In the digital era, Europeans push for stricter regulations to protect digital rights amid privacy concerns.

DIGITAL RIGHTS RESEARCH PROGRAMME

yourdigitalrights

Funded by
the European Union

yourdigitalrights

JÓVENES
EUROPEOS
FEDERALISTAS
ESPAÑA

CONTENT

ABSTRACT 5

INTRODUCTION 6

This report's value 6

SPECIFIC OBJECTIVES 8

Methodology 9

Conceptual frame 9

CONCEPTUALIZATION AND CONTEXTUALIZATION: THE ORIGIN OF THE SPANISH AND FRENCH CATALOGUE OF DIGITAL RIGHTS 11

HISTORICAL DEVELOPMENT OF DIGITAL RIGHTS 12

International context 12

European context 12

What are digital rights? 14

French and Spanish regulation 20

Influence of the GDPR 20

Individual context 20

Comparative on the matters regulated by France's and Spain's binding regulation on digital rights. 21

How new rights are promoted in the legal order. 21

Public services and economic transformation. 21

Rights related to data protection. 22

Other digital rights. 23

THE CONNECTIONS BETWEEN DIGITAL RIGHTS AND DIGITAL POLICY IN THE EUROPEAN UNION 26

COMPARATIVE REGULATORY AND PUBLIC POLICY ANALYSIS IN SPAIN, BELGIUM, FRANCE AND ESTONIA 30

Cyber-attacks and cybercrime prevention 31

Resources for promoting safety and well-being of children 34

Information and regulation on the use of personal and non-personal data by private and public sector 36

How the State uses its resources as well as EU ones to help people with difficulties accessing the online world 43

Case study: How Spain accompanied its binding regulation on digital rights with public policy instruments and strategies 52

How is promoted in the state a healthy use of digital tools (that means dealing with the difficulty of disconnecting and finding a good online/ offline balance) 58

What kind of public free resources are available for people learning new digital skills as well as their rights. 61

What kind of existing metrics measure the environmental impact of digital products and services in the country 65

WHAT IS MISSING? PUBLIC SURVEY QUESTIONS TO BETTER UNDERSTAND THE NEEDS OF EU CITIZENS MEASURES FOR THE DEVELOPMENT OF OUR DIGITAL RIGHTS (ELECTRONIC ID) 67

Relationship between digital identity and digital rights 68

The impact of digital identity on European citizens' digital rights 68

Challenges and opportunities for ensuring digital rights in the context of digital identity 69

Types of digital identity 69

Analysis of the development of digital identity in the European context 71

A pragmatic review of measures for the development of digital identity in Europe 71

Review of measures for the development of digital identity in Spain 72

Review of measures for the development of digital identity in Estonia 73

Review of measures for the development of digital identity in Belgium 75

Review of measures for the development of digital identity in France 75

Analysis and evaluation of best practices 77

Conclusions 78

LITERATURE REVIEW AND BIBLIOGRAPHY 79

ABSTRACT

We are currently living dual lives, the way in which our mobile phones have become a ubiquitous tool in our daily lives, enabling us to partake in the digital world. It serves as an extension of our selves, up to the point of we frequently check notifications almost every minute.

A world in which all our private information is stored: names, relatives, text and voice messages, videos and images, home addresses, your social security number and your entire identity is encapsulated in this virtual reality. The internet, which was once a tool for communication, has grown into a broad range of activities such as, learning, commerce, and activism. For instance, as we become increasingly connected it has also become a place to connect with our loved ones, it is now a place where we extrapolate our personal spheres too.

As this transformation has taken place, we have not always been able to recognize its novelty and the risks associated with it. Consequently, we do not usually realize how vulnerable we are when we give away our most sensible data to strangers online. As European citizens we recognise the Rule of Law as the bedrock of our Union and our future, and we have started demanding a deeper regulation of issues such as data protection, privacy, freedom of speech and the protection of minors.

In conclusion, Europe has faced the challenge of adapting Human Rights to the new digitalised spheres by both creating new rights and redefining existing ones. How has Europe managed to grant these rights and freedoms to its citizens throughout the Digital Revolution? This ongoing process forces us to face new challenges as we navigate this rapidly evolving digital landscape.

INTRODUCTION

In the year 2021, European Commission founded the beginning of the *Digital Decade* and developed the guidelines of the "Digital Compass" project. The goal of this plan is to reaffirm Europe's historic leadership in the pursuit of Human Rights and to strengthen its position during the global digital transition that is underway. As part of this initiative, several declarations as Tallin's or Lisbon's took place and open public consultations collected citizens ideas on the matter, establishing metrics which were carried out to know people's actual needs. Among those measures, the Special Eurobarometer 518 highlighted citizens' urgent need for legislation on *digital rights* as a starting point.

Once public claims were published, the European Parliament, along with the Council of the EU, approved the *European Declaration on Digital Rights and Principles for the Digital Decade* in January 2022. This declaration serves as a shared guide for the Union and member states' laws regarding the challenging expansion of democracy to these new, technological, and intangible borders which grants nobody is left behind in a fast-enough way.

To summarise, the *Declaration* considers the results of the Eurobarometer and offers *common* guidelines on how to address the challenges of the Digital Transition by prioritizing a democratic approach *which* defends people's rights *while provides them the necessary means to take an active role and become our most asset in the transformation.*

THIS REPORT'S VALUE

It is now our duty to discuss whether if we have fulfilled this goal or not. Taking the mentioned Eurobarometer and the Declaration on European Digital Rights and Principles as a basis to evaluate how Spain, France, Belgium and Estonia have contributed to the transformation by means of legal procedures, legislation, and several public policies. The reason for this selection is based on the fact that only Spain and France have regulated using binding legal instruments this matter, so their experience would be compared with the one developed in the other two countries where our project partners are based. We have posed ourselves some questions such as: “Have our rights been secured?” or “Do we have the adequate tools to face the upcoming digitalised world?” Questions which we will try to answer in the following pages.

This report is meant to be the first step of a thousand miles project supported by Erasmus+ Programme as a KA2 project to engage the youth on these matters while enhancing synergies between academic experts, institutional-related workers, and ordinary partner’s view.

Therefore, the project includes: (1) the creation of a web portal that hosts an online and accessible training platform on European digital principles and Digital Rights Laws that will be nourished by all the information and every developed tool gathered in the report, (2) the organization of an International Capacity Building Seminar held in Estonia where assistants will be taught how to raise awareness among the population about digital rights and, lastly, (3) a series of follow- up activities planned to spread knowledge of digital rights among EU population.

SPECIFIC OBJECTIVES

The European Declaration on Digital Rights and Principles is an attempt by the European institutions to unify and promote the digitalisation of Member States without losing sight of their fundamental values. As it is said at the beginning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) "Rapid technological developments and globalization have brought new challenges for the protection of personal data."[1]. The purpose of this report is to determine to what extent progress has been made towards the success of the objectives set out at the start of the Digital Decade, where it has been effective and where it could be improved.

Thus, our main objectives are:

1. **Observe** the actions of Member States aimed at meeting the goals of the Digital Transition. Ranging from legislation, rules and regulations to public policy plans carried out by state or local governments in the Union.

2. **Analyse the way in** which these actions have been implemented and assess their results with special attention to their scope according to criteria of geography (rural vs. urban environment) and age (young vs. old population).

3. **Compile** all tools, educational resources, grants and scholarships, citizen and business assistance programmes developed of free access, to make them available to citizens in a centralised and simple way.

Our field of study is limited to the Commission's objectives related to the protection of rights and freedoms in the digital environment. Therefore, the specific aspects that we will observe and assess are broken down into eight **sub-objectives.**

1. **Identify** legislation and public policies that act to promote the Digital Transition.
2. **Consider** how digital rights, especially those of minors, are protected.
3. **Evaluate** the measures taken to integrate people with special needs into the change and determine whether new technologies have an impact on their well-being.
4. **Judge** whether enough is being done to overcome the digital divide both in terms of connectivity in rural areas and in terms of facilitating access to digitised services for the ageing population.
5. **List** the means that the State offers citizens, businesses and researchers to take advantage of digitalisation in a positive way.
6. **Check** whether the ecological impact of this transformation is considered and whether the digital transition enhances environmental protection.
7. **List** actions to promote appropriate use of electronic devices, with a particular focus on the workplace and combating digital fatigue.
8. **Examine** the level of the Union's cyber security and what challenges the impending large-scale transformations present for the Union.

