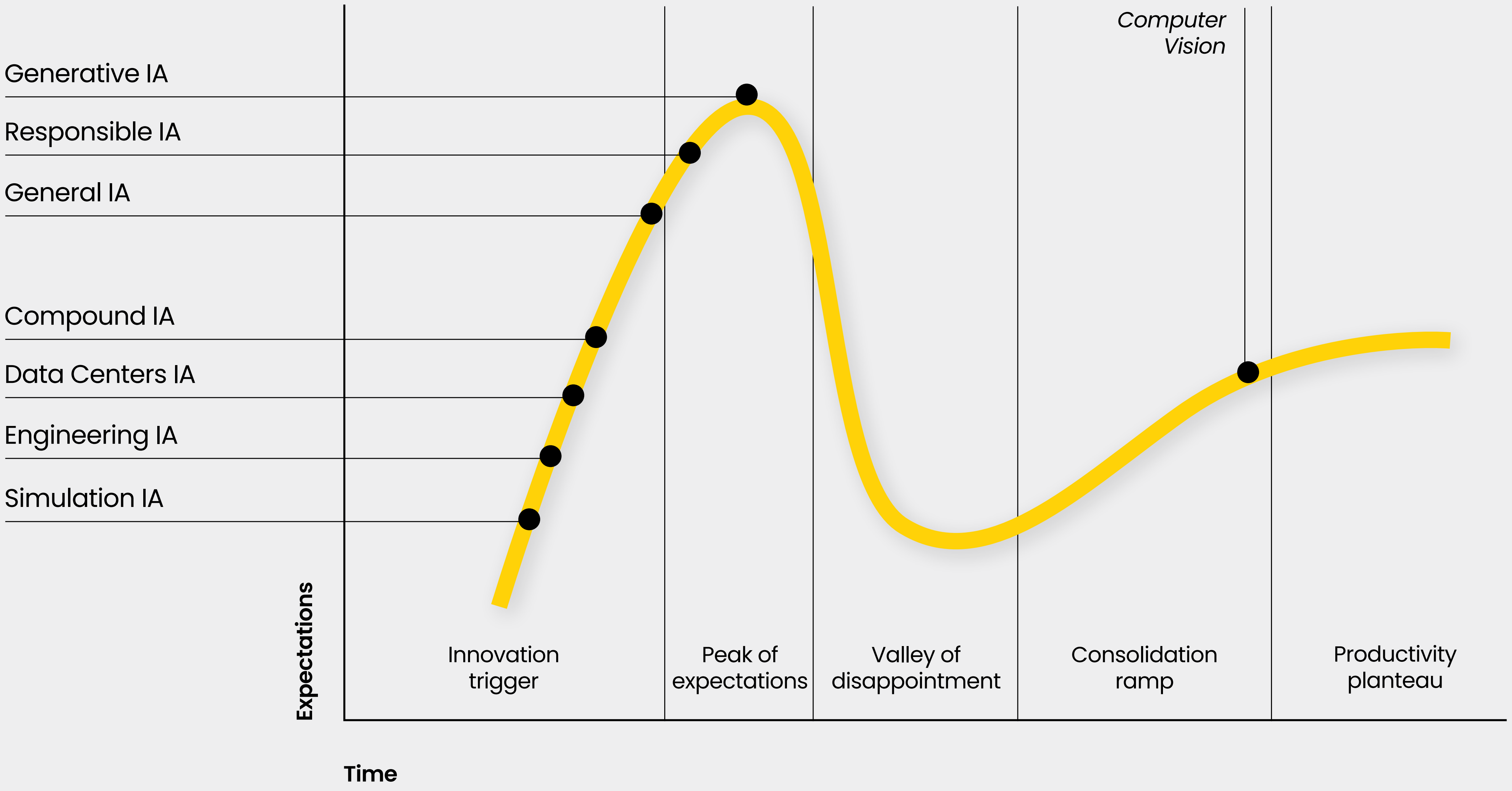
On the productivity plateau, technology will stabilize, **becoming an active and productive part of the market,** generalizing its adoption by demonstrating effective and efficient results.

Graphic 3

Gartner's Emerging Technologies Expectation Cycle

(Hype Cycle for Emerging Technologies)

Source: Prosegur Research, 2024 based on Gartner



Disruptive waves

Analyzing AI is past, present, and as a promising technology, **is thinking towards the future.** As if it was like a tsunami, the increasing implementation of AI in areas and sectors in an amplified way can lead to **disruptive waves that generate dystopian scenarios** related to the above concerns. Next, these are some points of interests shared:

A

Phygital world

- AI brings the physical and digital worlds closer together, causing **excessive dependency** on technology and accentuating the impact of **technological inequality.**
- Criminological phenomena combine more physical and digital behaviors, as well as **physical security** and **cybersecurity** are increasingly **interrelated.**

B

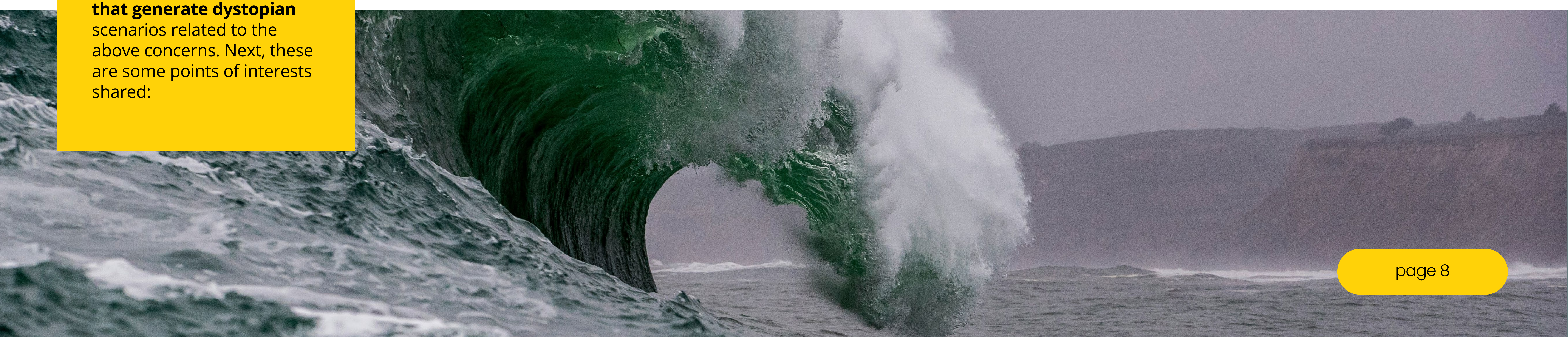
Changing the rules of the game

- Technological convergence goes faster than the regulation and adaptation of the system and modifies many aspects of society, while creating **new distributions of power and capacity,** affecting from organizations and countries to employees and citizens.

