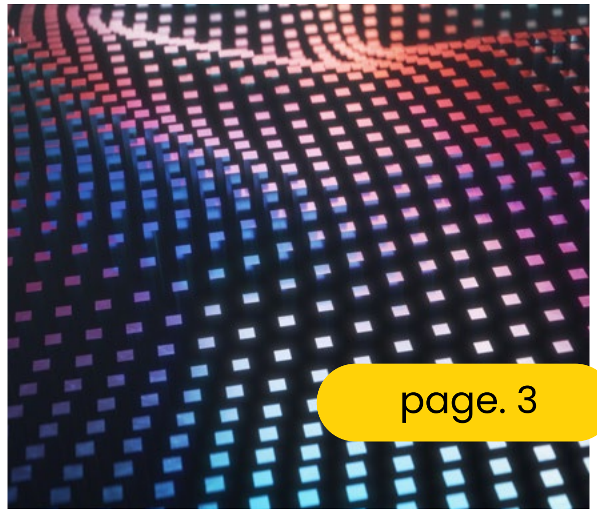
PROSEGUR RESEARCH

The strategic value of data

PROSEGUR

↓01

Data today



page. 3

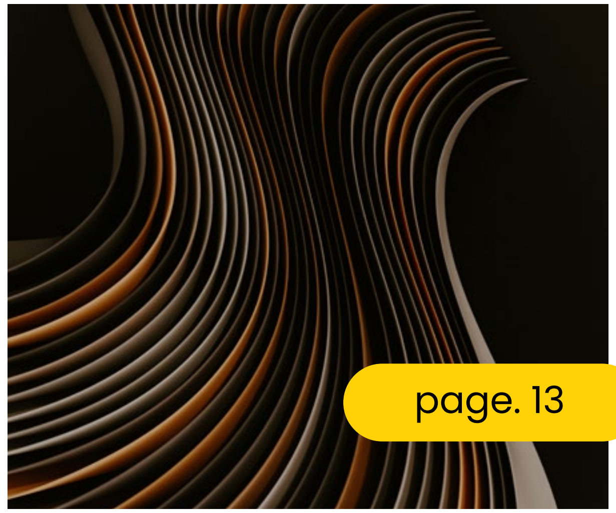
↓02

Data at risk

page. 8

↓03

The transformation of data in a changing environment



page. 13

↓04

Modeling innovation for security

page. 17

This is an **interactive** document

01

Data today

01 Data today

> “Without data you only have an opinion; with data you can have a well-founded opinion.”
>
> **W. Edwards Deming**

1.1 The exponential rise of the data era

Together with technology and people, data is interrelated through complex processes that enable efficient and agile strategic decision making, in response to disruptive changes.

Data is a way of representing reality, in other words, an objective fact, qualitative or quantitative, regarding an occurrence or an event.

We live in the data era: the volume of data has increased exponentially worldwide, with approximately 2.5 bytes created daily[1]. The management of the massive volume of data – big data – poses an important challenge for any company.

New technological developments, such as sophisticated programming of languages or programming adapted to data visualization, have gained prominence within the framework of big data. In addition, three explanatory and facilitating elements of this **exponential** nature stand out[2]:

On the one hand, **computation** has become cheaper, being accessible to a multitude of people and companies – although there are substantial inequalities regarding access to technology in different geographical locations–.

On the other hand, the **digitalization and ´technalization´** of society have resulted in hyper-connected citizens and increased coding of behaviours and connections of everyday objects to the internet.

Finally, **Social networks** transform the individual into a user and, in turn, into a data provider: in addition to offering opportunities for the population, they collect data on **audiences and consumer behaviours.**

---

[1] According to the source **The Next Tech.**
[2] Recommended reading in a **Harvard-Deusto** magazine.

The **value of data in the business environment** has increased significantly in recent years: as Benjamins and Salazar explain, “It all comes down to data”[3]; its mass collection has changed traditional business models on a global scale.

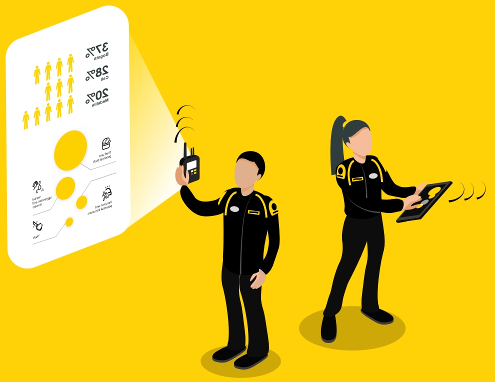
Consequently **three characteristics** characteristics have been identified as determining the value of large data sets: **volume, variety, and velocity.** These three factors are key in assessing the quality of the samples and its value, being greater in the presence of larger quantities of data needed to be processed and the transversality of its information; as well as the rate at which it can be obtained and processed. The convergence of these three characteristics determines the quality of the sample and, consequently, its value.

Data becomes valuable when it interacts with other data in an appropriate ecosystem, when it evolves, when it is susceptible to being correlated with certain topics of interest to the company or the managing institution. Therefore,

> It is not in the data itself, but in the presence of large quantities of it and within an exploitable environment where its value lies.

Likewise, the current implementation of methodologies in the field of data analysis has led to an increase in the **density of information** and the need to adapt to a **new mentality** when drawing conclusions.

The growth of **information density**

	Social networks	At home	Security
2010	 • 140 characters • Low resolution and compatibility	 • DVR, Blackberry (3G)	 • CRA with installed technology
2020	 • 280 characters and introduction of gifs, videos, images, hashtags, emojis, streamings, tweets, etc. • High resolution and compatibility. Inclusion of stickers, filters, music.	 • Smartphone (LTE or 5g), Netflix, Nintendo Switch, Apple Watch.	 • iSOC with operating technology

---

[3] Idoia, S. y Richard, B.: **The myth of the algorithm.**

In essence, when we talk about the value of data, we are referring to the quality of input in its environment[4], as well as leveraging its use to understand the world and act accordingly. Thus, it can be said that **the value of data is bidirectional:** on the one hand, companies have a fundamental asset for their business strategy and, on the other, users receive services that are more adapted and appropriate to their personal interests.

As subsequent elaboration will show, data is comprised of valuable information for companies – such as transactions, dates, quantities– which, when used in the appropriate way, can guide an action plan towards a specific business objective. This is what we call a **data-driven strategy.**

1.2 Working with data is a long-distance race

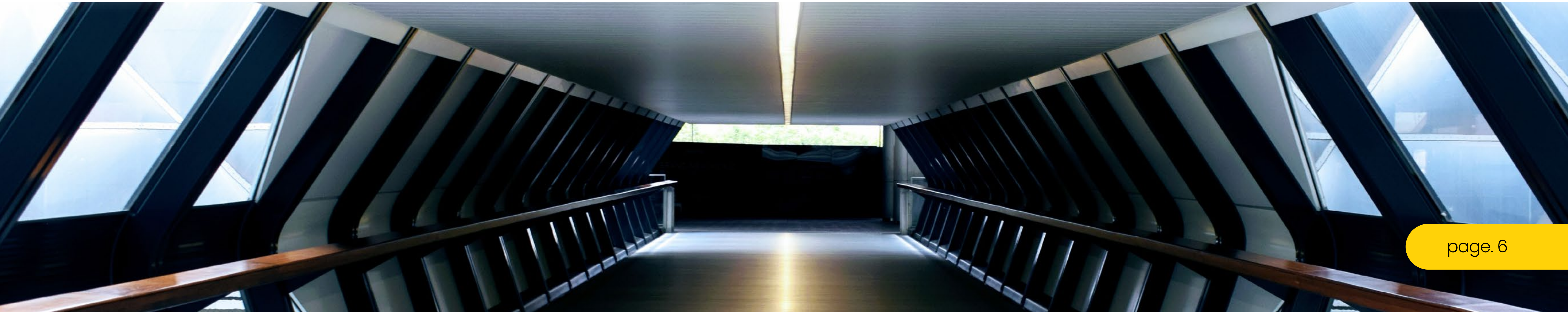
The use of **data analysis** for decision making that involves taking action is one of the most useful assets for companies today. The analysis of large volumes of data has become a decisive tool in planning and decision-making due to the **cost-effectiveness, speed and accuracy** it offers. Its applications in the business world have a **cross-cutting nature:** its use in areas ranging from marketing to sales, through finance or even recruitment, highlights its importance for the growth and operation of a company; which at the macro level ends up making it a **factor of economic growth.**

Each company processes user data according to its activity, establishing **customized strategic approaches.** In this way, the company's operations in the market, especially the tasks of attracting and processing customers, become more efficient. As an example, the processing of massive data can be reflected in the musical suggestions that a music application can make, in the dissemination of personalized ads that can be sent to users or in the adaptation of content for each individual on web pages or mobile applications, among others.

