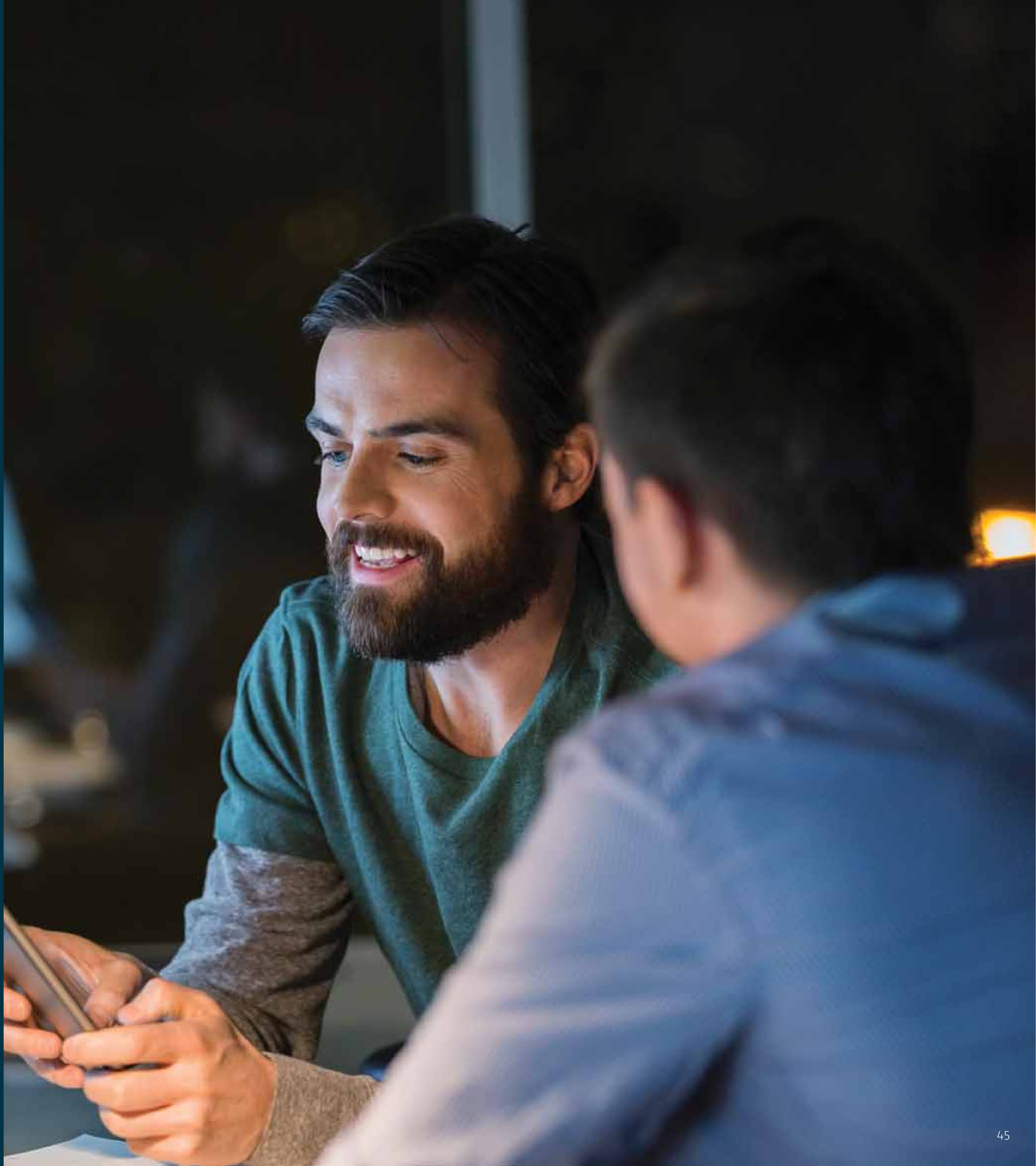
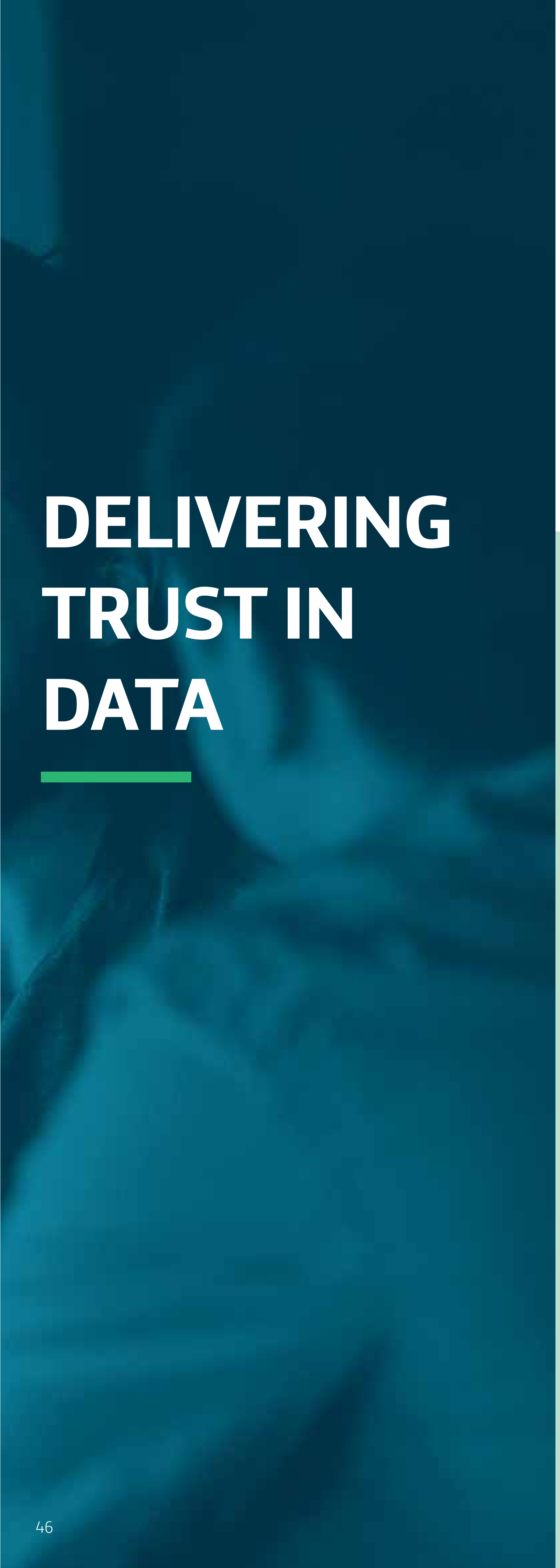
03 DELIVERING TRUST IN DATA