C

Artificial hallucinations and natural biases

- Depending on its programming, AI can **enhance biases and discrimination** in decision-making, especially in cases where people place high credibility on the machine.
- So-called **hallucinations,** or safe AI responses that do not seem to be justified by your training, are configured as another structural element that can create deficiencies in decision making.



D

Homo legalis

- Reactive over-regulation, without preventive measures or proactive strategies, could lead to a scenario where **excessive restrictions,** rather than fostering responsible development, could lead to paralysis in innovation and **technological stagnation.**

E

Consented data

- The transfer of data and its algorithmic use required for the operation of AI can generate enormous **privacy and ethical problems** if users lack due control, consent, and transparency.
- It is necessary to protect customer data; this is increasingly **demanded by the user.** In turn, in those who consent to its use, and this is ethical, allow to anticipate innumerable problems of safety, health, etc.

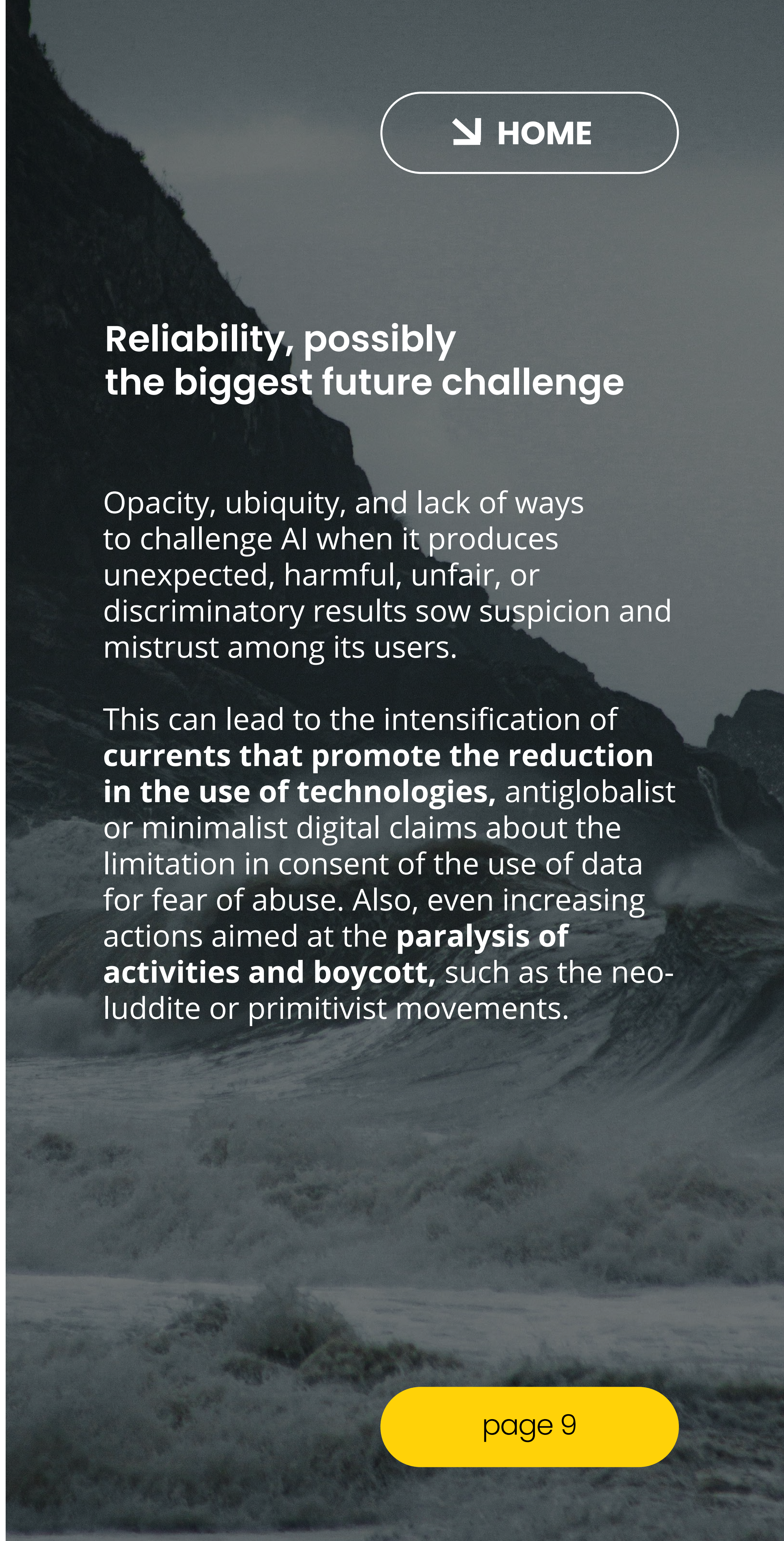
F

Uncritical thinking

- The ability to make deepfakes with video, image or voice adheres to the progressive increase of disinformation in news. This combination can lead to an **erosion of trust** in traditionally reliable sources of information, transforming critical thinking into cynicism and resulting in **disinterest in knowledge.**

Creating an **ecosystem of trust** based on legality, transparency and respect for human rights would allow the advancement and **innovation of AI** in a **responsible way and focused on good use,** from an ethical perspective in its design.

HOME



Reliability, possibly the biggest future challenge

Opacity, ubiquity, and lack of ways to challenge AI when it produces unexpected, harmful, unfair, or discriminatory results sow suspicion and mistrust among its users.

This can lead to the intensification of **currents that promote the reduction in the use of technologies,** antiglobalist or minimalist digital claims about the limitation in consent of the use of data for fear of abuse. Also, even increasing actions aimed at the **paralysis of activities and boycott,** such as the neo-luddite or primitivist movements.