METHODOLOGY

As our study is focused on the actions of public bodies in member countries, the sources we will consult will be of the following nature:

1. Legal. We will consult laws and changes in Member States' regulations related to the subject of the report.

2. Public policies. We will focus on state or local actions carried out by Member State agencies. We will look at official publications, websites and statistical consultations carried out by public bodies that measure the performance of such schemes.

3. Survey. In the framework of elaboration of this report, a personalised questionnaire addressed to young people will be developed to help in the evaluation of the actions of public authorities.

4. Secondary sources. Adjacent to the latter, we will use the opinions of academics and professionals who are experts in the topics covered. We will use evaluation reports, articles and papers, among others.

CONCEPTUAL FRAME

Concluding this section, we offer a list of terms frequently used throughout the study.

CYBERSECURITY

Practices aimed at protecting data, systems and networks from operational threats or information theft.

RIGHT TO DATA PROTECTION

Set of rights ensuring that personal data are processed in accordance with the principles set out in Article 5 of the GDPR

OPEN DATA

Information in a format that can be understood, used and shared by anyone, which is standardised and is machine-readable.

DIGITAL RIGHTS

Or internet rights. These are a set of human rights applied to the online environment.

DIGITAL GAP

Lack of equal opportunities in accessing digital public services or taking advantage of digital tools causing major inequalities among the population.

DIGITAL FOOTPRINT

A set of information associated with a specific person, consisting of their data, browsing history and any traceable online events.

DIGITAL FATIGUE

Effect of prolonged exposure to electronic devices that can cause insomnia and reduced cognitive abilities.

SPECIAL CATEGORIES OF DATA

Sets of information relating to a person's ethnicity, sexuality or beliefs that could lead to discrimination.

FUNDAMENTAL RIGHT

A right considered to be a foundational right of the rule of law and enshrined in its constitution.

PERSONAL DATA

Any information on a natural person identified or identifiable by, for example, a name, an identification number or data descriptive of the person.(GDPR, 2016, article 4)

DATA PROCESSING

Any operation carried out with personal data, from its collection to its destruction, storage or use. (GDPR, 2016, article 4)

DATA CONTROLLER

Person or entity determining the purposes and means of the processing. (GDPR, 2016, article 4)

RIGHT TO NET NEUTRALITYA

The right to equal opportunities in the online environment. This refers to the means of access as well as the skills and treatment received.

CONCEPTUALIZATION AND CONTEXTUALIZATION:

1 - Historical development of digital rights

International context

European context

What are digital rights?

2 - French and spanish regulation

Influence of the GDPR

Individual context

3 - Comparative on the matters regulated by France's and Spain's regulation on digital rights.

How new rights are ptomoted in the legal order

Public services and economic transformation

Rights related to data protection

Other digital rights

THE ORIGIN OF THE SPANISH AND FRENCH CATALOGUE OF DIGITAL RIGHTS

HISTORICAL DEVELOPMENT OF DIGITAL RIGHTS

International context

Over a decade ago, our lives were irreversibly wrapped by Internet applications. Our social, labour, economic, and political relationships get increasingly dependent on cyberspace in a hyperconnected world like ours. Thus, from 2010 onwards we find digital related concepts examples in both national and international law. We become aware of this reality by observing, for instance, the pioneering 2013 reform of the Political Constitution of the United Mexican States[1], whose article 6 recognizes Internet access as one of its fundamental rights, or the Charter of Human Rights and Principles for the Internet[2] drafted by the Dynamic Coalition for Rights and Internet Principles (IRPC) within the framework of the UN Internet Governance Forum.

However, if we focus on the protection of citizen's rights within these new spheres, we ought to look to EU legislation for the last years as it has been the main benchmark on these matters.

European context

In 2010 the Commission provides a communication regarding an actualisation of the 1995 Personal Data Protection Directive attending to how "rapid technological developments and globalisation have profoundly changed the world around us and brought new challenges for the protection of personal data." (COM, 2010, p. 2)[3]. The goal was to defend the right to personal data protection in a context where "ways of collecting personal data have become increasingly elaborated and less easily detectable"[4].

In 2012 a Committee of Experts on Rights of Internet Users (MSI-DUI) was created by the Council of Europe. This Committee's' activity consisted of creating a Compendium of human rights for Internet Users. In other words, their chore was to establish how the Human Rights Declaration should be promoted online. This text once called the "Guide on Human Rights for Internet Users" received multiple modifications during many meetings so different stakeholders could participate. The final text had taken contributions from various expert's committees, civil society representatives and from the private sector and academia and so it was finally converted in the *Recommendation CM/Rec (2014)6 of the Committee of Ministers to member States on a guide to human rights for Internet users*[5] in 2014. A first step was taken towards a *digital rights* approach as Europe started to discern a new rights application field when the council established the Internet as a "valuable public service".

Finally, in 2016 a personal data protection regulation is approved by the EU's institutions following the 2012 European Commission Proposal. *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (GDPR) is conceived from a perspective which sees the previous *Directive 95/46/EC on General Data Protection Regulation* as outdated by the increasing speed of technological changes. The new regulation maintains the goals but tries to standardise the way in which member states collect, use and protect commercial private data aiming "to facilitate business by clarifying rules for companies and public bodies in the digital single market" (*Data protection in the EU*, 2021)[6]. To do so, the European Data Protection Board (EDPB) is established following the regulation instructions.

However, its elaboration was hard and controversial given the regulation action range (it would affect every company acting on EU ground or addressing EU citizens). Some US diplomats even accused the EU of doing "war on commerce" (Ramos, 2014)[7]. Therefore, this regulation does "not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity."(GDPR, p. 3, whereas 18)[8].

Regardless of the latter, it is still considered as a step forward. As Justice commissioner Didier **Reynders said,** "a reference point across the world for countries that want to grant to their citizens a high level of protection. We can do better though (...) we need more uniformity in the application of the rules across the Union" (*Press corner*, s. f.)[9]. *Given the momentum, the Eu Commission announces the* Digital Decade policy programme 2030 in which the digital future of the Union is set. On 26 January 2022, EU Parliament and Council agree on the aforementioned *European Declaration on Digital Rights and Principles for the Digital Decade.*

It is now relevant to analyse the status of the objectives of the proposed Digital Transition. We will begin by studying the legislation in France and Spain in regard to these objectives. As both countries have developed laws motivated by the GDPR that address some aspects related to the subsequent European declaration. It will be useful for this incoming *Decade* to expose and contrast how they have incorporated digital rights into their legal systems and what measures they have taken to enforce them.

What are digital rights?

European States began regulating data in the last century, as they became increasingly concerned rapid technological advances would enable despotic use of increasingly important information. This continues to pose a threat to society, and laws must try to keep pace with the times to keep it at bay. In the last decade, and even more so since the COVID-19 pandemic, we have witnessed how legal control cannot be limited to the protection of personal data. Internet has become a whole new universe, where the private and public spheres become intertwined in one.

Nowadays, as we work from home, we meet and keep in touch through social networks, we purchase goods and services online, and we educate and inform ourselves in digital media.

The Declaration of Human Rights is not a static text, nor are constitutions. Both must adapt to human changes where new needs arise in order not to become anachronistic. To do so, already engrained and consolidated freedoms must adapt to the new areas of action online and, more importantly, new fundamental rights *stricto sensu* must be developed which have to be legislated and recognised in constitutions. Examples are the right of universal access to the internet or the right to cybersecurity. (Barrio Andrés, 2021).

Broadly speaking, digital rights can be classified into different categories. The following are some of the most common ones:

1 RIGHT TO PROTECT THEIR PRIVACY IN THE DIGITAL ENVIRONMENT AND LIMIT ITS USE BY THIRD PARTIES.

2 PRIVACY RIGHTS

These include the right to privacy and the protection of personal data. This right allows citizens to control their personal data.