This chapter:

This chapter is about data, its huge importance and the innumerable ways in which it is empowering people in their daily lives. Here, we set out our vision for building trust: transparency, security and choice and putting people in control.





DELIVERING TRUST IN DATA

The Issue

- Data is an important part of our lives. It can enrich people's experiences and opportunities, benefit businesses and advance society as a whole.
- There is currently a lack of trust. People often do not feel in control of their personal data due to a lack of transparency and empowerment.
- Security threats are growing in importance in a digitalised and connected world, endangering people and businesses.

Our Belief

- Data is a force for good and we need to build trust by helping people to feel comfortable regarding the use of their data.
- We need new data ethics. People should be empowered to decide how and when their data is used and also be able to enjoy the value of their data.
- Transparency and choice are necessary to put people in control and build trust.
- Open Data can help to solve many social and economic challenges.
- Data security and confidentiality must be assured more than ever when everyone and everything is connected. New digital experiences should be designed around keeping people's data safe and secure.
- New forms of public and private cooperation are needed, as well as additional efforts to improve the security of products and services.
- Nation States have the responsibility to guarantee the security of their citizens but also need to respect their fundamental rights.
- Cybersecurity needs to be enhanced across the entire value chain of digital products and services, as the weakest link defines the security of the whole system.

The main challenge for a sustainable digitalisation process and Data Economy will be to mitigate the risks of data usage whilst grasping its opportunities.

Communications networks are the foundation of the Internet and the digital economy, as they transport amounts of data that are growing exponentially. In an increasingly digitalised and connected world, everything we do leaves behind a data footprint: every journey, shared moment, payment sent, celebration, news, reaction, travel and fun. And behind every data point, there could be a personal story.

And it's not only about personal data: millions of sensors generate huge amounts of data about weather, climate, pollution, traffic flows, consumption of energy and other resources. With the advent of the Internet of Things (IoT), the number of objects including sensors will grow very fast, opening up new and untapped ways of improving our world through more insights based on data. IoT, automation and Artificial Intelligence (AI) are creating additional opportunities for the reconfiguration of current industrial processes and supply chains based on data.

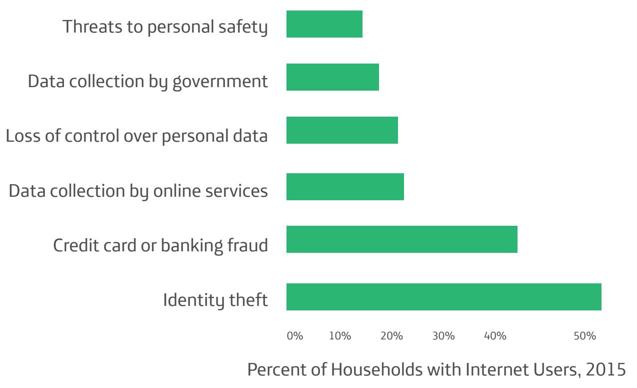
Data is at the heart of digital growth and, therefore, privacy and security are the pillars of a healthy and sustainable digital future. Digitalisation needs to be accompanied by new and responsible data ethics.

1. The lack of trust

Data-driven services and solutions exist in a social, economic and institutional context but, for many people, they are triggering a lack of trust, increasing uncertainty and a feeling of vulnerability.

Many individuals are increasingly concerned by the loss of control over their digital lives. People are no longer sure of how their personal data is collected, stored and used, by whom and for what purpose.