02

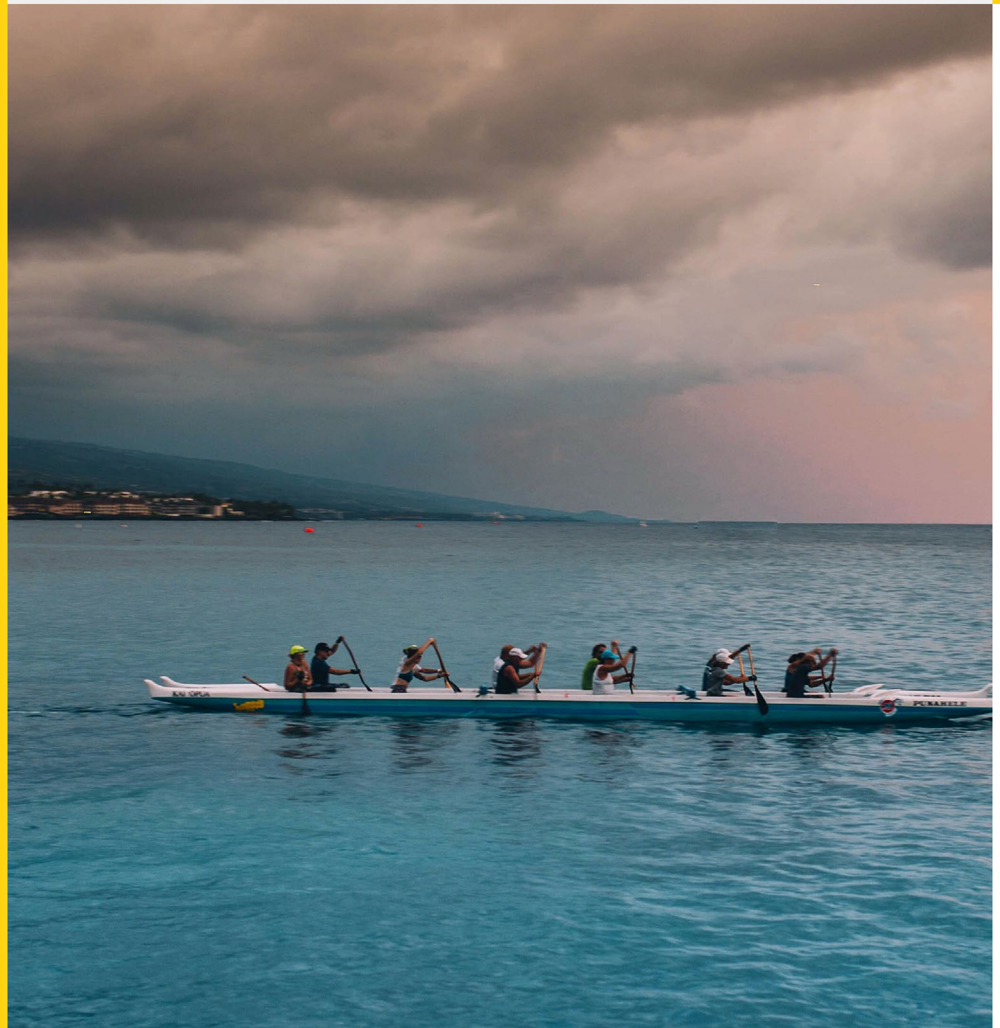
In the face of concern, **reflection**

HOME

HOME

IN THE FACE OF CONCERN, REFLECTION

> It's not that anything is on fire. It's that everyone in our organization is holding a flamethrower.
>
> ***Generative AI-nxiety,***
> **Reid Blackman**



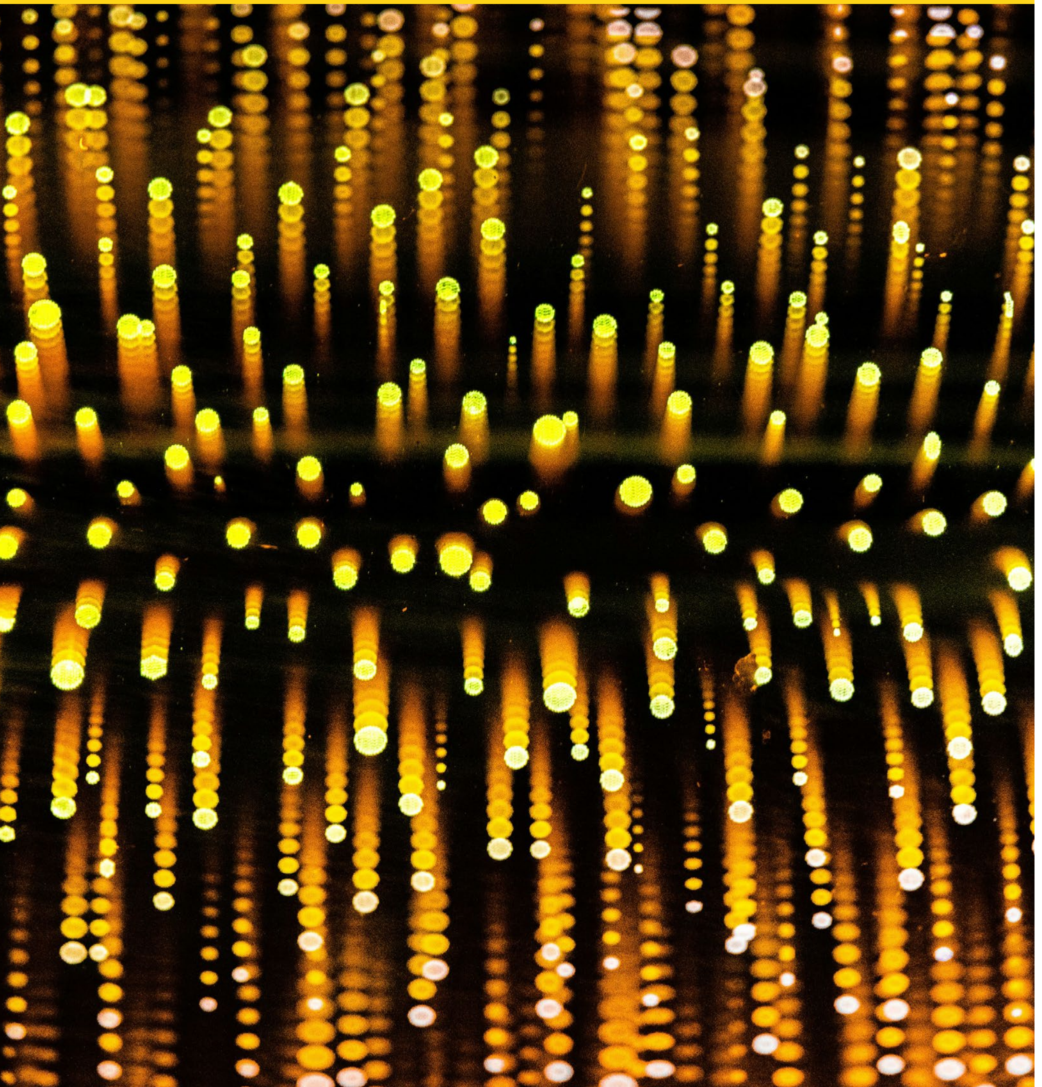
From the business point of view, and considering the multidisciplinary nature of AI, this technology shows a **double projection:**