3 FREEDOM OF EXPRESSION RIGHTS

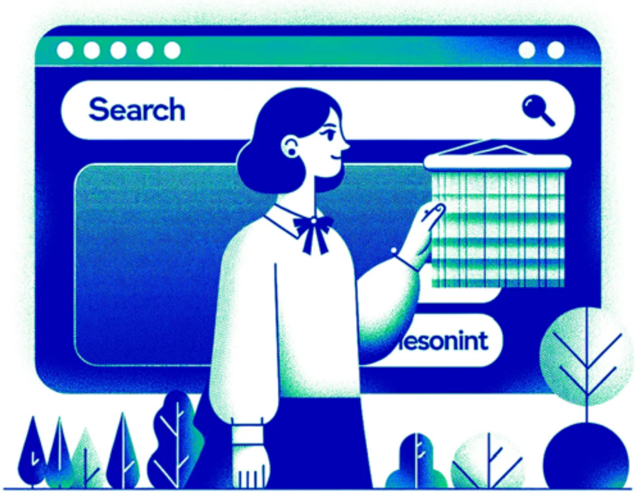
These include the right to free expression of opinions, ideas and thoughts on the Internet. This right protects citizens' freedom of expression online and ensures that they are not unfairly restricted.

4 ACCESS TO INFORMATION RIGHTS

These include the right of citizens to access public information and digital services provided by government and other organisations.

5 THE RIGHT TO NET NEUTRALITY

This right ensures that Internet service providers cannot discriminate against users on the basis of the content they consume.



6 THE RIGHT TO UNIVERSAL AND EQUAL ACCESS TO THE INTERNET

This right guarantees that all citizens have access to the Internet without discrimination.

7 RIGHT TO TRANSPARENCY AND ACCOUNTABILITY

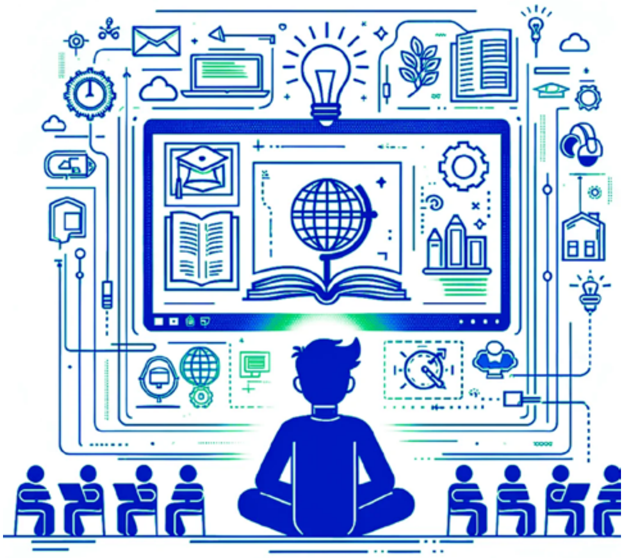
This right ensures that companies and governments are transparent in their use of citizens' personal data and are held accountable for its misuse.

8 CYBER SECURITY RIGHTS

These include the right to be protected against cyber attacks and the protection of confidential information. This right ensures that citizens can use the internet safely and securely.

9 RIGHT TO DIGITAL EDUCATION

This right ensures that citizens have access to education and training in technology and digital skills.



10 RIGHT TO ONLINE INTELLECTUAL PROPERTY

This right ensures that creators of digital content have their intellectual property rights protected and are fairly compensated for their work.

11 RIGHT TO BE FORGOTTEN

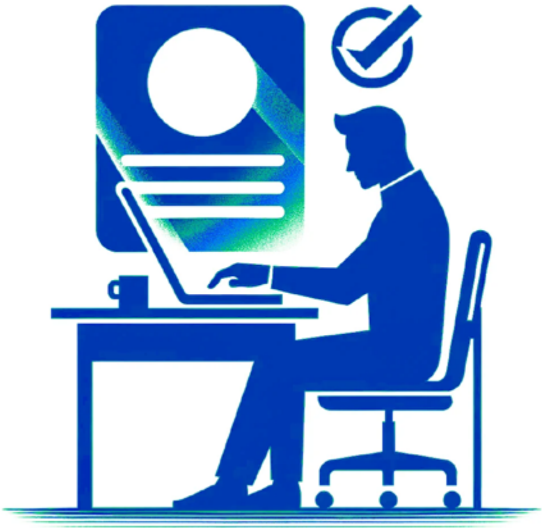
European citizens have the right to have their personal data removed from search engine results, provided that this data is inaccurate, outdated or irrelevant.

12 RIGHT TO DATA PORTABILITY:

Citizens have the right to receive a copy of their personal data in a structured format, so that they can easily transfer it to another service provider.

13 RIGHT TO RECTIFICATION

If a European citizen's personal data is inaccurate, he or she has the right to have it rectified without delay.



14 RIGHT TO RESTRICTION OF PROCESSING

Citizens have the right to request that the processing of their personal data be restricted in certain circumstances, such as when the accuracy of the data is contested or when an objection to the processing has been lodged.

15 RIGHT TO OBJECT

Citizens have the right to object to the processing of their personal data for legitimate reasons, such as direct marketing.

16 RIGHT NOT TO BE SUBJECT TO AUTOMATED INDIVIDUAL DECISIONS

Citizens have the right not to be subject to automated individual decisions, including profiling, which produce legal effects or significantly affect them in a similar way.

17 RIGHT TO PROTECTION AGAINST TRANSFER OF DATA TO THIRD COUNTRIES

European citizens have the right to have their personal data protected against transfer to third countries that do not provide an adequate level of data protection.

FRENCH AND SPANISH REGULATION

Influence of the GDPR

Law n° 2016-1321 of 7 October 2016 for a Digital Republic (Loi Lemaire) and the Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD) are drafted to go beyond the objectives and scopes of the GDPR.

The European Commission drafted such regulation to increase the effectiveness of personal data protection and to unify its implementation across the Union. The regulation maintains the objectives of the previous Directive 95/46/EC but considers that "Rapid technological developments and globalisation have brought around new challenges as far as personal data is concerned. The scale of the collection and sharing of personal data has increased significantly (...) Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data."

To meet the new challenges, the regulation, on the one hand, establishes the principles of personal data processing that must be complied with by all public and private entities operating in the territory of the Union or with its citizens: transparency, purpose limitation, data minimisation, accuracy, storage limitation and confidentiality and, on the other hand, it adds two novel concepts: the **single window system** as a form of supervisory authority (data protection agencies are created in each member country to form a European committee) and **active responsibility**, which means that the controller must be able to prove the lawfulness of its activity when required to do so.

Individual context

Loi No. 2016-1321 for a Digital Republic of 7 October 2016, also called the Lemaire Law, comes as part of a French government initiative to harness digitalisation as a lever for economic growth. An unprecedented citizen consultation inspired the draft law, which was subsequently opened to public input in an online process that allowed tens of thousands of contributions to result in ten new articles. This way of proceeding allowed the law a greater capacity to anticipate social changes, regulating *e-sports* by civil suggestion, for example. It also resulted in a unanimous approval in the Senate of the final text and a wider dissemination of the result among the population.

The case of *Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights*, or LOPDGDD, is a way of assimilating Regulation (EU) 2016/679.

The processing of this law began in 2016 and involved a public consultation process that was different from the French one, as it involved contributions from experts selected by the Ministry of Justice. Halfway through the process, Title X "Guarantee of digital rights" is added by amendment 298. The law then takes on an additional objective: "A desirable future reform of the Constitution should include among its priorities the updating of the Constitution to the digital era and, specifically, elevate to constitutional status a new generation of digital rights."(LOPDGPP, 2018, p. 119795)[11].

COMPARATIVE ON THE MATTERS REGULATED BY FRANCE'S AND SPAIN'S BINDING REGULATION ON DIGITAL RIGHTS.

How new rights are promoted in the legal order

In the French case, data protection and its implications for the freedom and privacy of citizens had already been developed in **Law n° 78-17 of 6 January 1978 on data processing, archives and liberties.** This law is the legislative development of French constitutional rights in the field of data processing. The Loi Lemaire does not repeal the previous law but updates it by accommodating the guidelines of the GDPR and adding new guarantees. Hence, what is introduced by the new law obtains great legal solidity.

In the Spanish case, the law was originally intended to accommodate the GDPR into national law and it is during its elaboration that an updated catalogue of perfectly defined rights is added. Unfortunately, the nature of Title X of the law is promotional because there are no precedents in Spanish law and there is no clear reference prior to its approval. Moreover, they lack institutional guarantee, as their promotion does not fall under the competence of the Spanish Data Protection Agency (AEPD) (Barrio Andrés, 2021, p. 109)[12].

In conclusion, the aim of the law is to serve as a bridge for the rights it contains to enter in the legal order by linking them to Article 18.4[13] of the Spanish Constitution and in this they collaborate with constitutional jurisprudence, which has declared rights such as the right to data protection to be fundamental rights (STC 94/1998 of 4 May 1998 - BOE núm. 137, de 09 de junio de 1998).