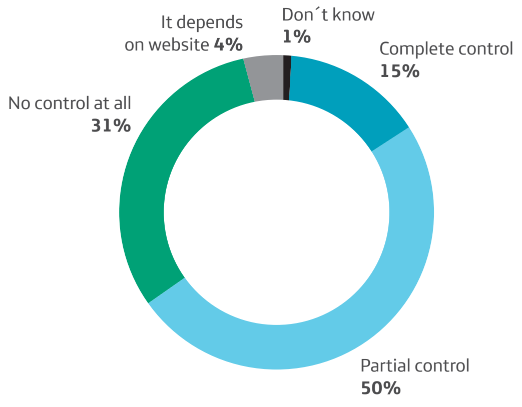
Chart 1. USA - Major concerns related to privacy and security risks[17]



Source: NTIA Digital Nation Data Explorer, 2016

Chart 2: EU - Perception of control over data shared online

How much control do you feel you have over the information you share online?



Source: Eurobarometer 2015

The less comfortable people feel about how their data is being used, the less willing they will be to share it. For a society with a growing dependence on digital technologies, this is a considerable issue and can even become a barrier to digitalisation.

Building trust in relation to personal data could be improved by tackling the following:

- **Transparency:** people should be allowed to access all the information they generate.
- **Putting people in control:** people should have access to tools that enable them to reap the full benefit of their personal data in simple and convenient ways.
- **Choice:** people should have meaningful choices about how and for what purpose their data is used.
- **Data security:** in order to guarantee privacy, people's data need to be kept safe and secure.

2. Data as a force for good

Data underpins new experiences, new services, and is transforming entire industries. Without access to data, progress would stop. More than ever before, we have access to information and metrics that can make the world more efficient, resourceful and informed.

Open Data represents an important opportunity to solve many of the current social and economic challenges we face, such as the reduction of energy consumption and pollution, the optimisation of traffic and the improvement of healthcare.

Administrations, companies and citizens should all work closely together to build an ecosystem that can capitalise on Open Data.

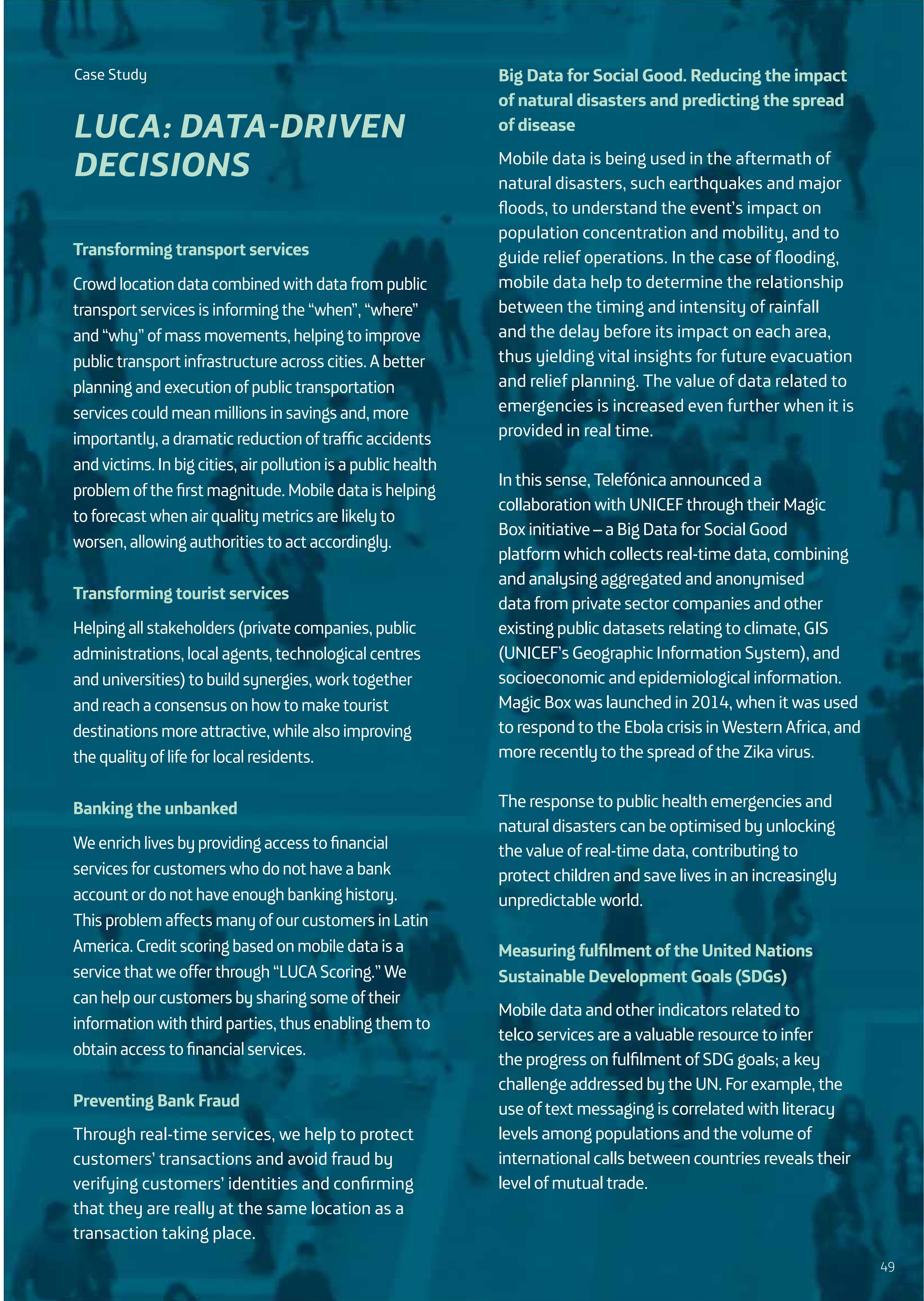
We consider that public data should be:

- Available for everyone without restrictions.
- Available and accessible online, ready to use.
- Shaped for its reuse and redistribution, even for transformation.