- On the one hand, greater exposure to threats emanating from the digital sphere **increases the vulnerability of companies,** making AI a risk asset likely to create friction with aspects of law and even the integrity of security systems or protocols.
- On the other hand, it becomes the **core of the comprehensive safety strategy** while, as a tool, boosting the capabilities of employees in various work matters, increasing productivity, and optimizing costs.

Misuses

Artificial intelligence powers **illicit activities** in a variety of ways, from design and implementation to use.

Some of them may be:



Enhancing crime as a service

AI poses the risk of professionalizing cybercrime and facilitating the democratization of the provision of criminal services to non-experts. This dynamic is called by **Europol** as the shared criminal economy, where **crime as a service** acquires a growing relevance: the automation of attacks, the generation of malicious content and the optimization of botnet networks to facilitate denial of service (DDoS) attacks are just some examples of formulas that are difficult to mitigate, made efficient by AI.

AI for all types of fraud

The aforementioned ability of AI to design attacks based on social engineering is an important support for the commission of **fraud or traditional** scams thanks to preparatory tasks such as the impersonation of third parties that mislead potential victims or the management of mass distributions via mail. This can also serve as support for other types of computer crimes, affecting in many cases the physical plane, especially from within the company, such as **internal fraud.** In addition, AI is able to modify images and content in a substantial way without authorization, providing them with new meanings and illicit uses. It also powers information theft, particularly **intellectual property,** through malicious software or brute force attacks, which, along with the increased ability to analyze and process large amounts of information, is registering a great proliferation in **financial fraud.**

Great ally of organized crime

AI increases the sophistication and scale of organized crime activities. Optimization of **logistics operations** in all types of trafficking, analysis of large amounts of data for **financial fraud and money laundering** to gain sophistication or support in **surveillance and counterintelligence,** including the use of drones and information management to generate targeted attacks, are ways in which AI enhances criminal effectiveness and efficiency, without the need for a high level of qualification.

New ways for industrial espionage

The potential capabilities offered by AI in terms of big data analysis, network monitoring and social engineering make it a high value asset in the criminal environment related to industrial espionage, can be applied to tasks aimed at detecting strategic information, **automating surveillance or designing advanced attacks** against competing targets, including from the theft of key information to the identification of formulas to manipulate employees or customers in order to reveal confidential information. In the field of industrial property, in addition to data theft, the use of **reverse engineering** stands out, which can help break down patented products or processes to understand their internal functioning and replicate them without authorization.

HOME

Focusing on: **wAIponization**

Rapid technological developments have facilitated the integration of AI into a wide range of applications and stand as a double-edged safety weapon. Thus, its application as a tool in systems that may pose a threat has resulted in the emergence of a new concept: **“wAIponization",** which describes **the use of AI as a weapon in security contexts,** including both armed conflicts and criminal activities.

AI is already widely used for a variety of purposes, especially those related to passive security systems, such as **military operations planning, ubiquitous surveillance, pattern recognition and cyberthreat detection.**

This image has been created with generative artificial intelligence.

However, **their use in offensive decision-making,** target-setting, or the use of autonomous AI-powered weapons systems, stands as one of the main focuses of **weapon investment** in the medium term and poses important ethical-legal challenges in terms of responsibility and human control. Thus, **the reduction of the human factor in the conduct of hostilities** generates frictions around the degree of compliance with the **basic principles of jus in bello** of International Humanitarian Law.

In a context of increasing non-State violent actors, **AI empowers criminal organizations** and its use as a weapon accentuates professionalization by facilitating access to more sophisticated operational means.

In **armed conflicts or violent disturbances,** the widespread use of low-cost smart weapons enhances **asymmetry,** hindering the ability to control, anticipate and analyze the adversary; at the same time, paradoxically, empowers actors who until now had no comparable capabilities.

[1] WAIponization is the result of the combination of the terms ‘weaponization’, which refers to the process of weaponisation, and AI, which stands for Artificial Intelligence.

Good uses

Increasing human capabilities with artificial intelligence **allows both improving security and generating new products and services** for companies and people.

At Prosegur, we have integrated technology development and good uses of AI into our hybrid safety model to be more effective and efficient in delivering integrated, comprehensive security services, with the goal of making the world a safer and more prosperous place. Here are some of the infinite good uses of AI in the field of safety:

Pattern recognition

It allows you to analyze data from security cameras to **identify unusual patterns and behaviors, as well as detect intrusions in real time** and alert you of any incident. For example, in a computer vision store, the **iSOC-connected security guard** has information about suspicious behavior based on a proprietary algorithm that identifies potential thefts you understand.

People flow analysis and crowd management

It allows to **analyze movement patterns to optimize the provision of safety resources** and helps manage large crowds by identifying potentially dangerous situations. In security work for major musical and sports **events,** this analysis is carried out through the use of robotics that provides information on the capacity of the areas and needs for greater operational support.

Connected sensors and advanced alarm systems

It interprets sensor data to identify potential threats, such as fires, floods, or intrusions. **Sensors with integrated AI** are able to perceive fire when smoke is not yet detectable to human sight and smell.

HOME

Integration with management systems

It **allows iSOCs to operate by leveraging the convergence of technology, real-time data and the experts** who make security decisions. Now, with a very high level of analysis capacity, a more efficient allocation of resources is achieved in the whole set of linked security services: cameras, monitors, sensors, robots and drones, etc. This significantly improves detection and response to shoplifting, for example.