Public services and economic transformation

In the French case, the Digital Republic takes advantage of the technological transition and advances in data collection and processing to turn open data into a public service.

> *Precisely, the title I (circulation of data and knowledge) introduces multiple modifications to advance in the implementation of e-Government (...) It also makes access and circulation of public data and data of general interest more flexible for administrations and other entities in charge of public service missions, with special attention to areas such as the environment or energy, in line with the G8 countries' agreement on open data, but also recognising it as an axis of modernisation of the administration itself and a public service. (...) It also disciplines the publication in digital format, open and free of charge, of data such as those relating to the time spent by public officials in the media, road traffic, the results of research financed mainly by public funds and even certain administrative decisions; all of this, obviously, with respect for the limits set by privacy, private life and intellectual and industrial property.* (Boto Álvarez, 2018, p. 9)

In the Spanish case, the legislation limits itself to setting the framework to further foster the transformation of the public administration and economy with a view to complying with the provisions of Title X. It is worth mentioning that digital public administration regulations in the country are contained in other relevant legal instruments that are not part of the current report.

The rights relating to data protection are protected by the Spanish Data Protection Agency (AEPD) as dictated by the GDPR, but the rest of the added rights are progressively developed through subsequent legislation, such as in Law 10/2021 of 9 July on distance work. Issues that the French law explicitly addresses, such as the economic transformation of companies, territorial connectivity, and telecommunications, are developed in Spain by means of public policies and ministerial plans guided by the LOPDGDD, such as the Recovery, Action and Resilience Plan of the Ministry of Economic Affairs and Digital Transformation.

Rights related to data protection

Regarding data protection, Spanish legislation is in line with European legislation and transposes the GDPR guidelines one by one. Although it sometimes specifies some aspects that were imprecise in the former, it has been accused of causing regulatory inflation and devaluing the effectiveness of its imperatives: "the more rules are issued, the less value they have" (Barrio Andrés, 2021, p. 109)[16]. It therefore includes: the **right of access**, the **right of rectification**, the **right to erasure** (or the right to be forgotten), the **right to object** (to data being processed if the guarantees are not complied with), the **right to limit processing** to the purposes for which consent is given and the **right to portability**.

On the other hand, the Loi Lemaire does not redefine these rights, but opts for an individualised specification of each one in the different areas concerned. In other words, the French law expands and specifies the spheres of action of each right and frames them within the aforementioned complete transformation of the republic, in addition to providing additional means for the exercise of these rights by means of a supervisory body that pre-existed the supervisory authority that the European regulation orders to be created (in Spain, the Spanish Data Protection Agency).

AS A NOVELTY, BOTH LEGISLATIONS INCLUDE THE CONTROL OF DATA OF DECEASED PERSONS.

This is not covered by the GDPR (it is made explicit in Recital 27). It is possible for the heirs or persons related to the deceased to exercise the rights of access, rectification, and deletion of their data. In the event of the death of minors or disabled persons, the powers may also be exercised by a legal representative such as parents or guardians. The French law, as a novelty, adds that the deceased may designate instructions for his or her digital footprint after death and a person in charge of enforcing them and that, if this person is unable to do so, the responsibility would pass to the heirs.

Other digital rights

Finally, in the following table we can see how each law guarantees or includes the digital rights described by the United Nations and set as a common guideline for the Digital Decade.

	REGULATION (EU) 2016/679	LOPDGDD	LAW FOR A DIGITAL REPUBLIC
RIGHT TO INTERNET	-	It is only stated in Article 81.	Internet is guaranteed as a minimum public service: Article 108 outlaws cutting off network services. It was also recognised as a basic right by the French Constitutional Council.
NET NEUTRALITY	Creates “special categories of personal data” so as not to discriminate.	It is the same as the GDPR and defines the right in Article 79.	Article 42 gives ARCEP (Electronic Communications and Postal Authority) sanctioning powers to ensure net neutrality.
CONNECTIVITY	-	This matter is developed in later plans since 2020.	Several articles (69, 70, 74, 77) are devoted to national fibre deployment and local digital service provision plans.
DIGITAL GAP	-	Digital competences are added to public employee’s test. It is addressed systematically in posterior government plans.	The France Relance plan establish it as a priority.

PROTECTION OF MINORS	There are several articles specific to the protection of minors (8, 40, 57) and issues of consent are defined.	It sets the age of consent at 14, establishes a special criminal regime for offenders and proposes a specific law for the protection of minors.	Like the Spanish one, it adds a special right of erasure for data obtained from persons when they were minors in Article 63.
INTEGRATION OF PEOPLE WITH SPECIAL NEEDS	-	Some mentions, but no concrete means.	It obliges to adapt the relevant information on the web portals of its public administrations, as well as some services of large companies (Arts. 105 and 106).
DIGITAL WILL	It does not provide for this as part of its regulation (recitals 27 and 158).	The heirs of the deceased may exercise the power to decide on the fingerprint. In the event of the death of minors or disabled persons, the powers may also be exercised by parents or guardians. (Articles 3 and 96).	A directive on one's own personal data may be defined after death, a responsible person may be appointed and, if he or she is unable to do so, the heirs shall be responsible (Art. 63).
LABOUR RIGHTS	-	The right of disconnection is the most striking novelty. It is inspired by French labour law. It is developed in other laws. Regulates data protection in electronic business devices (arts. 87-91).	It regulates these aspects in its labour legislation, the novelty of the law is that it adds professional e-sports players to such regulations.

ENVIRONMENTAL IMPACT	-	-	In several articles it introduces the concept of “*Dematerialisation*”. It takes advantage of digitalisation to reduce energy and resource costs (examples in Art. 59, 6, 7 and 23).
EDUCATION IN DIGITAL RIGHTS AND COMPETENCES	It proposes the creation of State Data Protection Agencies to promote these purposes.	Amend education and university laws to integrate these skills.	The law provides the framework for this to be developed in subsequent plans and public policies.

THE CONNECTIONS BETWEEN DIGITAL RIGHTS AND DIGITAL POLICY IN THE EUROPEAN UNION

The development of digital rights and digital policy as an area of competence of the EU emerged in practice after the entry of the Maastricht Treaty in 1993. Digital technologies and systems were beginning to reshape important policy areas. In the period between 1993 and 2000, the share of information communicated through the internet rose from 1 to 50 percent of the total passing through telecommunications networks on the planet. The Delors Commission responded to this evolving digital space with two directives that would set the stage for future developments in this domain.

The Data Protection Directive of 1995 was aimed at addressing divergences in privacy laws among the member states, especially after the reunification of Germany in 1990. This drive relied on earlier negotiations on the automated processing of personal data at the Council of Europe. This led to the inclusion of articles on the respect for privacy and the protection of personal data in the Charter of Fundamental Rights, proclaimed in 2000. The Electronic Commerce Directive of 2000 was designed to provide a common legal framework for the provision of online services. It was therefore closely tied to the EU's core objective of developing the European Single Market. Both directives have their respective successors in the General Data Protection Regulation, adopted in 2016 and the joint Digital Services Act and Digital Markets Act, adopted in 2022. With this foundation, the EU institutional and policy environment began to consider additional areas from a rights and markets view, such as data economies, social media, connectivity infrastructure, cyber resilience, electronic governance and artificial intelligence.

The Barroso Commission took the next important step for the EU's digital policy, with its first ten-year strategy document, the Digital Agenda for Europe, released in 2010. The agenda broadened the established focus on digital protections to digital access and inclusion. Additional five-year strategy documents in 2015 and 2020 further enhanced the attention on the economic and societal importance of digital technologies. When in 2019, Ursula von der Leyen was appointed to the Commission's Presidency, she defined six priorities for the mandate, including one titled A Europe Fit for the Digital Age. The second ten-year strategy document, the Digital Compass, followed in 2021. This time, clear and ambitious targets on societal outcomes were set on digital skills, digital infrastructure, network connectivity, and digitalisation of public services.

The Commission’s strategies showed an increasing awareness of the interlinkages between digital policy and citizen’s rights. In these years, member states took complementary steps towards the enshrining of digital rights. The Tallinn Declaration of 2017 was signed by member states of the EU and European Free Trade Association (EFTA), who committed to improving the access to user-centric digital public services for their citizens. The declaration maintained a focus on EU legislation, such as compliance with GDPR and fundamental rights, such as the freedom of expression, the protection of privacy and the protection of personal data. This was expanded in two subsequent declarations. The Berlin Declaration of 2020 strengthened the call for democratic values to be present in the digitalisation of public administrations.