Data enriches people's lives, but can also help organisations to make better decisions and improve the quality of everyone's life:

- Transport can become smarter, reducing congestion, improving air quality and also minimising traffic accidents and victims.
- City infrastructure can be developed with better insight into people's needs, making all civil services more efficient and saving money that could be allocated to other needs.
- Epidemics and natural disasters can be better managed, saving human lives.
- Migration due to climate change can be monitored in order to measure its impact and plan actions accordingly.
- Diseases can be diagnosed earlier, making better healthcare possible, increasing quality of life for patients and their families.

Data can enrich people's lives, benefit businesses and advance society as a whole. Indeed, data analytics will be crucial for the transformation and progress of societies and in creating a better future.



Case Study

LUCA: DATA-DRIVEN DECISIONS

Transforming transport services

Crowd location data combined with data from public transport services is informing the "when", "where" and "why" of mass movements, helping to improve public transport infrastructure across cities. A better planning and execution of public transportation services could mean millions in savings and, more importantly, a dramatic reduction of traffic accidents and victims. In big cities, air pollution is a public health problem of the first magnitude. Mobile data is helping to forecast when air quality metrics are likely to worsen, allowing authorities to act accordingly.

Transforming tourist services

Helping all stakeholders (private companies, public administrations, local agents, technological centres and universities) to build synergies, work together and reach a consensus on how to make tourist destinations more attractive, while also improving the quality of life for local residents.

Banking the unbanked

We enrich lives by providing access to financial services for customers who do not have a bank account or do not have enough banking history. This problem affects many of our customers in Latin America. Credit scoring based on mobile data is a service that we offer through "LUCA Scoring." We can help our customers by sharing some of their information with third parties, thus enabling them to obtain access to financial services.

Preventing Bank Fraud

Through real-time services, we help to protect customers' transactions and avoid fraud by verifying customers' identities and confirming that they are really at the same location as a transaction taking place.

Big Data for Social Good. Reducing the impact of natural disasters and predicting the spread of disease

Mobile data is being used in the aftermath of natural disasters, such earthquakes and major floods, to understand the event's impact on population concentration and mobility, and to guide relief operations. In the case of flooding, mobile data help to determine the relationship between the timing and intensity of rainfall and the delay before its impact on each area, thus yielding vital insights for future evacuation and relief planning. The value of data related to emergencies is increased even further when it is provided in real time.

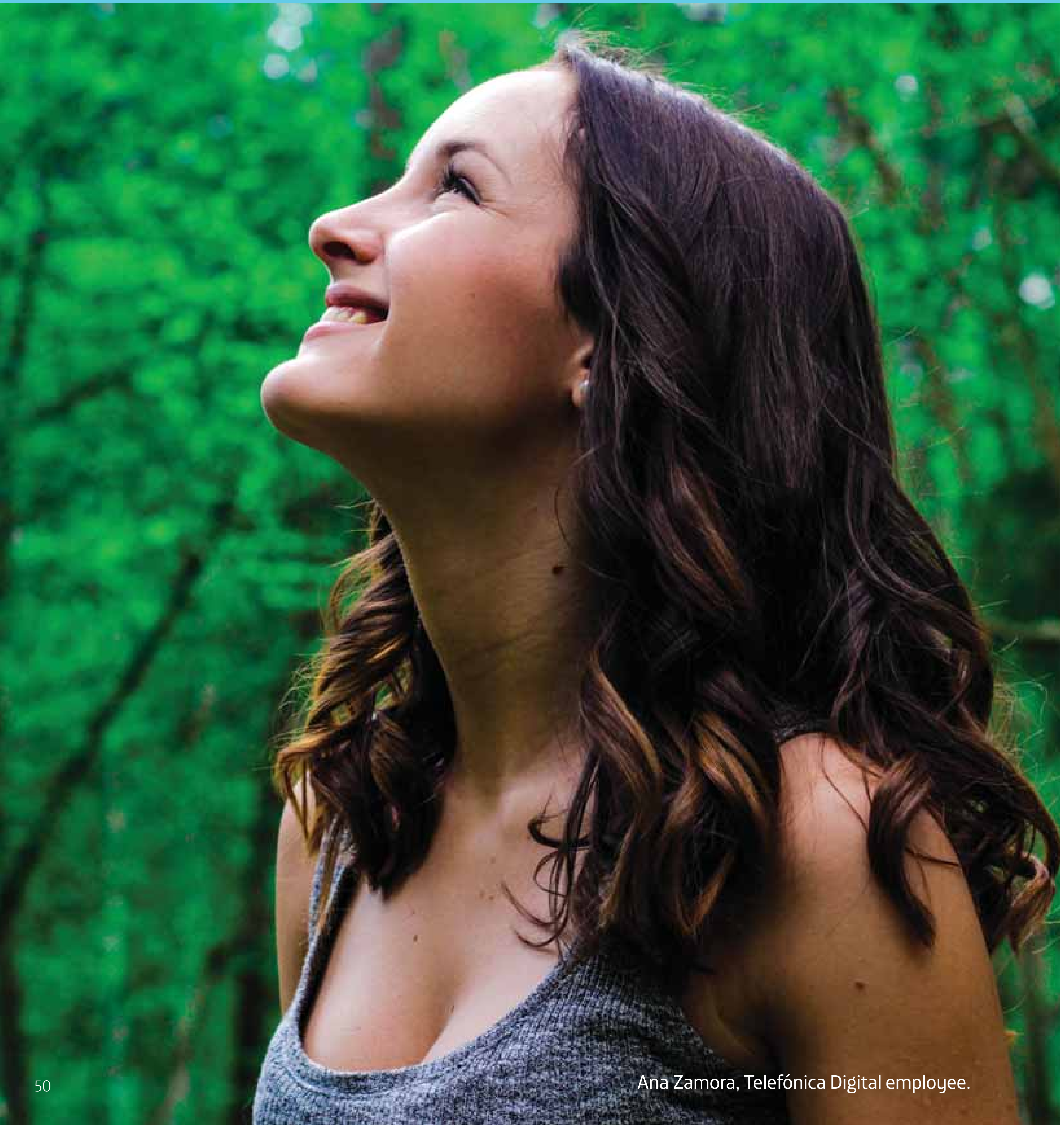
In this sense, Telefónica announced a collaboration with UNICEF through their Magic Box initiative – a Big Data for Social Good platform which collects real-time data, combining and analysing aggregated and anonymised data from private sector companies and other existing public datasets relating to climate, GIS (UNICEF's Geographic Information System), and socioeconomic and epidemiological information. Magic Box was launched in 2014, when it was used to respond to the Ebola crisis in Western Africa, and more recently to the spread of the Zika virus.