Models for the future

Algorithms and mathematical models can detect and anticipate areas of higher risk based on massive historical and current data, such as incident and crime information. The **great paradigm shift** comes hand in hand with the parallel use of real-time data, and the use of these to identify medium- and long-term courses of action.

HOME

03

Empowerment as a habit

HOME

03

EMPOWERMENT AS A HABIT

Although AI has seven decades of history, it has been during the last few years when its role as a **driver with potential for transformation in the labor landscape has increased,** empowering workers' capacities in organizations across all sectors to improve efficiency, productivity, and innovation. However, **the real value of AI lies not in replacing workers, but in empowering their skills.**

Currently, the challenge of training in technology, usually called **Media and Information Literacy (MIL),** is one of the main future axes for corporate and social development, in order to **maximize its benefits and minimize its risks as far as possible.** In this sense, the World Economic Forum (WEF) has identified in 2024 the adverse **results of AI as the sixth largest global risk** for the next decade.

According to some data, although 60% of all jobs have at least some tasks that could be automated, **only 5% of jobs could be fully automated.** This, **far from being a threat, represents an opportunity** of great impact for organizations: facilitating bureaucracy and the automation of repetitive and monotonous tasks would allow the dedication of working time to work that requires the most purely human capacities, such as those related to communication or the resolution of complex problems, among others. In addition, AI, along with convergence and overall technological development, can **generate fields and market niches in the future that now seem unthinkable.** Just think of the professions related to influencers or gamers, which just a few decades ago might certainly seem dystopian.

It is in this context that **intelligent empowerment** arises, a conceptual framework based on training and the improvement of human skills through technological application. Rather than substitution or mere complementation, **intelligent empowerment seeks a symbiosis between humans and disruptive technology** to expand the range of opportunities at all levels.

At the corporate level, a security company must adapt to a multitude of situations, actors, and contexts due to its operational flows, since each client is unique and has a series of requirements and particularities. Under the framework of **hybrid safety, people are the very essence of the model,** since without experts you cannot carry out thousands of operations, controls, and daily reports at different geographical points simultaneously. Thus, following the **taxonomy of skills and competencies for hybrid safety** developed by Prosegur Research, the main **features of intelligent empowerment thanks to AI are highlighted below:**

HOME

1 **Security** skills

Due to widespread uncertainty today, remembering terms like VUCA, BANI or TUNA, companies require **professionals with knowledge and experience in risk management and security to** adapt to the contexts and the business framework in which they operate, with a systemic vision and understanding the value and transversality of all organizational processes.

In the **data age,** artificial intelligence has become a catalyst for the empowerment of knowledge in various spheres and areas of today, from geopolitical and geoeconomic to social or regulatory, with multiple impacts on corporations. Thus, **AI has the potential to modify the way security professionals'** access, process and apply the information they have.

In this way, AI is **reconfiguring** the collection and analysis of information on global dynamics and trends. Access to information sources and the ability to analyze large volumes of data, media and social networks is one of the great areas of empowerment thanks to this technological development, with the aim of generating hypotheses, defining early warnings, identify trends or carry out evaluations of contexts with high insecurity, allowing to make more informed and effective decisions.

2 **Digital** skills

Technological development, interrelated with the evolution of corporate operations, requires security professionals who know the applications of the most disruptive innovations. There are currently many emerging areas, from blockchain to quantum computing, so companies must have **diverse teams, with multidisciplinary backgrounds and a holistic vision** of both technology and the organization itself.

In the digital component, security companies have witnessed in recent years the **gradual transfer of human behavior from the physical to the digital.** In this regard, increases in illicit activities such as **computer scams** and other threats to business continuity and reputation, such as industrial espionage or cyberattacks, are the result of malicious use of technologies. In this way, AI can play a relevant role in detecting malicious activities, such as social media interactions with criminal activity or mass publication of illicit content, using messaging and profiling techniques faster than human experts.

In the more purely technological component, knowing the design and implementation of innovations in the field, requiring hard skills as programming, allows **establishing operational services with greater knowledge of specific security needs,** like cloud tasks or digital twins, among others.

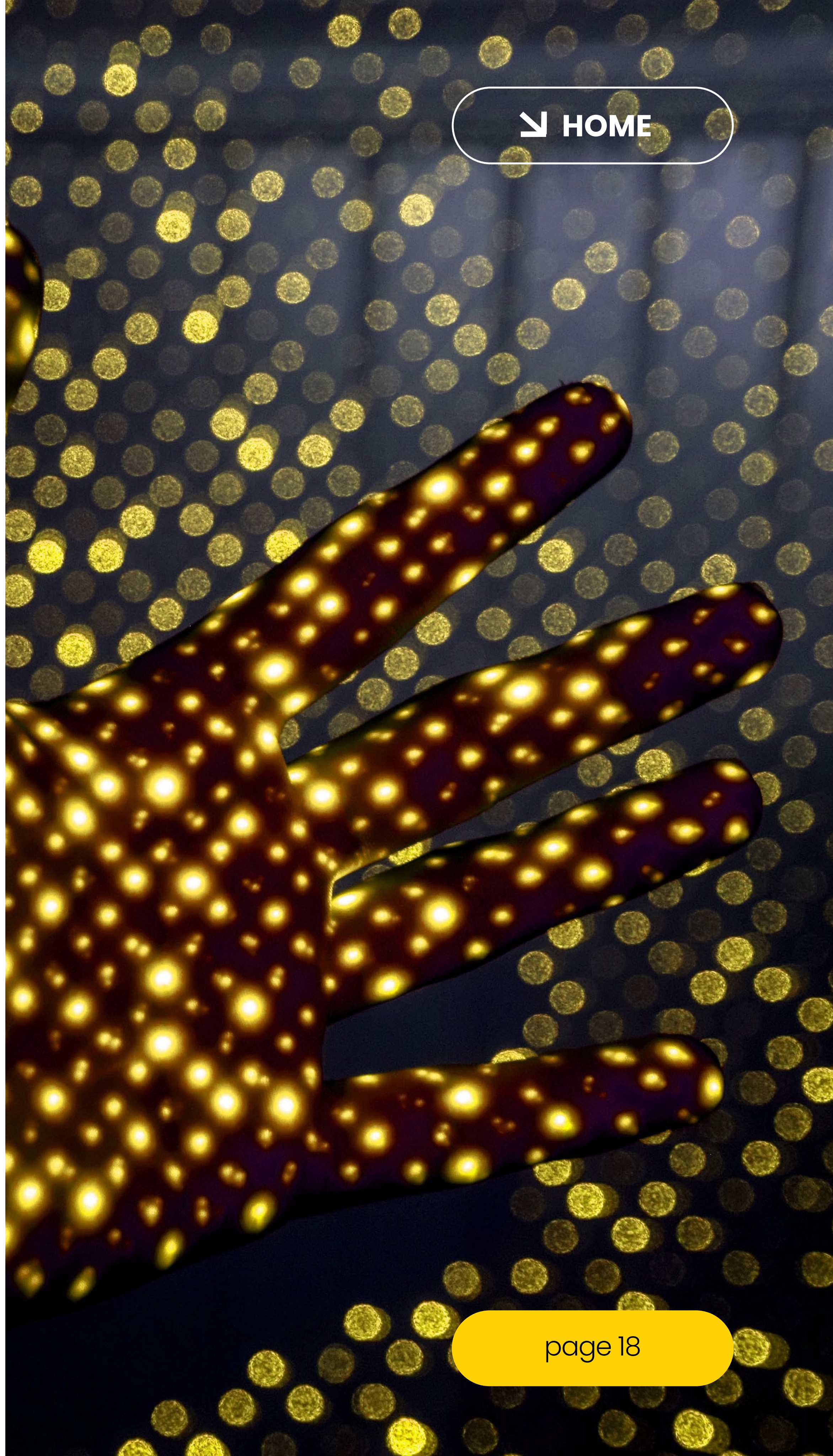
Therefore, beyond the existing and potential risks, AI can represent a significant advance in the capabilities of workers in security companies. For example, automated analysis of behavior patterns in video surveillance circuits can enhance the capabilities of security operations centers (SOC) and alarm centers, **overcoming that way the limitations and biases of human attention.**