“IT IS OUR PROPOSED LEVEL OF AMBITION THAT BY 2030 THE PRODUCTION OF CUTTING-EDGE AND SUSTAINABLE SEMICONDUCTORS IN EUROPE INCLUDING PROCESSORS IS AT LEAST 20% OF WORLD PRODUCTION IN VALUE.”

[CITATION: EC, 2021]

The Lisbon Declaration of 2021 focused on balancing technological development with the respect for ethical principles and the promotion of human rights. These steps were crucial in the development of the EU’s digital agenda with an understanding of its interconnectedness with core EU principles and objectives. This understanding set the stage for the Commission’s initiative to address digital rights head on.

In her State of the Union address in September 2021, Ursula von der Leyen announced that the Commission was working on a declaration of digital principles. This initiative was presented at ensuring that EU values and rights are reflected in the digital space. Early discussions focused on key commitments, such as ensuring universal access to the internet, the creation of algorithms that respect people, and the management of a secure online environment. Thereafter, in January 2022, Thierry Breton, Commissioner for Internal Market, and Margrethe Vestager, Commissioner for Competition, presented the draft of the Declaration on Digital Rights and Principles. After an agreement was reached between the Commission, the Parliament and the Council in November, the declaration was finally signed in December 2022. In public affairs discussions, the initiative was viewed as providing a framework to shape the future of EU digital policy and digital transformation. Importantly, it also enshrined the concept and cases of EU citizen’s digital rights into the language of the institutions, as separate from past appeals to fundamental rights or core objectives.

The declaration made key normative statements on rights over access to empowering technologies, access to affordable connectivity, rights to digital skills education, rights to online protections at work, and online public services. Meanwhile, on algorithms and artificial intelligence, online safety, personal data, child protection the declaration made prescription statements, which are perhaps best read as policy intentions. The development of the EU's digital policy and digital rights has therefore been connected since its earliest stages. In the space of 30 years the EU institutions have prepared a growing number and breadth of responses to a likewise growing digital domain. The appropriateness of this development, which some authors qualify as "exponential" is the subject of much academic debate. For the purposes of this study however, it suffices to conclude that, should this trend persist, it is likely that the codification of digital rights at the EU level will continue to respond to and shape legislation of the digital space.

COMPARATIVE REGULATORY AND PUBLIC POLICY ANALYSIS

1 - Cyber-attacks and cybercrime prevention

2- Resources for promoting safety and well-being of children

3 - Information and regulation on the use of personal data and information by companies and public administrations

4 - How the State uses its resources as well as EU ones to help people with difficulties accessing the online world

5 - How have these states promoted a healthy usage of digital tools

6 - What kind of public free resources are available for people learning new digital skills as well as their rights.

7 - What kind of existing metrics measure the environmental impact of digital products and services in the country.

IN SPAIN, BELGIUM, FRANCE AND ESTONIA

Given the composition of the partner's consortium of the Erasmus + project that supports this research, we'll perform in the following pages a comparative review on how regulations, policy instruments and publicly available learning resources for citizens have been deployed in the only two European countries that have passed binding laws regulating digital rights, France and Spain, as well as in the other two countries which our partners are based, Estonia and Belgium. In order to perform the mentioned analysis, the following dimensions will be assessed:

1. Cyber-attacks and cybercrime prevention.
2. Resources for promoting safety and well-being of children.
3. Information and regulation on the use of personal data and information by companies and public administrations.
4. How the State uses its resources as well as EU ones to help people with difficulties accessing the online world (such as elderly people or those facing economic barriers).
5. How have these states promoted a healthy usage of digital tools (e.g. on/offline balance, disconnection, depression, addiction, physical health)?.
6. What kind of public free resources are available for people learning new digital skills as well as their rights.
7. What kind of existing metrics measure the environmental impact of digital products and services in the country.

Cyber-attacks and cybercrime prevention

The European Union recognizes the growing threat posed by cyber-attacks and cybercrime and has been taking measures to enhance cybersecurity and combat these challenges. Here are some key initiatives and developments:

EU Cybersecurity Strategy: In December 2020, the European Commission presented the EU Cybersecurity Strategy, which aims to bolster the EU's resilience against cyber threats and build a more secure and trusted digital environment. The strategy focuses on areas such as strengthening cybersecurity capabilities, fostering innovation, enhancing cyber resilience, and promoting global cyberspace stability. On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the response to cyber threats across the EU. The proposal will include a **European Cybersecurity Shield** and a comprehensive Cyber Emergency Mechanism to create a better cyber defence method.

NIS Directive: The EU adopted the Network and Information Security (NIS) Directive in 2016, which establishes security and reporting obligations for operators of essential services (OES) and digital service providers (DSPs). The directive sets out requirements for managing cybersecurity risks and reporting significant cyber incidents, aiming to enhance the overall cybersecurity posture across critical sectors.

European Cybersecurity Certification Framework: The EU has been developing a framework for certifying the cybersecurity of products, services, and processes. The European Cybersecurity Certification Framework aims to establish a common set of criteria and standards, allowing businesses and consumers to make informed choices about trustworthy and secure digital solutions.

Cooperation and Information Sharing: Collaboration and information sharing among EU member states and other relevant stakeholders are crucial in addressing cyber threats effectively. The EU encourages cooperation through initiatives like the European Union Agency for Cybersecurity (ENISA), which assists member states in improving their cybersecurity capabilities and facilitates the exchange of information and best practices.

Cybercrime Legislation: The EU has been working on strengthening legislation to combat cybercrime. The EU Cybercrime Directive, adopted in 2013, harmonizes laws related to attacks against information systems, child pornography, and other cybercrimes. Additionally, the EU is considering the proposed European Cybercrime Centre (EC3) to enhance the fight against cybercrime across member states.

Public-Private Partnerships: The EU promotes public-private partnerships to tackle cyber threats collectively. Initiatives like the European Public-Private Partnership for Resilience (EP3R) and the European Cyber Security Organization (ECSO) aim to foster collaboration between industry, academia, and governmental bodies to enhance cybersecurity capabilities and innovation.

It is important to note that cyber threats are continuously evolving, and combating cybercrime requires ongoing efforts and adaptability. The EU and its member states remain committed to improving cybersecurity and preventing cyber-attacks through collaborative approaches, legislative measures, and the promotion of best practices in cybersecurity.

Here some examples of **resources and initiatives developed** in France, Spain, Belgium, and Estonia **to fight against cyber-attacks and cybercrime:**

France

National Agency for the Security of Information Systems (ANSSI): ANSSI is the French national cybersecurity agency responsible for protecting government networks, critical infrastructure, and assisting public and private sector organizations in enhancing their cybersecurity capabilities. ANSSI provides technical expertise, guidance, and incident response support.

Cybercrime Prosecution Office (OCLCTIC): OCLCTIC is a specialized unit within the French National Police that investigates and combats cybercrime. It focuses on areas such as cyberattacks, online fraud, identity theft, child pornography, and terrorism-related cybercrime.

Spain

National Cybersecurity Institute (INCIBE): INCIBE is a Spanish government entity responsible for promoting cybersecurity and digital trust. It offers various resources, such as training programs, awareness campaigns, and technical assistance to individuals, businesses, and public administrations. INCIBE also operates the "Cybersecurity Emergency Response Team of Spain" (CERTSI) to respond to cyber incidents.

Joint Cybercrime Action Taskforce (J-CAT): Spain is an active participant in the J-CAT, an international initiative coordinated by Europol. J-CAT brings together cybercrime experts from EU member states, as well as non-EU partners, to collaborate and conduct joint operations against significant cyber threats.

Belgium:

Centre for Cybersecurity Belgium (CCB): CCB is the central authority for cybersecurity in Belgium. It coordinates efforts to protect the country's critical infrastructure and networks, promotes information sharing, and provides guidance on cybersecurity best practices. CCB also operates the Belgian Cyber Emergency Team (CERT.be) for incident response and coordination.

Federal Computer Crime Unit (FCCU): The FCCU is a specialized unit within the Belgian Federal Police that investigates and combats computer-related crime, including cybercrime. It focuses on areas such as hacking, online fraud, child pornography, and cyber terrorism.