The response to public health emergencies and natural disasters can be optimised by unlocking the value of real-time data, contributing to protect children and save lives in an increasingly unpredictable world.

Measuring fulfilment of the United Nations Sustainable Development Goals (SDGs)

Mobile data and other indicators related to telco services are a valuable resource to infer the progress on fulfilment of SDG goals; a key challenge addressed by the UN. For example, the use of text messaging is correlated with literacy levels among populations and the volume of international calls between countries reveals their level of mutual trade.

> *“A more human-centric approach is needed which empowers individuals to control how their personal data is collected and shared”.*
>
> *Giovanni Buttarelli, European Data Protection Supervisor*



Ana Zamora, Telefónica Digital employee.

3. Building trust in data through new data ethics

Given the huge value of data-driven services for people and society, data ethics are becoming increasingly important, embracing responsibility, transparency and choice.

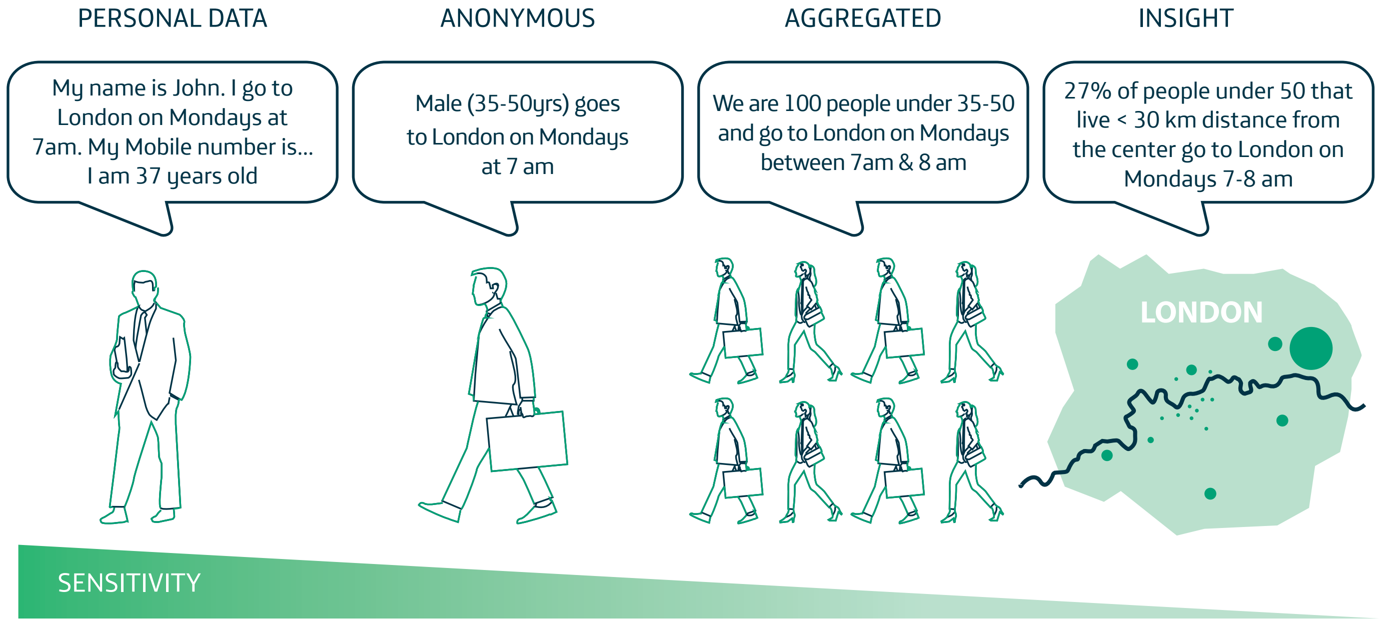
Data is powering the digital economy, but to have value, data must be put to work, not locked away. The power and number of opportunities that data presents grow rapidly when different types of data from various sources are combined. For example, data about non-human activity, such as weather and environmental data, can provide significant value, especially when combined with other information.