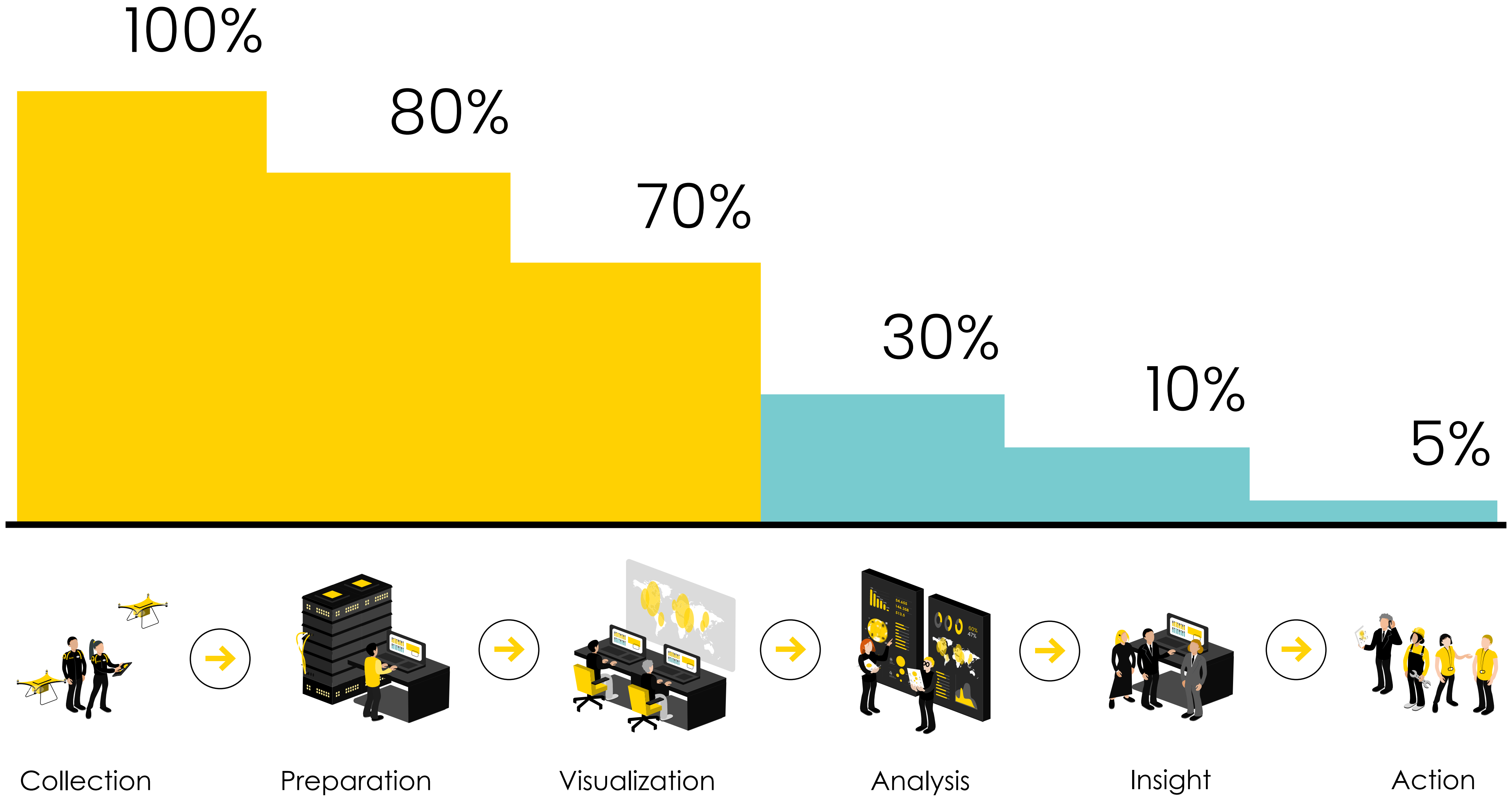
However, the main difficulty of data derives not only from its **enormous volume** and the **massive infrastructure** needed to process it, but also from adapting a **corporate culture of data management.** A **study** conducted in 2018 highlighted that corporations have invested millions of dollars in modernizing and digitizing their businesses. However, **up to 70% of the initiatives have failed** by prioritizing technology as a standalone element instead of integrating it into an ecosystem of strategic vision and data leverage.

---

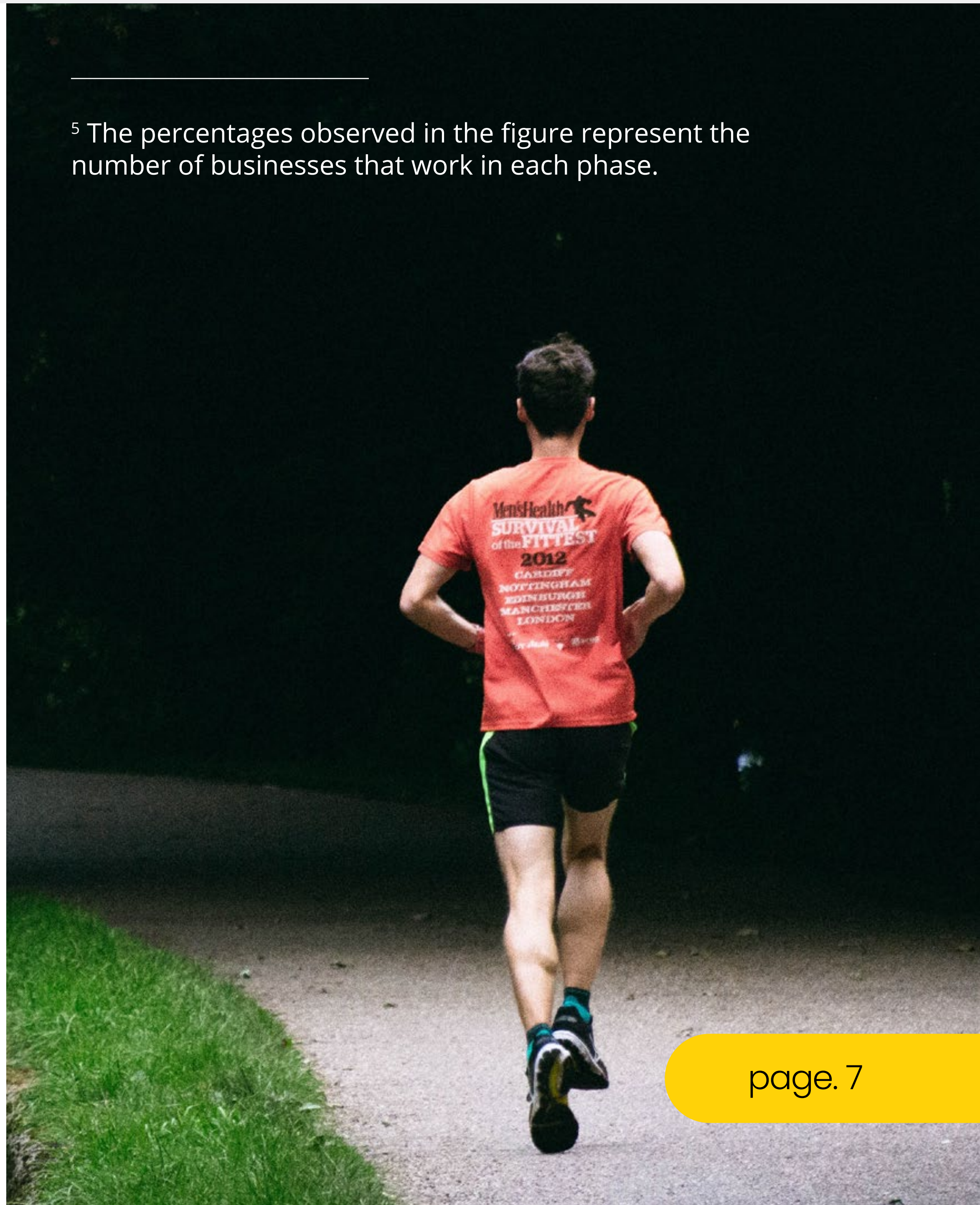
[4] In his book **Factfulness,** Hans Rosling encourages his readers to have a healthy diet with data.