3 **Human** skills

As noted above, purely human skills, known as soft skills, which include creativity, critical thinking, solving complex problems or empathy are **more necessary than ever.** Sometimes **technology contains biases,** since behind each technological development there is a group of people: from the definition of objectives to the selection of models and the interpretation of results people play a fundamental role. However, artificial intelligence can improve organizational capabilities through what has been called the **augmented workforce.**

Creativity and **analysis of adverse scenarios** require a complex mental process, overcoming limitations such as the innovator's dilemma with the aim of increasing the organization's competitive advantage. For this reason, AI by automating tasks and streamlining bureaucracy can eliminate burdens that workers have to deal with on a daily basis, reorienting their workday toward jobs that truly make a difference. In addition, the possibility of creating scenarios and simulations can allow departments and innovation specialists to identify new solutions aimed at specific security needs.

Moreover, the analysis of data through algorithms and new technological developments enables the identification of patterns of action or consumption of customers, allowing workers to detect and improve operational services and communication with them. This **generation of ideas and integrative thinking** makes companies evolve into such agile corporate ecosystems.



HOME

HOME

4 **Self-management** skills

In the dynamic and agile current context, with progressively more systemic and demanding environments, self-management is configured as an **essential axis to ensure a correct security service** for companies in the sector.

Professionals must constantly adopt **new learning strategies** according to the context in which they are, applying different tools relevant to each situation. Therefore, **Generative AI** (GenAI) represents an advance in the access and management of information, especially in intelligence capabilities in open sources (OSINT), highlighting some developments such as ChatGPT or Perplexity. For example, the analysis of large volumes of data on financial issues, technical-legal documentation, tenders, or reporting are just some of the areas in which generative AI has already involved an operational change. However, human capabilities such as critical thinking noted above should not be overlooked in these contexts: possible misstatements in AI results, the biases that may contain in its formulation or the interests and values themselves organizations not contemplated need a person to analyze and validate the results.

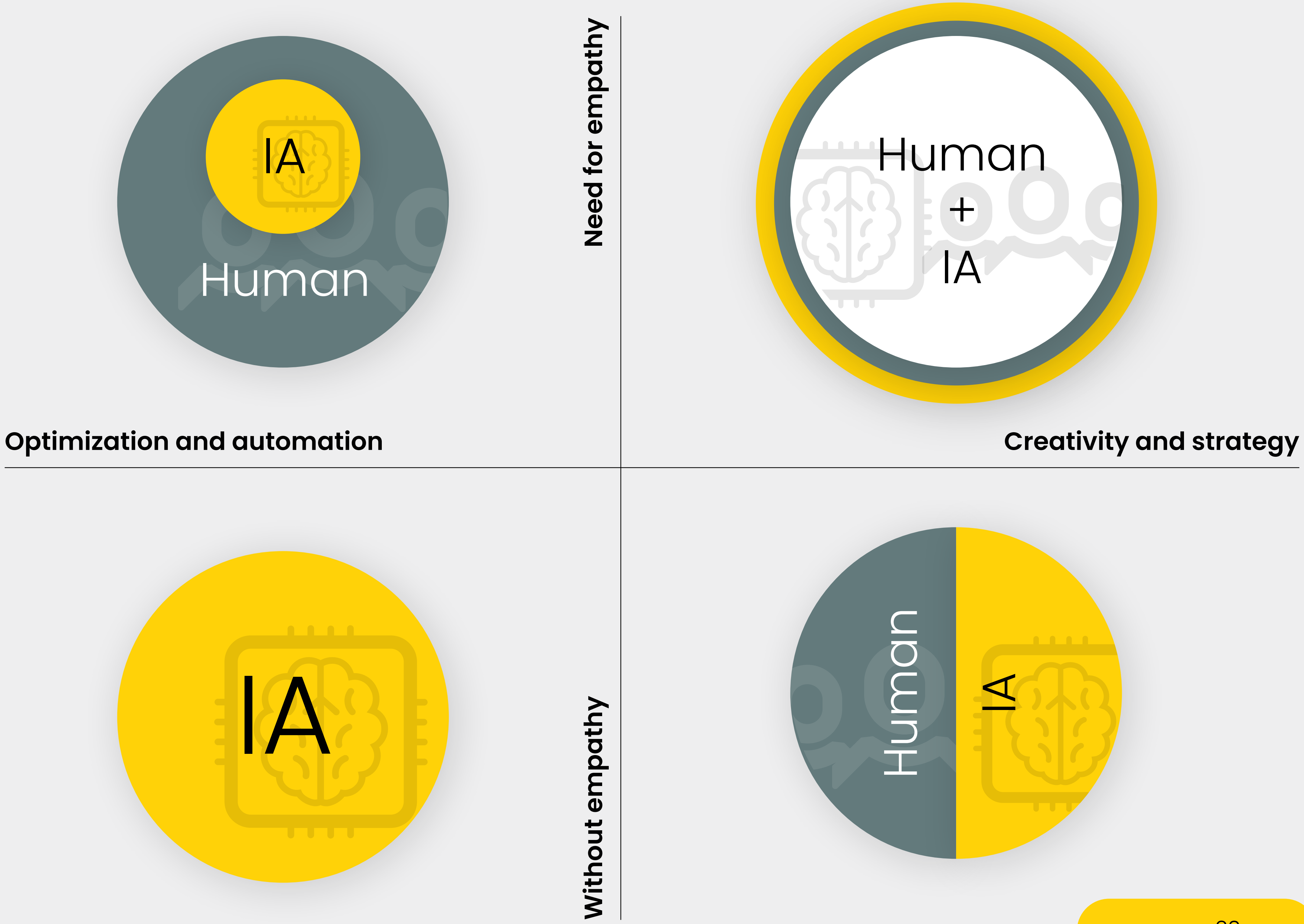
In addition, AI can promote the **creation of personalized work and/or academic development plans,** with high value and return in the business environment. In this regard, some studies have indicated that generative artificial intelligence can have **up to seven different types of roles** to enhance human capacities: from the tutor or the student to the motivator or the simulator, among others. In other words, GenAI **can provide alternative views, teach learning techniques, apply knowledge and scenarios or feedback on the results of a learning process,** ultimately enhancing the human and self-management skills identified.