At this point, it is relevant to bear in mind the differences between personal and non- personal data. **We can consider as personal data any information that is linked to a customer and enriches the understanding of their reality. Non-personal data refers to information that is not linked to any specific customer.** For example, anonymous data is non-personal data. Much of the value and benefits of data usage can be harvested by using non-personal, anonymised data and insights based on data, thus respecting people’s privacy[22] (see case study on Luca).

Building trust in data is an ongoing process. **Better transparency should mean being open with people about what data is being collected, when it is collected and how it is used.** Common approaches are being reconsidered, so that long, complex and generally unread “terms and conditions” may cease to pass for transparency[23]. In order to achieve a meaningful level of transparency, people should be offered access to their personal data in a way that is simple and easy to use.

In that regard, Big Data and AI also represent an opportunity to improve transparency. Companies can use these technologies to build a personal relationship with each individual customer, tailored to their needs and preferences. In other words, they can provide people with better access to their own information, helping them to understand their options and giving them the ability to make personal choices. Such transparency is related to pricing and billing conditions, technical service features, liabilities and, most importantly, how personal data is collected, stored, processed and used[24].

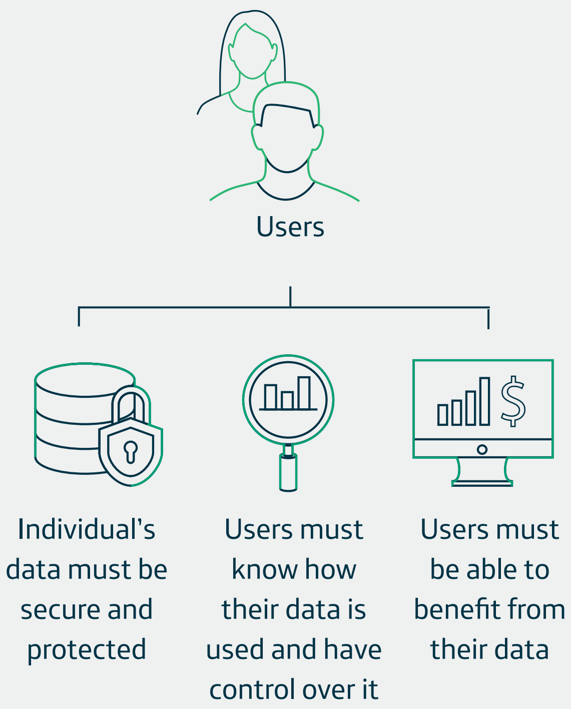
Chart 3: Personal info to anonymous insights


PERSONAL DATA
My name is John. I go to London on Mondays at 7am. My Mobile number is... I am 37 years old
ANONYMOUS
Male (35-50yrs) goes to London on Mondays at 7 am
AGGREGATED
We are 100 people under 35-50 and go to London on Mondays between 7am & 8 am
INSIGHT
27% of people under 50 that live < 30 km distance from the center go to London on Mondays 7-8 am
LONDON
SENSITIVITY

People should be empowered with their personal data, giving them control over how it is used. This means helping them to understand their data and giving options about its use.

Jessica Rodriguez, Daniel Souto and Marieli Granato,
Telefónica's Brazil employees.

Chart 4. How we do things.


Users
Individual's data must be secure and protected
Users must know how their data is used and have control over it
Users must be able to benefit from their data

1. Data must be safe and secure. Data security and customer privacy are the foundation of our business and our primary consideration when designing our services and collaborating with partners.
2. People should be able to decide how their data is used and remain in control of it. We will provide simple tools to manage their data-sharing choices, enabling easy access to their data, helping them decide how it is used and highlighting the associated risks and benefits.
3. We will make is easy for our customers to unsubscribe from services if they change their mind.
4. We will provide choices beyond the usual "take it or leave it" terms and conditions.
5. People should benefit from their data. Subject to their approval, we will use our customers' data to offer them simple and helpful services. We will provide personalised experiences and services. We will innovate with third parties to provide new data-enhanced services and generate value for our customers: value for themselves.

Data protection laws ensure fair processing and transparency practices, but the application of these concepts can be ineffective, since the global nature of data flows creates a complex situation for enforcement beyond national borders. Better international harmonisation of data protection and enforcement would help. In fact, cross-border data flows are increasingly regulated at international, regional and national levels to help protect people's privacy (see chapter 5 Modernising rights and policies).