In addition, **the process of working with data must be goal-oriented: a concrete action to improve a specific business area.** In this regard, we highlight the Forbes' model of the **analitycal marathon:** companies work in a process consisting of six stages or milestones, from collection to action[5]. Most companies obtain information and usually prepare it, but very few manage to reach the **"last mile"**, where changes are actually analysed, discussed and implemented. Some studies indicate that **94% of Spanish companies consider data as a fundamental** for their companies.



Source: Prosegur, 2023 based on Forbes



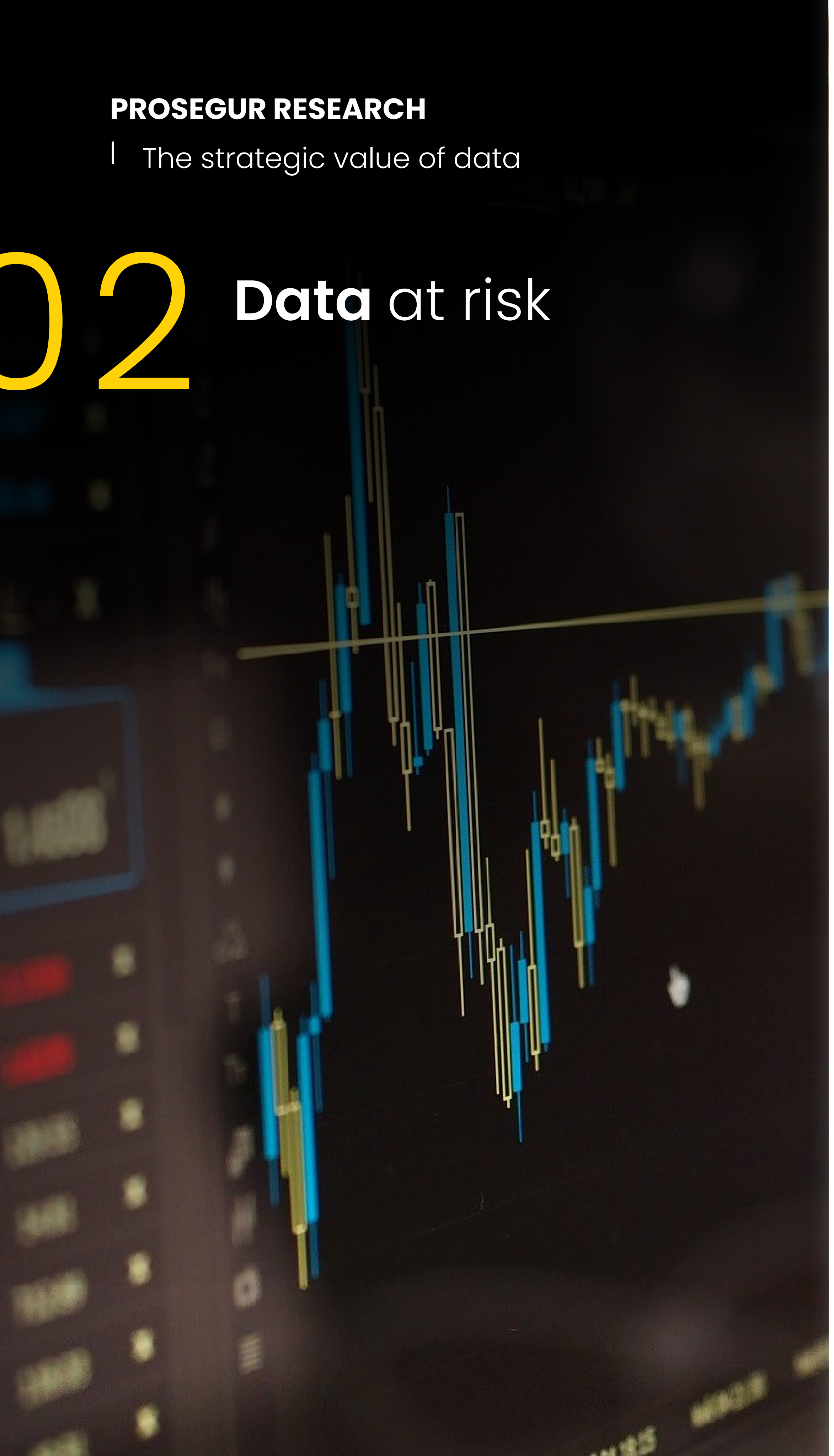
---

[5] The percentages observed in the figure represent the number of businesses that work in each phase.

02

Data at risk

02 **Data** at risk



2.1 Criminal exploitation of data

For this reason, guaranteeing data quality and integrity is one of the greatest challenges in this area. However, there are threats and risks that companies that handle data must detect, mitigate or avoid, but above all anticipate. In the words of Cristina Colom, "the rapid growth of datafication and the digitization of almost every aspect of modern society have intensified the risks".

It highlights the value that **data has acquired as another trading asset.** The **Dark Web Product Price Index 2022** points out that some of the most popular "products" to trade on the Dark Web are credit cards (ranging in price from $20 to approximately $100), passwords to log into platforms such as Netflix or Paypal, or email addresses.

For its part, **ENISA** (2022) – the European Union Cybersecurity Agency - recalls that the prominence of data as an enabler of economic decisions is a **major attraction for cybercriminals.** Threats against data can be aimed at gaining unauthorized access or disclosing information, as well as manipulating data to interfere with a systems behavior. These threats are also at the basis of many other existing threats, such as ransomware or RDoS, which aim to deny access to data and possibly charge a payment to restore this access. In addition, **data manipulation,** such as phishing in its novel implementation based on deepfakes, can sometimes lead to misinformation.

According to the same report, **the most attacked assets are the servers** that contain the data, the devices that transform them and the people who work with them. In this sense, it is thus essential to work with **hybrid security** that encompasses data, technologies and people. It is worth noting the main threats within each of the pillars:

2.2 Security trends which affect data

The following are the **three key security trends** affecting data-driven strategies:

1

Firstly, the exponentially accelerated growth of both data and technology is noteworthy. This has amplified the terrain in which attacks occur while simultaneously providing public and private organizations dedicated to security with important tools to make it possible to obtain intelligence with much more precise data.