The question, therefore, is whether companies are prepared for AI. Robotics and drones may incorporate intelligent sensors that detect an alteration in weather conditions before humans, but machines, at least for the time being, cannot replace the generation of hypotheses or empathetic and direct communication with the user. It is enough to imagine, as the writer and businessman **Kai-Fu Lee** indicates, in the doctor who diagnoses and communicates an ailment to the patient. Thus, **intelligent technological empowerment** should not be seen as a watertight and timely process in companies but should be **incorporated as a habit:** if technologies follow a cycle called **technological hype,** only organizations that keep constantly updated on the most disruptive innovations will be able to surf the wave -or tsunami- of hype, staying ahead and setting a differential value.

↘ HOME

Graphic 5

Symbiosis between AI and the worker according to need and degree of optimization and human attention



Source: Prosegur Research, 2024 based on BBVA

HOME

04

AI in an expanded **business ecosystem**

HOME

04 AI IN AN EXPANDED BUSINESS ECOSYSTEM

Artificial intelligence has changed the way the world works for decades. Its current popularization and convergence with other technologies is assuming a rapid growth for many organizations, configuring formulas and approaches especially useful in the field of security. From Prosegur Research we understand that **the main opportunities of technologies lie in their potential to empower experts;** that is, the ability to increase the skills of security professionals, greatly increasing effectiveness and efficiency as never before seen.

However, it must be understood that algorithms do not act in isolation but are assembled in a technological ecosystem together with drones and robots, RFID systems, NFC technology and LiDAR. As a result, **opportunities and risks become systemic,** so security and cybersecurity, as well as regulatory compliance, are basic pillars that give robustness to the design, implementation and use of all technologies, not just AI.

In this context, the hybrid security model integrates artificial intelligence as a tool that empowers security experts, allowing strategic use of data and highlighting the importance of integration and technological convergence. Of course, the approach to this model must also be comprehensive and holistic. It is vital to consider the **technological and business ecosystem** in which we work. The involvement of employees and stakeholders, as well as top-notch academic and research organizations and clients in the design, allows a genuine review and improvement of the AI application with the intention of adjusting innovation formulas. In short, embracing technologies as part of our usual working tools from a **systemic, humanistic and therefore empowering vision** allows us to accompany and even push the waves of change in the world.

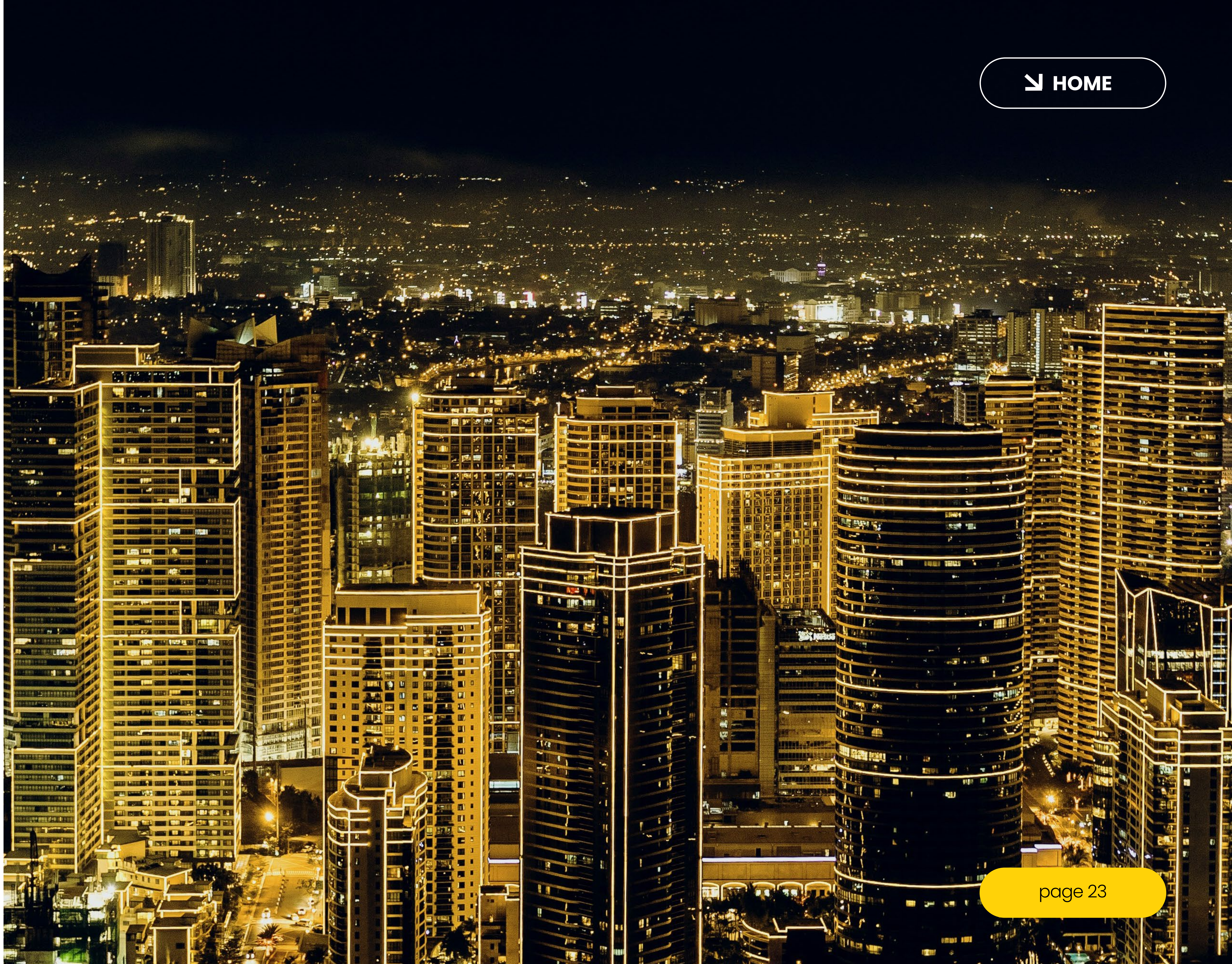
> The coming decade will be about human collaboration and AI. Our mission will be to automate routine and humanize the exceptional.
>
> ***Peter H. Diamandis***