Estonia:

Estonian Information System Authority (RIA): RIA is the central authority for cybersecurity in Estonia. It develops and implements national cybersecurity policies, provides guidance on cybersecurity practices, and operates the national Computer Emergency Response Team (CERT-EE) for incident response and coordination.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE): Estonia hosts the CCDCOE, an international organization focused on research, training, and exercises in the field of cybersecurity. It serves as a hub for NATO and allied countries to enhance cyber defense capabilities and collaborate on cyber policy matters.

These are just a few examples of the resources and initiatives in France, Spain, Belgium, and Estonia. Each country has its own specific organizations, agencies, and strategies to combat cyber attacks and cybercrime, reflecting their national priorities and cybersecurity landscapes.

Resources for promoting safety and well-being of children

It is crucial to release resources for promoting the safety and well-being of children in the digital world due to the following reasons:

Protection from Online Threats: Children are particularly vulnerable to various online threats, such as cyberbullying, harassment, exposure to inappropriate content, online grooming, and identity theft. By providing resources, guidelines, and educational materials, we can help children understand these risks, learn how to protect themselves, and empower them to make informed decisions online.

Digital Literacy and Responsible Internet Use: Releasing resources that promote digital literacy helps children develop the necessary skills to navigate the online world responsibly. They learn about privacy settings, critical thinking, media literacy, and how to identify and avoid potential dangers. These resources empower children to make positive choices, engage in responsible behavior, and develop a healthy relationship with technology.

Parental Guidance and Support: Resources can offer guidance and support to parents and caregivers in understanding the digital landscape and the challenges their children may face. By providing information about online safety measures, parental control tools, and strategies for open communication, parents can actively engage in protecting and guiding their children's digital experiences.

Mental and Emotional Well-being: The digital world has a significant impact on children's mental and emotional well-being. Resources that address topics like online harassment, cyberbullying, and excessive screen time can help children understand the potential negative effects and provide strategies for self-care, resilience, and seeking support when needed. These resources contribute to fostering a positive and healthy digital environment for children.

Collaboration and Awareness: Releasing resources on child online safety fosters collaboration among various stakeholders, including parents, educators, policymakers, and tech companies. It raises awareness of the importance of protecting children in the digital realm and encourages collective efforts to create safer online spaces. Collaboration is essential to developing effective policies, practices, and tools to mitigate risks and promote the well-being of children online.

Legal and Ethical Considerations: Releasing resources also aligns with legal and ethical obligations to protect children's rights. Many countries have enacted laws and regulations to ensure children's safety in the digital world, and providing resources helps fulfill these obligations. It demonstrates a commitment to safeguarding children's rights, privacy, and well-being in the context of advancing technology.

By releasing resources that promote the safety and well-being of children in the digital world, we can empower children, support parents and caregivers, foster collaboration, and address the unique challenges that arise in the online environment. These resources contribute to creating a safer, healthier, and more inclusive digital space for children to explore, learn, and thrive.

Considering the previous, given the final scope of this research to be the base for the **development of an online toolkit and training website,** below can be found some concrete **examples of free resources available** in Spain, France, Belgium, and Estonia for promoting the safety and well-being of children when using the internet and digital devices

Spain

“Internet Segura for Kids” by the Spanish Safer Internet Centre (IS4K): This initiative provides free resources, such as guides, videos, games, and workshops, to educate children, parents, and educators about safe internet use.

“PantallasAmigas”: This Spanish organization offers various free resources, including guides, videos, and interactive materials, to raise awareness about responsible digital citizenship and online safety for children and teenagers.

One click away from helping them: The Spanish Data Protection Agency collaborates in the campaign ‘A click away from helping them’ to raise awareness among minors about the risks they face on the Internet. It is an initiative of the European Association for Digital Transition, with the collaboration of the ATRESMEDIA Foundation and the ANAR Foundation. The aim is to help parents with the online activity of minors, alerting them to the risks and giving advice.

On the website of this campaign the user will also find help resources from the Agency, such as the ‘Guide that does not come with the mobile’ and the Priority Channel to request the removal of sensitive content published without consent.

Priority Channel: This is an online report channel available for any kind of citizen designed to to report the illegitimate publication on the Internet of sensitive, sexual or violent content, even without being the affected person. This channel has been set up to deal with exceptionally sensitive situations, when the contents (photographs or videos) are of a sexual nature or show acts of aggression and the rights and freedoms of those affected are being put at high risk, provided that they are Spanish nationals or are in Spain, especially if they are minors or victims of gender-based violence. Once the claimant uses this channel to report any kind of content that may infringed the previous, the Agency will analyse the claim as a priority and, if necessary, it will order the removal of the content to the service provider or platform where it is being disseminated. In addition, if there are indications of a crime, the Agency will bring it to the attention of the Public Prosecutor’s Office. In such circumstances, the Agency will inform the claimant of these steps. If appropriate, the investigation will continue in order to process a sanctioning procedure against the persons responsible for the dissemination.

France

“Internet Sans Crainte” by the French Safer Internet Centre: This platform offers free resources like guides, teaching materials, and games to help children, parents, and educators navigate the digital world safely.

“Mon-enfant-et-les-ecrans.fr” by the French Ministry of Health: This website provides information and resources to support parents in managing their children’s screen time and promoting a healthy digital environment.

Estonia

“DigiPesa” by the Estonian Union for Child Welfare: This program provides free resources, including games, videos, and teaching materials, to teach children about internet safety, privacy, and responsible online behavior.

“Noored Kooli” (“Youth to School”) Foundation: This Estonian organization offers free resources and training programs for teachers, including guidance on promoting digital well-being among students and addressing online risks.

Belgium

“Child Focus”: This Belgian foundation offers free resources, such as educational materials, advice, and awareness campaigns, to protect children from online risks and promote their well-being.

“Safeonweb”: This initiative by the Belgian Federal Public Service offers free resources and tips on safe internet use, including specific materials for children and young people.

These examples highlight a range of initiatives and organizations in Spain, France, Belgium, and Estonia that provide free resources aimed at promoting the safety and well-being of children when using the internet and digital devices.

Information and regulation on the use of personal and non-personal data by private and public sector

In today’s data-driven world, information has become a valuable asset for governments, businesses, and individuals alike. Two important categories of data that are extensively utilized for various purposes are personal data and open data. While both types of data contribute to the development of public and private initiatives, they differ significantly in their nature and usage.

Personal data refers to any information that relates to an identified or identifiable individual. It includes data such as names, addresses, social security numbers, financial details, and even digital footprints. Personal data is typically collected and processed with the consent of the individual and is subject to strict regulations and privacy considerations to safeguard individuals' rights and protect their privacy.

On the other hand, open data refers to the information that is freely available to the public, often provided by government agencies, organizations, or individuals. Open data is characterized by its accessibility, usability, and the absence of restrictions on its use. It encompasses a wide range of information, including government reports, statistical data, geographic data, scientific research, and more. The purpose of open data is to promote transparency, enable innovation, and foster collaboration by allowing individuals, businesses, and researchers to access and utilize the data for various purposes.

In this context, countries such as France, Spain, Belgium, and Estonia have recognized the potential of both personal data and open data for driving public and private initiatives. They have implemented regulatory frameworks to govern the responsible use and protection of personal data, ensuring individuals' privacy rights are respected. Simultaneously, these countries have established initiatives and legal frameworks to promote the availability and reuse of open data, enabling innovation, research, and the development of public services.

By understanding the distinctions between personal data and open data, and the regulatory frameworks surrounding their use, these countries aim to strike a balance between harnessing the power of data for societal benefit while safeguarding individual privacy and promoting transparency. This article will delve into how France, Spain, Belgium, and Estonia utilize personal data and open data for public and private initiatives, while also exploring the regulatory instruments they have developed to govern these data categories.

Considering the previous, in the following lines it can be found an overview of how France, Spain, Belgium, and Estonia **use personal data and open data for developing public and private initiatives:**

France

France has implemented various initiatives to leverage personal data and open data for public and private purposes. The French government has created the Open Data Portal (data.gouv.fr), which provides access to a wide range of public datasets. These datasets are used by both the government and private organizations to develop innovative solutions, research projects, and public services.

Spain

Spain has been actively promoting the use of personal data and open data for public and private initiatives. The Spanish government operates the Open Data Portal (datos.gob.es), which offers access to a vast array of public datasets. These datasets are utilized by various stakeholders, including government agencies, businesses, researchers, and developers, to drive innovation and create new services.