2

Secondly, the convergence of technologies, which increases complexity, making it difficult to detect threats and risks, but at the same time makes the impossible possible, exponentially enhances the capacity of the actors operating in data ecosystems. As we have seen, it is up to analysts and decision-makers (in short, people) to make this convergence strategic.

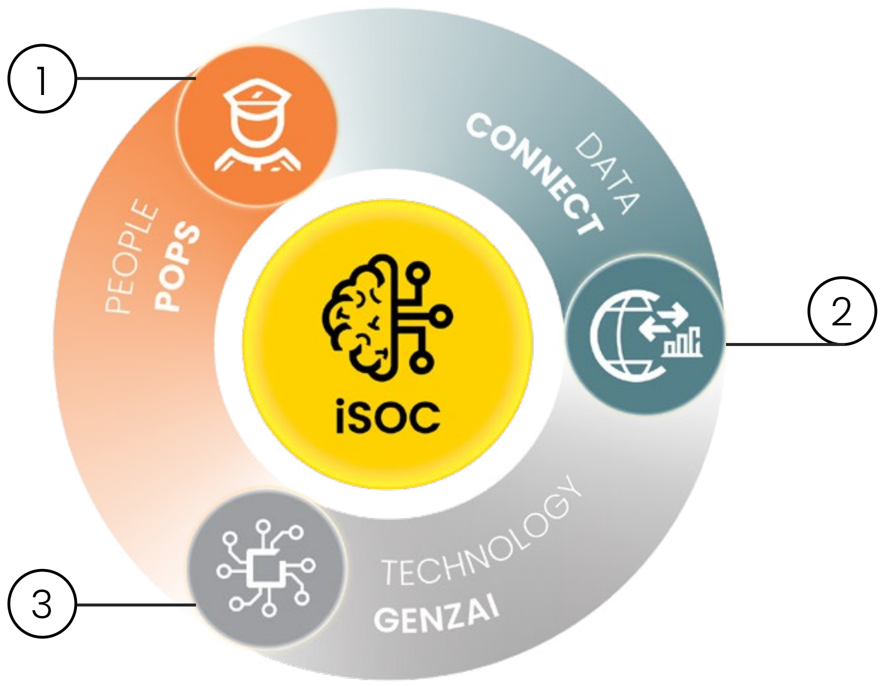
3

Thirdly and finally, there is the increased empowerment of actors, from individuals to non-state entities, including companies and criminal organizations; therefore, any data analysis must in turn assess their geostrategic scope, as well as key technological and sociological trends.

Source: Prosegur, 2023 based on ENISA

Data threats ①

Criminal behaviour targeting data falls under technology-based[6] crimes, which are related to the **confidentiality** (access is restricted to authorized users), **integrity** (data are correct, reliable, and valid) and **availability** (systems and data are accessible to those who request them) of computer systems and data. Unlawful acts include, but are not limited to, illegal access to a computer system or computer data; illegal interception of computer data or illegal acquisition of computer data; or illegal interference with data and systems.



Threats through technology ②

Technology-facilitated[7] crimes, take advantage of data as a means for their criminal purpose. Such is the case of computer-related **scams, frauds and forgeries** (bank fraud, phishing, advance fee fraud scam, romance scam and other fraud-related scams); **identity-related** computer crimes; or crimes related to **product counterfeiting,** brand abuse and corporate impersonation.

Data crack is an event that may cause the unintentional release of sensitive, confidential or protected data due to, for example, configuration errors, vulnerabilities or human error, but never includes intentional attacks.

Data leak is an intentional attack carried out by a cyber criminal with the aim of gaining unauthorised access to and releasing sensitive, confidential or protected data. In other words, it is a deliberate and forceful attack against a system or organisation with the intention of stealing data.

Threats from individuals ③

People, from outside or inside the company, can use business data in many different ways, since **82% of data threats involve human** action, as explained by ***ENISA*** (2022). In this context, **data leakage** is one of the oldest, yet increasingly important threats given the amplified amount of vulnerable data that all companies currently process, such as the data leakage phenomena.

In addition, individuals can exploit company **data unfairly** through industrial espionage, abusive exercise of the right to information and the discovery and disclosure of company secrets. On a more **intimidating note,** threats, coercion, and extortion are also other forms of data exploitation, both at the corporate and personal level, against customers, employees or managers.

---

[6] Which, according to **UNODC** (2022)) the objective is aimed at ICTs and would not be possible without the use of this technology.
[7] Following the UNODC framework (2022), they are the more traditional ones on which ICTs play a fundamental role in their commission.

Moreover, **social engineering** is one of the biggest threats to data and asset protection, whereby a user is tricked by different **manipulation techniques** into believing that they are a trusted person, institution, or company, with the aim of gaining access to confidential information. Accordingly, technology-based crimes have increased significantly in the last decade: some reports indicate that **cybercrime has increased by 600% since the COVID-19** pandemic, referring that the global economic cost could reach over **10 trillion dollars per year** by 2025.

Additionally, the **Data Breach Investigations Report** (DBIR) notes other types of human-related incidents, such as **"miscellaneous errors,"** whereby the security of an asset or system is accidentally compromised, or **asset loss.** It is a data breach whereby valuable information is lost without malicious motivation (although sometimes there may be malicious intentions).

Working on human skills is one of the core elements to be encouraged in order to prevent and reduce the impact of cybercrimes. In this regard, the World Economic Forum warns that, **beyond technical knowledge, human skills must be developed simultaneously,** integrating various disciplines such as sociology, psychology, management and communication.

By anticipating these threats and mitigating their risks, we will be able to take advantage of the full potential of data from a secure environment.

03

The transformation of data in a changing environment

03 The transformation of data in a changing environment

> “In an economy where the only certainty is uncertainty, the only source of assurance for competitive advantage is knowledge”
>
> **Ikujiro Nonaka, 1999**

This is how the theorist Nonaka defined the turbulent international economic context back in 1999, pointing out that knowledge is the only tool that can provide a company with unique value compared to its competitors.

In the midst of an uncertain international landscape, the presence of new hybrid threats have a cascading affect on all tiers of societies and furthermore, consequential effects on global problems. Therefore, orienting actions towards an objective in an environment with these characteristics requires a strategic vision, in which the **efficient management of data, information and knowledge** is adopted in order to, on the one hand, detect trends in advance and, on the other, know how to adapt to them. This consequently allows for the creation of innovative solutions and processes, from a dual human and technological perspective.

However, intangible aspects such as experience, the know-how, cultural influences or ethical considerations are some of the elements that technology, at least for the moment, is not fully capable of integrating. The TAY **chatbot** chatbot for Twitter developed by Microsoft that was revoked just 24 hours after its launch due to the use of offensive language; or the AI-based **tool** created by Amazon to streamline its recruitment process that discarded women's resumes are two examples among the many cases that can be highlighted.

The **DIKW model** (an acronym for data, information, knowledge and wisdom), which dates back to the second half of the 20th century by authors such as **Ackoff** – in addition to other similar contributions applied to the business world such as those of Davenport and Prusak[8]–, which is also known as the **hierarchy of knowledge,** attempts to organize the structural and/or functional relationships between data, information, knowledge and wisdom (or what we adapt and call intelligence).

> The objective is clear: on account that they are not interchangeable concepts, the success (or failure) of corporate actions can be due to the correct or incorrect use or visualization of data.

---

[8] Davenport y Prusak: **Working Knowledge: how organizations manage what they know.**

In accordance with the two aforementioned authors, and as referred to in the first section, data is a fact about an occurrence or an event. Thus, **data has no meaning by itself,** nor does it provide an explanation as to why something happens.

Therefore, the 70,481 residential burglaries that were recorded in Spain during 2020[9], a fainting episode during an artist's concert; or a social mobilization in the center of a city, are some examples of data that, being objective and verifiable, do not allow us to explain why any of these events occurred.