A further step is to share the value of people's data with them. Such value may be realised in terms of improving digital products and services, making them better and simpler to understand. This also involves finding better ways to educate people about how their data is being generated and used. Transparency is a prerequisite for this control because it enables an understanding of the available choices. True choice is not possible without transparency.

People may also be presented with opportunities to use their data to generate value for third parties. Telefónica is developing a range of partnerships in order to allow our customers to put their data to work for them.

In addition, data portability needs to be improved. People should be able to use data for their own benefit across different platforms of their choice. For this to happen, people will need tools that facilitate access to the data they generate when using digital services and that enable them to transport that data.

In general, a good practice to achieve better privacy is "privacy by design". This ensures that privacy risks are fully considered and mitigated at the design stage of products and services.

Case Study

AURA, THE NEW RELATIONSHIP MODEL WITH OUR CUSTOMERS

Aura

Telefónica has developed Aura, an Artificial Intelligence (AI) service which aims to establish a new relationship model with customers by using personal data and cognitive services on top of our telecommunication infrastructure.

Aura aims to provide our customers with four superpowers:

- **Simplifying.** Performing actions and sending commands to the network and services quickly, just by talking to the tool.
- **Running algorithms** on customer datasets to infer insights that enrich their experience with Telefónica's services.
- **Empowering,** providing transparency and control over data generated by using Telefónica's services.
- **Discovering** what customers can do with the data they generate (proposals to use data for a purpose in exchange for a benefit/value, protecting privacy).

Aura's value proposition improves over time; it will be a trust path for customers: Aura will start with simple and enhanced ways for customers to interact with the company's existing services and will subsequently increase customers' benefits through new services, allowing them to control and exploit their own data within the telco or with third parties.

Aura uses cognitive intelligence to understand customers' needs and help proactively them by transforming available information into valuable knowledge. This knowledge about customers evolves over time, as they use Telefónica's products and services, while always leaving in the customers' hands to decide which of this knowledge the company maintains.

1. **Aura is a cognitive intelligence platform that listens to Telefónica's customers,** learning from them and enriching their experience of Telefónica's products and services.
2. Aura offers **a new way for customers to establish a relationship with Telefónica, introducing natural language capabilities:** technology adapted to people, not the other way round.
3. **Aura will empower people,** providing new ways for them to use their data, such as improving and personalising Telefónica's services and helping them to discover new ways to put their data to work for their benefit.
4. **Aura will give customers the power to decide** what data can be used in this knowledge generation process.
5. As **a cognitive intelligence platform,** Aura can be accessed through different paths (proprietary channels like our Mobile app, third party channels like Facebook Messenger and even through other assistants).

Aura is focused on helping customers get more from Telefónica's services and technology.

Digital transformation should put people first. It is enabled by disruptive technologies that both consume and produce data. Companies must protect and respect the data generated by users. Empowerment is key to a successful and trusted digital transformation. This can transform society and create a better future.

In short, Telefónica believes that platforms and services that adopt strong ethical principles, including transparency and control, will command trust and confidence and thus achieve the greatest and most sustainable success.

4. Rights and security

Networks and information systems play a crucial role in our current society. Their reliability and safety are essential for economic and social stability. Cybersecurity incidents can interrupt economic activities, generate considerable financial losses, undermine user confidence and cause great damage to a State's economy.

By 2022, 29 billion objects will be connected[18]. As the IoT grows, cars, planes, homes, cities and even animals will be interconnected, so the number of incidents affecting citizens' privacy and cybersecurity is also set to increase. Insufficient attention by the public and private sectors to cybersecurity could undermine trust in the Internet and jeopardise its ability to act as a driver of innovation.

Security and rights are inextricably linked. National security activities, like mass surveillance, need to guarantee human rights, which should be upheld by both public and private sector organisations. A stronger global dialogue, along with cooperation and standards, are needed in order to manage the inherent tension between cybersecurity and fundamental rights.

Initiatives by governments[19] and private companies are underway to promote annual transparency reporting regarding[20] government requests for data.

One example is the Global Network Initiative (GNI)[21], which takes a multi-stakeholder approach.

Others are more government-based, working within the United Nation system, or academic, like Ranking Digital Rights[22].

Such initiatives support collaboration between the public and private sectors for a healthier and sustainable digital ecosystem while developing global standards for transparency reporting by companies and government accountability regarding cybersecurity activities.

Keeping people's data safe should inform and shape the design of a new digital experience. Preventing data breaches should be a priority for every company. The complexity of technology, cyber threats and the potential for human error can lead to information being lost, deleted or falling into the wrong hands. Risk management is a continuous process and a prerequisite for building confidence.

Public and private cooperation, along with trust building and information sharing, are essential in order to anticipate attacks. Likewise, this cooperation is essential for incident management, in order to mitigate the impact and reverse the effects of any incidents.

Encryption has emerged as an essential security technology and is now widely deployed to guarantee data privacy. While it is a key security technology, it is equally important that it does not frustrate the efforts of public authorities to protect national security and public safety. Security and policy authorities like the FBI argue that they are ultimately unsuccessful to access encrypted information with legal authorisation, and call for a solution to this urgent public safety issue. It is vital that the impact of technologies on different rights is properly assessed and the principle of proportionality is respected. Ultimately, lawful and appropriate processes need to be defined to grant authorities proportionate access to information in a similar way as it happened with traditional telephony in the past.