Belgium

In Belgium, personal data and open data play a crucial role in public and private initiatives. The Belgian government promotes the use of open data through the federal open data portal (data.gov.be) and regional portals. These platforms offer access to a wide range of datasets for businesses, researchers, and citizens to utilize in developing innovative solutions and improving public services.

Estonia

This Baltic country is widely recognized as a pioneer in utilizing personal data and open data for public and private initiatives. The Estonian government has implemented the X-Road platform, which securely integrates various databases and enables the exchange of data between government agencies, private organizations, and citizens. This infrastructure forms the basis for a wide range of digital public services in Estonia. The country has also embraced the concept of "data embassies," where copies of government data are stored and protected in secure data centres located in other countries.

Overall, France, Spain, Belgium, and Estonia have implemented initiatives to promote the use of personal data and open data in developing public and private initiatives. They have established open data portals, all have implemented national data protection regulations that comply and complement the GDPR, and created frameworks to facilitate innovation, research, and the development of digital services. These efforts aim to balance the benefits of data utilization with the protection of individuals' privacy and security.

Considering the previous, it is convenient to list at this point the **regulatory frameworks for open data and information reuse in the public and private sectors** of France, Spain, Belgium, and Estonia:

France

French Digital Republic Act (Loi pour une République Numérique): This legislation in France promotes open data and information reuse. It establishes the principle of open by default for public sector information and mandates the publication of certain types of data through the Open Data Portal (data.gouv.fr). It also defines the rights and obligations related to open data reuse by both the public and private sectors.

Spain

Spanish Reuse of Public Sector Information Act (Ley de Reutilización de la Información del Sector Público): This law promotes the reuse of public sector information in Spain. It establishes the framework for making public sector information available for reuse, ensuring transparency and fostering innovation. It defines the rights and obligations of public sector bodies and users regarding the reuse of information.

Belgium

Belgian Reuse of Public Sector Information Act (Wet Hergebruik van Overheidsinformatie): This legislation encourages the reuse of public sector information in Belgium. It sets out the rules for the availability and reuse of public sector information, aiming to stimulate innovation, economic growth, and transparency. It outlines the rights and obligations of public sector bodies and users regarding the reuse of information.

Estonia

Estonian Public Information Act (Avaliku teabe seadus): This law in Estonia governs the availability and reuse of public sector information. It ensures that public sector information is open and accessible, promoting transparency and innovation. It establishes the rights and obligations of public sector bodies and users regarding the reuse of information.

These regulatory frameworks provide the legal basis for open data and information reuse in the public and private sectors of France, Spain, Belgium, and Estonia, emphasizing the importance of transparency, accessibility, and innovation by enabling the reuse of public sector information for various purposes, including research, business development, and service improvement.

Considering the previous, this section would finish identifying some concrete national good case practices of these type of data use in both the public and private sphere:

Here are some concrete examples of **businesses** from France, Spain, Belgium, and Estonia **that have utilized open data from their respective states to enhance their activities:**

France

BlaBlaCar: BlaBlaCar, a well-known French ride-sharing platform, leverages open data from various sources, including government transport data, to optimize its services. By integrating open data on public transportation schedules, traffic conditions, and road networks, BlaBlaCar improves its route planning algorithms, estimates travel times more accurately, and enhances the overall user experience.

Dataiku: Dataiku, a French data science and AI software company, utilizes open data to enhance its data analysis and machine learning capabilities. By accessing open data sources such as government statistics, weather data, and demographic information, Dataiku empowers organizations to derive valuable insights, build predictive models, and make data-driven decisions.

Spain

Idealista: The most famous Spanish real estate platform, utilizes open data from government sources to provide comprehensive property listings and insights to its users. By integrating open data on property prices, neighbourhood demographics, and transportation networks, Idealista offers accurate and up-to-date information to home buyers, renters, and real estate professionals.

Carto: This Spanish location intelligence and data visualization platform, harnesses open data to create interactive maps and spatial analytics solutions. By accessing open data on demographics, infrastructure, and environmental factors, Carto enables businesses to gain valuable location-based insights, optimize resource allocation, and make informed decisions.

Estonia

Bolt: This Estonian ride-hailing and transportation platform, utilizes open data, including government transport data, to provide efficient and reliable transportation services. By integrating open data on public transportation routes, traffic congestion, and road conditions, Bolt optimizes its driver dispatch system, improves route planning, and enhances the overall ride experience.

Veriff: This Estonian identity verification platform, leverages open data for identity verification and fraud prevention. By accessing government-issued identity document data and other relevant open data sources, Veriff enhances its AI-powered identity verification algorithms, ensuring secure and reliable online identity verification for businesses and individuals.

Belgium

SNCB/NMBS: The Belgian national railway company, SNCB/NMBS, utilizes open data to improve its train services. By making real-time train schedules, delays, and disruptions available as open data, developers and businesses can create applications that provide accurate train information to commuters, facilitating better travel planning and reducing inconvenience.

TomorrowLab: This Belgian innovation consultancy, leverages open data from various sources, including government datasets, to drive innovation projects. By accessing open data on energy consumption, traffic patterns, and environmental factors, TomorrowLab develops solutions that promote sustainability, optimize resource usage, and address societal challenges.

These examples demonstrate how businesses from France, Spain, Belgium, and Estonia have utilized **open data provided by their respective states to enhance their activities.** By leveraging open data sources, these companies have improved their services, optimized operations, and delivered value-added solutions to their customers and clients. Additionally, some good examples of implementation of this utilization can be found in the development of certain services in the public sector of all these countries as can be found below:

France

Etalab: Which is the French government agency responsible for open data, has played a significant role in promoting open data practices in the public sector. Etalab has developed and maintained the Open Data Portal (data.gouv.fr), making a vast amount of government data available to the public. Through their initiatives, Etalab has fostered transparency, citizen engagement, and innovation by encouraging the reuse of open data for various purposes, including research, analysis, and the development of public services.

Spain

AEMET Open Data: The Spanish State Meteorological Agency (AEMET) provides open data on weather and climate conditions. By making this data freely available, AEMET enables citizens, businesses, and researchers to access accurate and real-time weather information. This empowers individuals and organizations to make informed decisions, such as planning outdoor activities, optimizing agricultural practices, and improving resource management.

Belgium

Open Knowledge Belgium: Open Knowledge Belgium is a non-profit organization that promotes open data initiatives in the country. They work closely with government agencies, civil society, and businesses to advocate for open data practices and provide guidance on data release. Their efforts have led to increased availability of open data in Belgium, enabling various stakeholders to utilize the data for research, innovation, and the development of public services.

Estonia

X-Road: Estonia’s X-Road platform is a notable example of open data utilization in the public sector. It enables secure data exchange and interoperability among government agencies, allowing for seamless sharing of information and efficient provision of public services. X-Road has enhanced data accessibility, reduced bureaucracy, and facilitated citizen-centric digital services, making Estonia a leading example in e-governance and open data utilization.

These case practices exemplify successful implementations of open data initiatives in the public sector. They highlight the benefits of increased transparency, citizen engagement, and data-driven decision-making. By making data openly available, governments foster innovation, empower citizens, and improve the efficiency and effectiveness of public services.

IN CONCLUSION, **THE COMBINATION OF OPEN DATA RESOURCES AND THE RESPONSIBLE USE OF PERSONAL DATA HOLDS IMMENSE POTENTIAL FOR ENHANCING DIGITAL ECONOMY-RELATED SERVICES AND BUSINESSES.**

By leveraging these two types of data, governments and businesses can foster innovation, drive economic growth, and deliver more personalized and efficient services to users.

Open data serves as a valuable resource that fuels innovation and promotes collaboration. Its availability enables businesses to access a wide range of information, including government statistics, geographic data, and research findings. By leveraging open data, businesses can gain insights, identify market trends, and make data-driven decisions that enhance their products and services. Furthermore, open data empowers entrepreneurs, researchers, and developers to create new applications, tools, and solutions that address societal challenges and drive economic development.

Simultaneously, the responsible use of personal data adds a layer of personalization and customization to digital economy-related services and businesses. By adhering to data protection regulations and respecting individual privacy, businesses can collect and analyse personal data to understand user preferences, behaviours, and needs. This allows for the creation of tailored offerings, personalized recommendations, and improved user experiences. For example, businesses can use personal data to provide personalized advertisements, customized product suggestions, or optimized user interfaces, enhancing customer satisfaction and loyalty.