Usually in business environments a large volume of data is handled and, sometimes, we tend to think that the more data we have, the more strategic or relevant we are as actors in a given sector or scenario. However, this can lead to an **infoxication** effect that can ultimately cloud our course of action and divert us from the objective to be achieved.

3.1

From Data to information:

the importance of context

Information is usually defined as a message or, in other words, a piece of data (or set of data) put into context. It therefore **reduces uncertainty and significantly increases its relevance and organization.**

It can be seen that, in general terms, it is a matter of "shaping" the data, answering questions such as "who" or "(with respect to) when", among others.

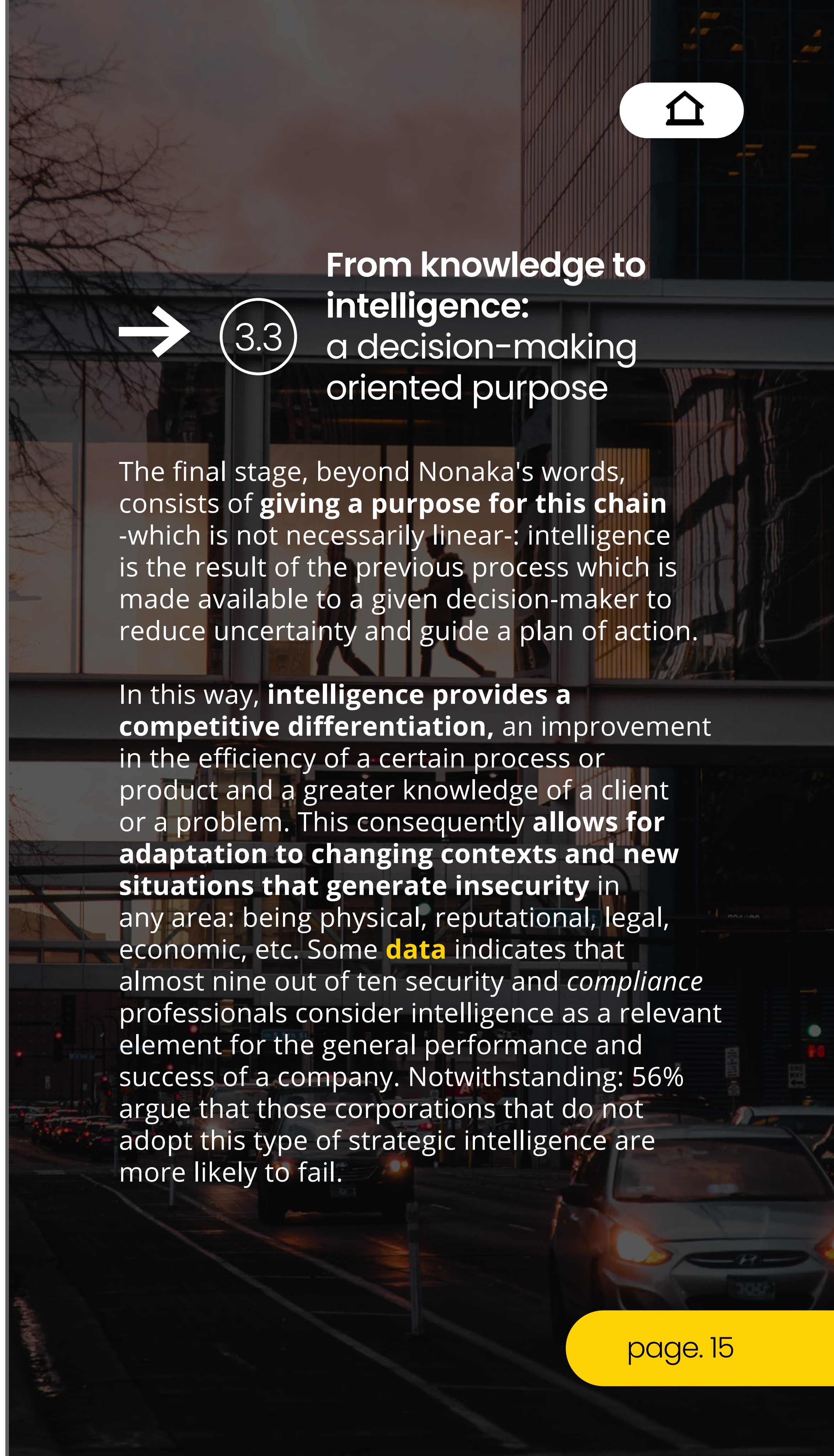
Sometimes we tend to overestimate the technological resources that empower our abilities and believe that technology alone can make up for some of our shortcomings. However, it is of little use to have, for example, the latest data analysis software if we do not program what we want to achieve with this tool from an idea developed by a person.

3.2

From information to knowledge:

the meaning as a means

The following step needed is to provide meaning, to try to explain why things happen, and consequently incorporating a fundamental aspect: **the understanding and integration of experiences.**



3.3

From knowledge to intelligence:

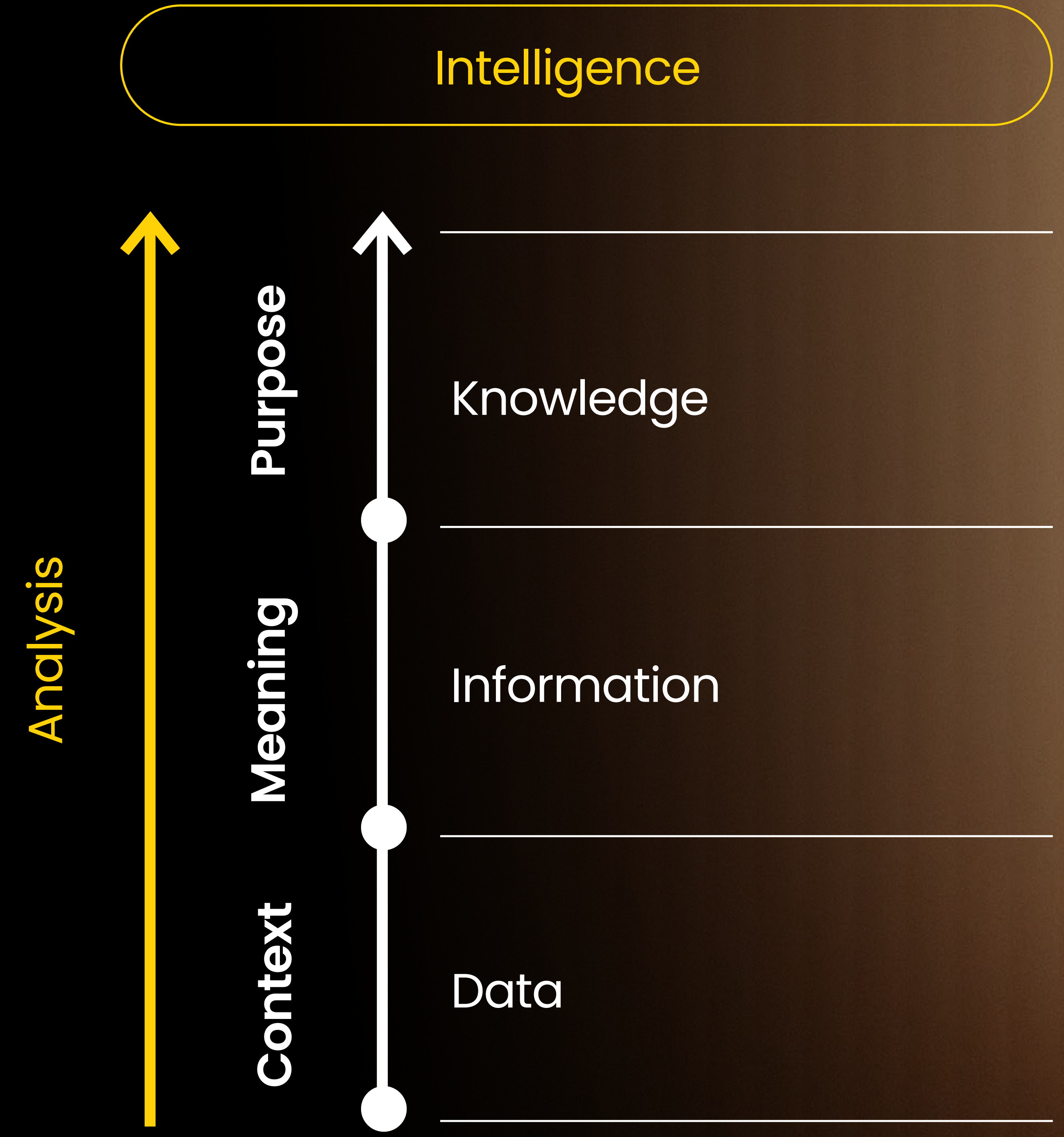
a decision-making oriented purpose

The final stage, beyond Nonaka's words, consists of **giving a purpose for this chain** -which is not necessarily linear-: intelligence is the result of the previous process which is made available to a given decision-maker to reduce uncertainty and guide a plan of action.

In this way, **intelligence provides a competitive differentiation,** an improvement in the efficiency of a certain process or product and a greater knowledge of a client or a problem. This consequently **allows for adaptation to changing contexts and new situations that generate insecurity** in any area: being physical, reputational, legal, economic, etc. Some **data** indicates that almost nine out of ten security and *compliance* professionals consider intelligence as a relevant element for the general performance and success of a company. Notwithstanding: 56% argue that those corporations that do not adopt this type of strategic intelligence are more likely to fail.

---

[9] Data provided by the Ministry of the Interior.