5. Security in products and services

Going forward, the growth of the Internet of Things (IoT) will enable the connection of all devices and this greater dependency on technology is going to generate new security concerns that will require a more comprehensive and resilient security environment.

Society is adopting technology faster than it can secure devices, so risks will be exponentially multiplied despite the efforts made and best practices applied by the industry.

Additionally, the level of protection of digital products and services regularly declines over time. Therefore, all players across the entire value chain must strive to incorporate security measures into their products, from the first stages of engineering to the last (security by design). Furthermore, product manufacturers must maintain a strong commitment with security and respond quickly to deliver patches that solve new vulnerabilities as soon as they become aware of them. A clear security maintenance policy for devices should be a key topic of any contractual relationship.

The cost of security and the need to shorten time-to-market cannot be an excuse to avoid building the safe and secure products and services that consumers demand and need. It will be important to create a level playing field to enhance levels of cybersecurity across the entire value chain like, for example, the new EU NIS Directive does. Current regulatory asymmetries should be modified by adopting a "same service, same rules" approach for all companies, seeking to protect their users when they access any product, service or device. The IoT will interconnect all products and will turn all companies into technology companies. Any cybersecurity approach should, therefore, have a holistic and horizontal focus.

It is important to explore new ways of providing better cybersecurity:

- Cybersecurity self-certification of products, apps and services based on stakeholders' best practices and recommendations would set common standards and improve transparency for consumers and businesses.
- Consumers should have the possibility to update their digital products and services to the latest security standard within a reasonable timeframe.
- Improved awareness and knowledge by consumers through campaigns and better education on cybersecurity.

Case Study

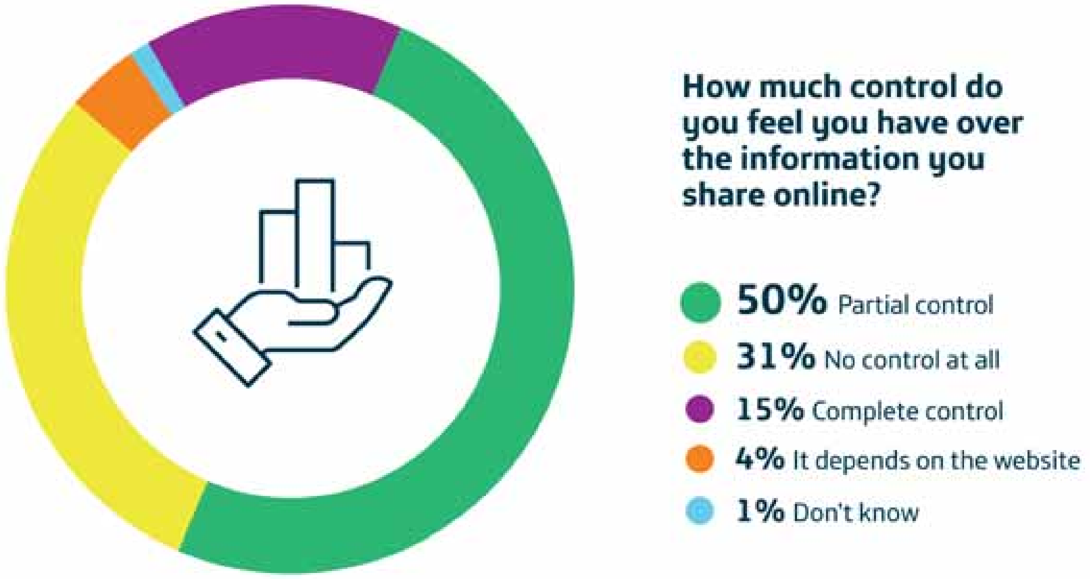
WANNACRY RANSOMWARE

- On May 12th 2017, 300,000 computers across 150 countries were frozen by a ransomware attack known as WannaCry.
- The attack crippled several hospitals in the British Public Healthcare System and infected a significant number of computers in multiple companies. China and Russia in particular were hardly affected.
- Spain was one of the first countries to acknowledge that it had been targeted by the ransomware, due to Telefónica's quick response confirming the attack the same morning its computers were infected.
- From the beginning of the incident, Telefónica contacted the authorities to inform them about the situation and collaborate in its resolution, opening an investigation and alerting other companies.
- Internally, security protocols were activated and none of the customer network's services were affected. The impact of the incident on the internal network was contained and normality was restored within 48 hours.
- Telefónica decided not to keep quiet in an exercise of transparency that helped governments and other companies to coordinate actions and mitigate the ransomware's effects.

Chapter 3: At a glance

The Issue

Data can enrich people's experiences and opportunities, but people often do not feel in control of their personal data and security risks are increasing.



Source: Eurobarometer (2015)

Our Belief

01. NEW DATA ETHICS

A human-centric approach should empower people to decide how and when their data is used.

02. TRANSPARENCY AND CHOICE

People should have access to their data and to all the information generated by them while having meaningful choices to be able to enjoy the value of their data.

03. NEW FORMS OF PUBLIC AND PRIVATE COOPERATION

New forms of public private cooperation as well as additional efforts to improve the security of products and services are needed.

04. GUARANTEEING SECURITY

It will be important to create a level playing field to enhance cybersecurity across the whole value chain.