The bias of AI is currently being **reflected** upon. However, the distortion of reality is something that belongs to all people in many areas. In Prosegur Research we are convinced that biases and distortion of reality surpass technology: it is so human that it has to be understood as a global challenge for all organizations, so transversal training initiatives, diversity and sustainability that address this challenge in a holistic way throughout the company, and not just for a technology or the field of innovation, are necessary if we truly want to embrace the changes of the world.

It can therefore be concluded that orienting the application of artificial intelligence as a formula of human empowerment, enhancing its capabilities, will be the transformative option of success; but it will require **courage** to overcome the short-term benefit of automation, **creativity** to identify the ideas never raised and the opportunities until now non-existent and **serenity** to take decisions from human and honest reflection.

If we redirect our efforts on artificial intelligence towards the empowerment of human skills, it will not only be a human-centered technology, but **a technology for getting to know each other better and preparing for change.** The future cannot be predicted, but one thing is clear: it will not be the same as the past. Companies that invest in empowering people will generate more prosperous societies and have competitive technology to influence the construction of their own new future.

From our hybrid security approach, we want to be part of the social and technological transformation, which together make up the best way to **make the world a safer place.**



HOME

Glossary

Following Gartner terminology,
the following are the main types of AI:

- **Generative AI**
  It refers to AI techniques through which a representation of artifacts is assimilated from data and with the aim of generating new and unique artifacts similar to the original ones, but without repeating them.

- **Responsible AI**
  It is a general term that encompasses the business and ethical decision-making aspects of AI adoption. It encompasses organizational responsibilities and practices that ensure the positive, responsible, and ethical development and functioning of AI.

- **General AI**
  (AGI) is intelligence (currently hypothetical) a machine that can perform any intellectual task that a human being can perform.

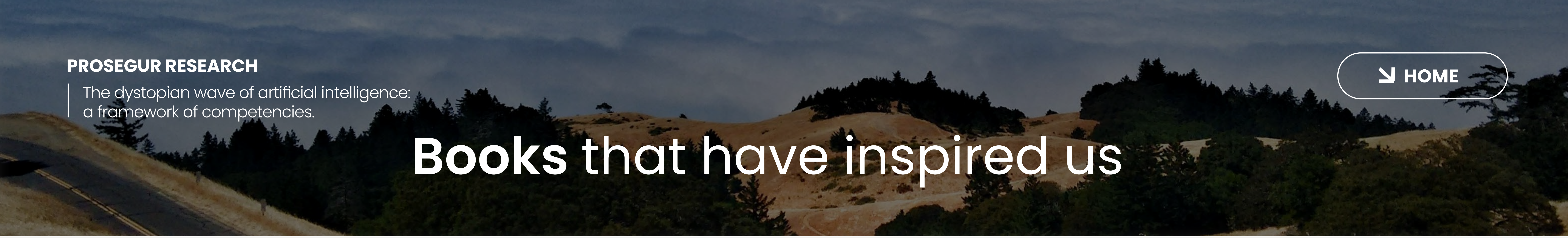
- **Composite AI**
  It refers to the combined application (or fusion) of different AI techniques to improve learning efficiency and expand the level of knowledge representations. It solves a wider range of business problems in a more effective way.

- **Data Center AI**
  Focuses on data enrichment to make data-driven decisions, improving quality, privacy, and scalability.

- **Engineering AI**
  It is critical for enterprise delivery of AI solutions at scale. Discipline creates coherent systems based on AI, delivery, and business development.

- **Simulation AI**
  Is the combined application of AI and simulation technologies to jointly develop AI agents and simulated environments in which they can be trained, tested, and sometimes deployed.

HOME



Books that have inspired us

AI and machine learning for Coders: a programmer´s guide to Artificial Intelligence
Laurence Moroney

AI tools and techniques for corporate facilitators and leaders
R.W. Rockwell

AI 2041: ten visions for our future
Chen Qiufan y Kai-Fu Lee

Artificial Intelligence. The new intelligence and the contours of the human.
Mariano Sigman and Santiago Bilinkis

Artificial Civilization
José María Lassalle

Competing in the age of AI: strategy and leadership when algorithms and networks run the world
Marco Iansiti and Karim R. Lakhani

The dream of artificial intelligence
Gisela Baños

The myth of the algorithm: tales and accounts of artificial intelligence
Richard Benjamins
and Idoia Salazar García

What do we do with human people?
César Antonio Molina

The age of AI
Henry Kissinger, Eric Schmidt
and Daniel Huttenlocher

The bussiness case for AI: a leader´s guide to AI strategies, best practices and real-world applications
Kavita Ganesan

PROSEGUR
SECURITY

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