Intelligence

Analysis

Purpose

Meaning

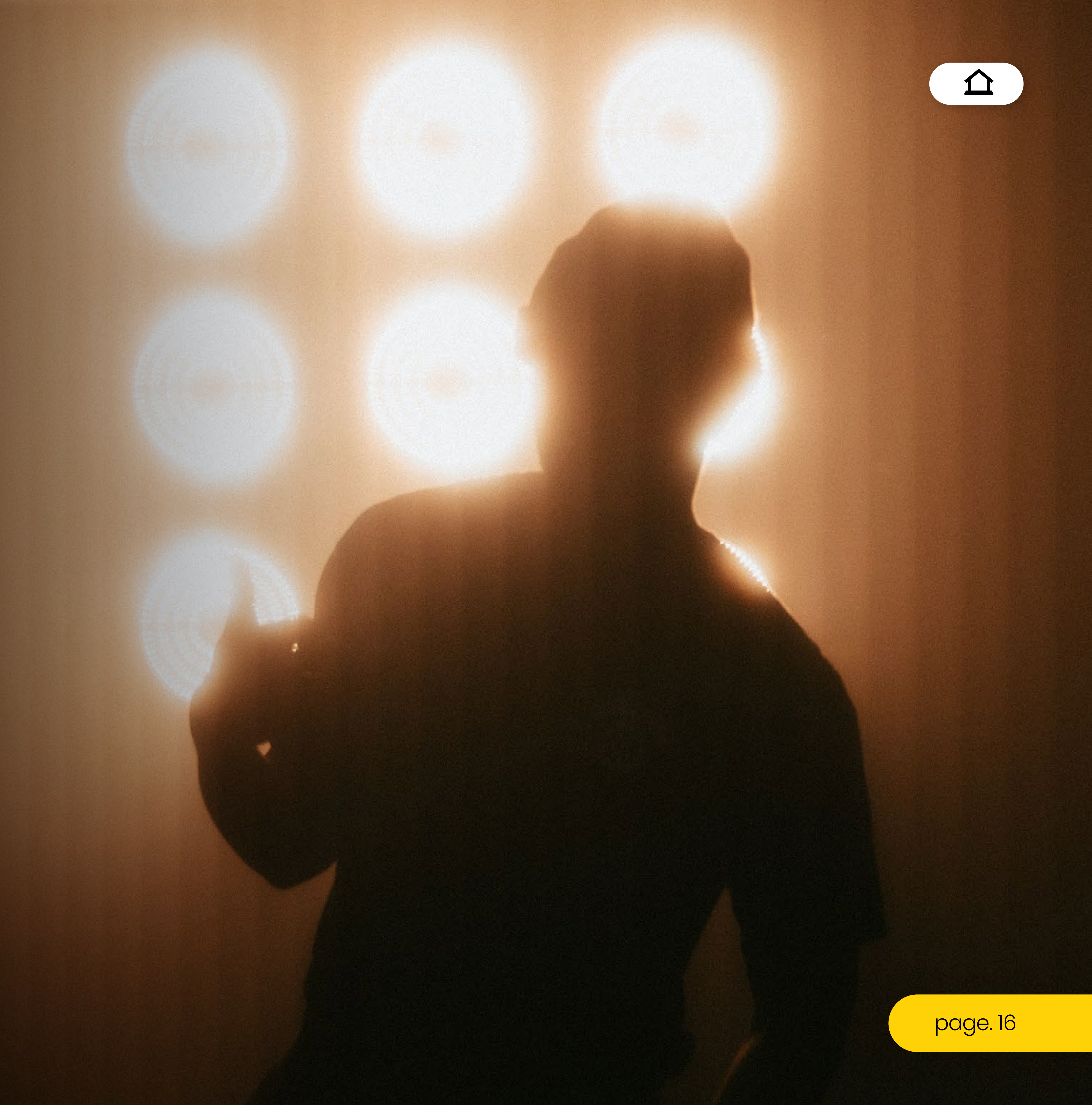
Context

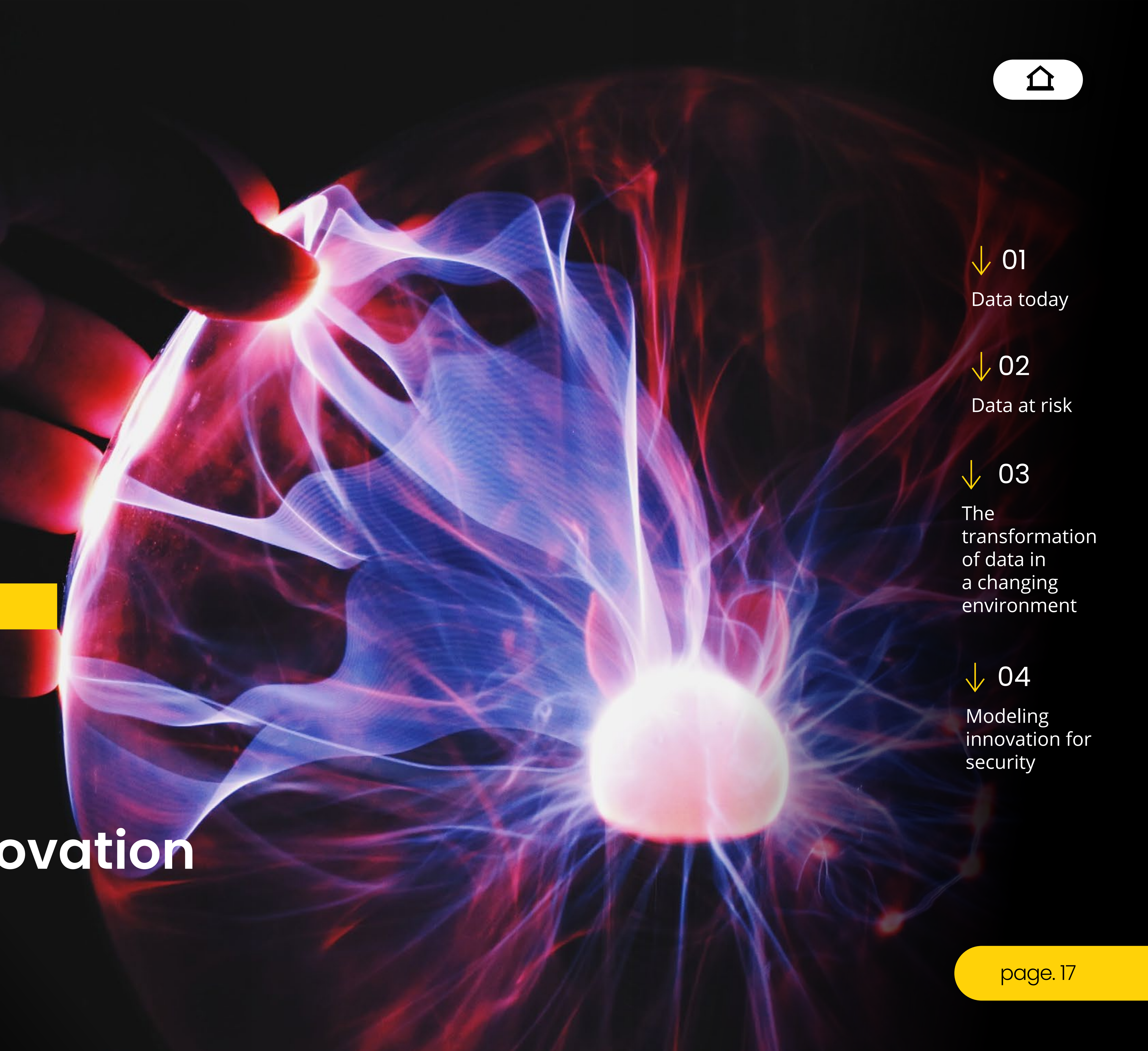
Knowledge

Information

Data

Source: Prosegur, 2023 based on AGT





04

Modeling innovation for security

04 Modeling innovation for security

> “It's not a technological revolution, it's a cognitive revolution”
>
> **José Manuel Leceta**

By analysing past data-driven trends from experience, critical and creative thinking and the most innovative technologies, it is possible to **anticipate actions, strategies and visions** that enable a genuine transformation of the organization. These different formulas for change in different timeframes are absolutely essential for any company that operates in the disruptive environment and needs to navigate the uncertainty of what the future holds. We propose three focuses of analysis for intelligent action with data:

→ 4.1 Overcoming biases

No person is exempt from committing biases in both data analysis and decision making[10].

Cognitive biases are mental shortcuts that people take to reach a certain conclusion faster, which can sometimes lead to analytical failures that impede or hinder the action plan due to inaccurate judgment or biased interpretation of a situation or time constraints, among other reasons.

One of the main reasons why we take these mental shortcuts is the well-known infoxication that was previously mentioned, which refers to an overload of stimuli and information that makes it unfeasible to properly manage large volumes of data. In this sense, some institutions such as the World Economic Forum warn of the so-called **“infodemic”.**

Of all the cognitive biases, we must pay special attention to those that impact or affect the evaluation we make of different evidence and for the estimation of probabilities.

This can be seen in business environments, where **anecdotal situations can be overestimated** and attributed a high statistical value, believing that the exception is more common than the rule. In addition, we sometimes tend to **fixate on an idea** and evaluate a situation based on information we already know or have just received, which is called **anchoring bias or the anchoring effect.** A further step is to try to confirm our own hypotheses through **confirmation bias** by looking for supporting information, which can affect objectivity in the phase of data analysis.

Moreover, people tend to **estimate the probability** of an event according to the **previous experiences** we have with it, which is known as **availability bias.** Similarly, through the **representativeness bias** we tend to think that two similar events are more likely to occur than those that are different.

---

[10] We recommend reading chapter 4 of the book **Upgrade** by Quintana and Alayón.

This can have an overflowing effect on the subsequent phases, once a given situation has been analysed. Some authors such as León (2001)[11] argue that there are also some **errors that hinder decision making,** among which are the constant **change of priorities and the lack of defining objectives,** the **lack of foresight** and imagination of alternatives, **the attempt to solve symptoms instead of causes or the overvaluation of intuition,** to name a few.

Likewise, León points out some cognitive **characteristics** that affect this decision-making process, such as **perfectionism** -which generates blockages when a perfect solution is not found-, the **need for security** -a strong reluctance towards doubt- or the **need for control** -fear of potentially unpleasant events-.

However, it is pointless taking these biases into account when analysing data and making decisions if we do not assume that **we all tend to have them in our daily lives, usually unconsciously.** Therefore, we must not forget the blind **spot bias:** the tendency to believe that we are less biased than others and that our biases affect us less than others.

4.2 Gaining insight

This is the final data-driven process: action-oriented insights. For this reason, insight is the conclusion of the analytical process, a fundamental step for any business area. Similar to the analytical marathon, Deskera points out that the **business insight** process requires four basic

01

Context

The first step is to proactively identify objectives and needs and to set deadlines and milestones to be achieved

02

Necessity

Establishing a business need helps to guide and prioritize the action plan that needs to be followed in the analytical process.

03

Vision

A holistic view of the issues and data is required, thus making management a key element in this process.

04

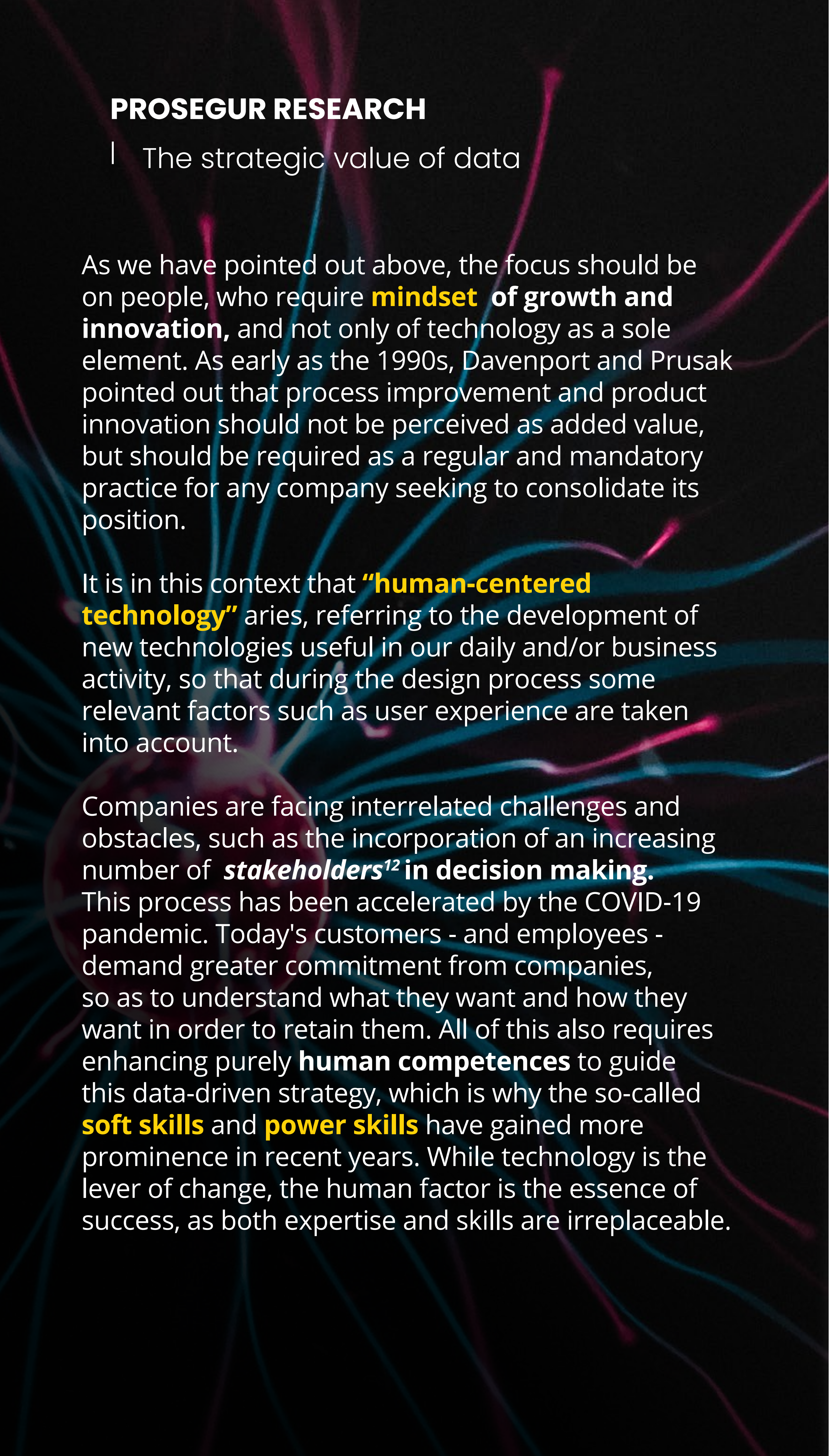
Results

Insights, as previously mentioned, help us to achieve a specific objective, therefore, it is important that this knowledge is stored and managed periodically for advancing business purposes.

Source: Prosegur, 2023 based on Deskera.

---

[11] Orfelio, L.: ***Making difficult decisions.***



As we have pointed out above, the focus should be on people, who require **mindset of growth and innovation,** and not only of technology as a sole element. As early as the 1990s, Davenport and Prusak pointed out that process improvement and product innovation should not be perceived as added value, but should be required as a regular and mandatory practice for any company seeking to consolidate its position.

It is in this context that **"human-centered technology"** aries, referring to the development of new technologies useful in our daily and/or business activity, so that during the design process some relevant factors such as user experience are taken into account.

Companies are facing interrelated challenges and obstacles, such as the incorporation of an increasing number of ***stakeholders***[12] **in decision making.** This process has been accelerated by the COVID-19 pandemic. Today's customers - and employees - demand greater commitment from companies, so as to understand what they want and how they want in order to retain them. All of this also requires enhancing purely **human competences** to guide this data-driven strategy, which is why the so-called **soft skills** and **power skills** have gained more prominence in recent years. While technology is the lever of change, the human factor is the essence of success, as both expertise and skills are irreplaceable.

4.3 And generating strategic convergences

The convergence of disruptive technologies generates **new risks and threats,** but also business **opportunities and potential improvements** in products and services. Therefore, technology is seen as a means to an end. The result of the analytical marathon and the DIKW model allows us to establish **global and peripheral visions,** which bring indisputable value to any company.

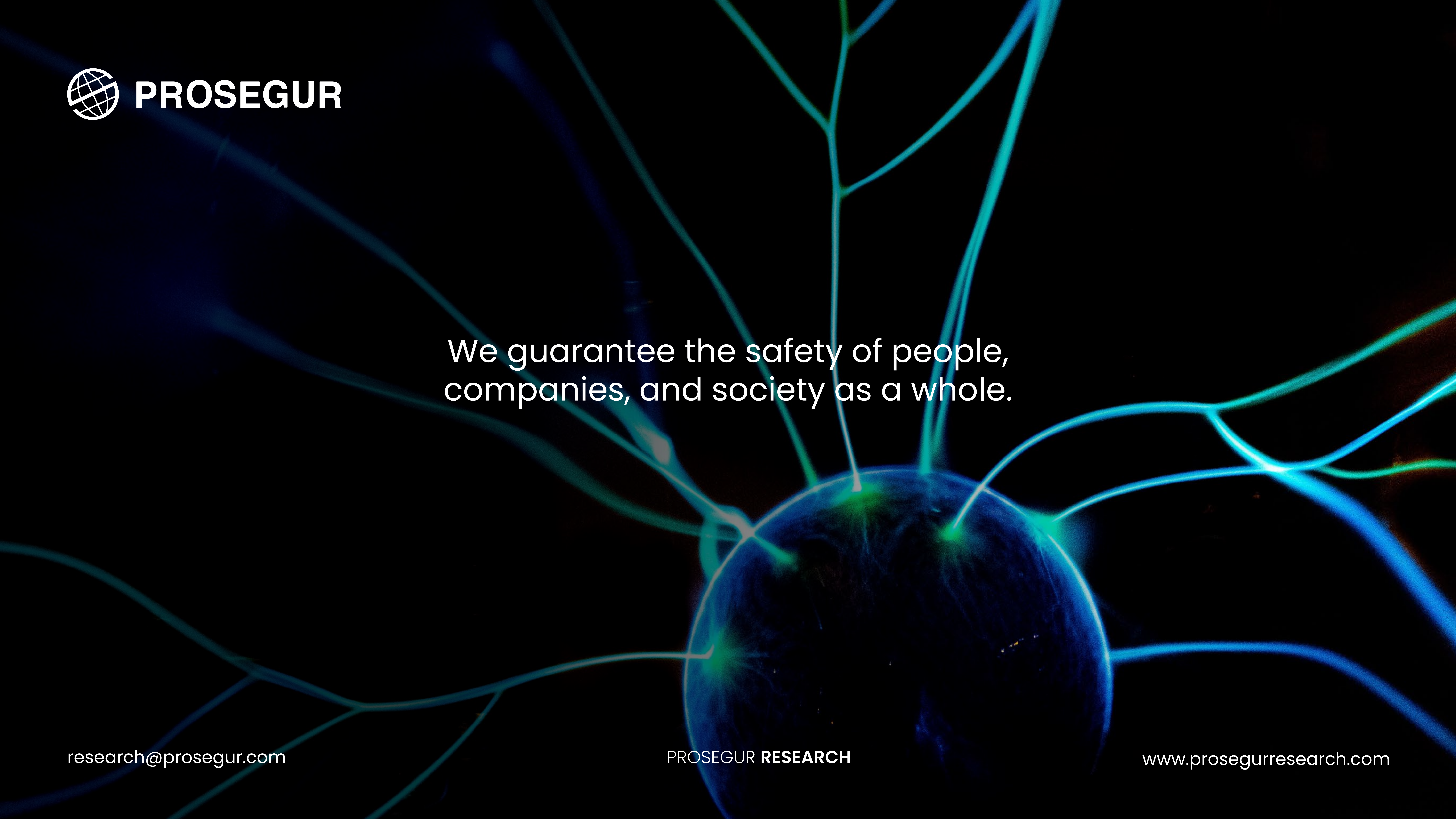
We talk about **disruptive technologies** because they barge in abruptly due to their exponential growth, while converging as they complement and enhance each other, further accelerating technological development. In fact, according to the consulting firm **Gartner,** by 2024 up to 40% of personal and individual activities and data will be digitally tracked.

All this is reflected in the prominence that the **Internet of Behaviour** (IoB) is gaining. By combining technologies, data analysis and behavioral psychology, we are trying to identify behavioral patterns in order to personalize services and products to a specific customer or user; once again, we see how technology, data and people are the three pillars for comprehensive hybrid security.

This transformation and hybridization of the world is not foreign to Prosegur, which through our ***hybrid security*** model, based on people empowered by intelligent technologies and the optimal use of data, we try to generate sophisticated operational strategies by integrating all the information through our iSOC. In short, we try to cover security needs by adapting to the requirements of the companies and people affected, customizing solutions following our "security-as-a-service" philosophy and providing added value in decision making.

---

[12] The term refers to the stakeholders that directly or indirectly impact business activity, ranging from shareholders to employees and customers or, ultimately, the public.



PROSEGUR

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

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com