The synergy between open data resources and the appropriate use of personal data creates a virtuous cycle. Open data provides the foundation for innovation and research, while personal data adds the dimension of individual preferences and context. By combining these data sources, businesses can unlock new insights, develop targeted strategies, and deliver services that cater to specific user needs.

This, in turn, drives customer engagement, fosters economic growth, and strengthens the digital economy ecosystem as a whole.

However, **it is crucial to emphasize that the use of personal data must be conducted ethically and with utmost consideration for privacy and data protection.** Data security measures, user consent frameworks, and transparent data governance practices are essential to build trust among users and ensure responsible data handling.

IN CONCLUSION, **THE COMBINATION OF OPEN DATA RESOURCES AND THE APPROPRIATE USE OF PERSONAL DATA PRESENTS EXCITING OPPORTUNITIES FOR THE DIGITAL ECONOMY. BY LEVERAGING THESE DATA SOURCES EFFECTIVELY AND RESPONSIBLY, BUSINESSES CAN DRIVE INNOVATION, CREATE PERSONALIZED EXPERIENCES, AND CONTRIBUTE TO THE OVERALL GROWTH AND DEVELOPMENT OF THE DIGITAL ECONOMY ECOSYSTEM.**

How the State uses its resources as well as EU ones to help people with difficulties accessing the online world

The digital divide is a phenomenon that has become increasingly important, disproportionately affecting different population groups. European Union citizens can face various types of digital divides that can hinder their access to and participation in the digital world. These divides include:

1 SOCIO-ECONOMIC DIVIDE

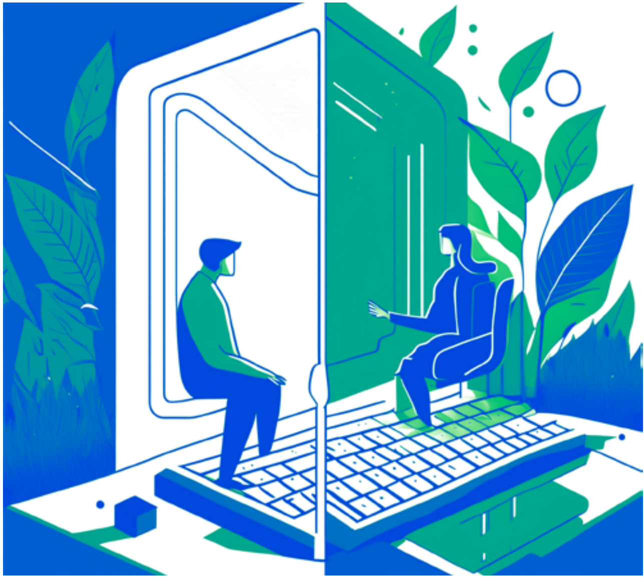
People with low incomes or limited financial resources may struggle to afford the necessary digital devices, internet connectivity, or access to digital services, creating a divide based on economic disparities.

2 AGE DIVIDE

Elderly individuals, who may have limited exposure to technology or digital skills, can face difficulties in accessing and utilizing online platforms and services, leading to an age-based digital divide.

3 DISABILITY DIVIDE

Individuals with disabilities encounter barriers in accessing the online world due to physical, cognitive, or sensory impairments. Inaccessible websites, digital content, and lack of assistive technologies contribute to a digital divide for people with disabilities.



4 RURAL-URBAN DIVIDE

Residents in rural or remote areas often have limited access to reliable internet connectivity and face infrastructure challenges, leading to a digital divide between urban and rural populations.

5 GENDER DIVIDE

Women may face specific barriers and inequalities in terms of internet access, digital skills, and opportunities in the digital sector, contributing to a gender-based digital divide.

Additionally, **specific groups of the population may encounter difficulties accessing the digital world,** including:

Elderly individuals: Older people may lack familiarity with technology and digital platforms, leading to challenges in accessing and using digital services effectively.

Low-income individuals: People with limited financial resources may struggle to afford internet access or digital devices, limiting their participation in the digital economy.

People with disabilities: Individuals with physical, cognitive, or sensory impairments face accessibility barriers that prevent them from fully utilizing digital platforms and services.

Rural and remote communities: Residents in remote or underserved areas may have limited access to reliable internet connectivity, creating barriers to online participation.

Women: Gender disparities can affect women's access to digital resources, digital literacy, and opportunities in the digital sector, contributing to the gender divide in digital inclusion.

Recognizing and addressing these digital divides and the challenges faced by these groups are crucial for promoting digital inclusion and ensuring equal access to the benefits of the digital world for all EU citizens. The European Union aims to bridge these divides through policies and initiatives that address infrastructure gaps, promote digital skills development, encourage diversity and inclusivity, and ensure equal opportunities in the digital sector.

From the perspective of public policy and legal framework, it is crucial to address this issue to ensure the full exercise of rights and equal opportunities for all citizens, regardless factors such as their economic status or age. In the **EU, citizens' digital competences are measured based on their competency level in five specific areas or dimensions:** searching and interpreting digital information, communicating and collaborating using digital tools, creating and publishing content, understanding the security implications of the digital world, and using digital tools to solve everyday problems.

Considering the previous, find below the analysis performed to identify how Spain, France, Belgium and Estonia use their public resources to help people with difficulties accessing the online world: In Estonia, France, Spain, and Belgium, various resources and initiatives are available to assist individuals with difficulties accessing the online world. These resources aim to promote digital inclusion, enhance digital skills, and provide support for those who face barriers to online participation. Here are some examples:

Estonia

e-Estonia Briefing Centre: The e-Estonia Briefing Centre in Tallinn provides information and training on e-governance, digital services, and innovative solutions. It offers guided tours, presentations, and consultations to individuals and delegations interested in learning about Estonia's digital transformation.

Tiger Leap Foundation (Tiigrihüpe): The Tiger Leap Foundation focuses on integrating digital technologies into education. It offers training programs, resources, and initiatives to improve digital literacy and skills among students, teachers, and the general public.

Spain

Red.es: Red.es is a public entity in Spain that promotes the digital transformation of society. They offer various programs and initiatives aimed at reducing the digital divide and fostering digital inclusion. These include training programs, grants, and support for digital infrastructure in underserved areas.

Telecentre Network: The Telecentre Network comprises community centers and telecentres throughout Spain that provide access to technology and digital training. They offer resources, courses, and workshops to enhance digital skills and promote social inclusion.

France

French Digital Inclusion Association (Inclusion Numérique): Inclusion Numérique promotes digital inclusion and offers support to people with limited access or skills. They provide training programs, resources, and awareness campaigns to bridge the digital divide and empower individuals in using digital technologies effectively.

Public Libraries: Public libraries across France play a crucial role in supporting digital inclusion. They offer free internet access, computer facilities, and digital literacy programs to help individuals acquire digital skills and access online resources.

Belgium

Digital Inclusion Plan (Plan d'Inclusion Numérique): Belgium has a Digital Inclusion Plan that focuses on reducing the digital divide and enhancing digital skills. The plan includes initiatives such as training programs, awareness campaigns, and partnerships to provide support to individuals and communities with limited access or skills.

Local Digital Inclusion Initiatives: Several municipalities and organizations in Belgium run local digital inclusion projects. These initiatives offer training sessions, workshops, and support to help individuals gain digital literacy skills and overcome barriers to online participation.

These are just a few examples of the resources available in Estonia, France, Spain, and Belgium. Each country has a range of governmental, non-profit, and community-based initiatives working toward digital inclusion and providing support to individuals who face difficulties accessing the online world.

In addition to the resources mentioned earlier, Estonia, France, Spain, and Belgium offer various online training materials and public aids to help individuals access the internet and improve their digital skills. Here are some examples:

Estonia

Eesti.ee: The official Estonian government portal, Eesti.ee, provides a wide range of online training materials and resources to help individuals learn about digital services and develop their digital skills. It offers tutorials, guides, and practical information on topics such as e-services, digital signatures, and online security.

France

PIX: PIX is a free online platform in France that offers self-assessment and training in digital skills. It covers various competency areas, including information and data literacy, communication and collaboration, and digital security. Users can assess their digital skills, access training modules, and earn digital certifications.

La Base: The General Interest Digital Database (La Base in French) allows to gather and organize on a single platform all the tools and resources at the service of general interest in terms of digital training. It is open to other stakeholders to host tools and resources, being the first national database of this matter.

Spain

Conecta Empleo by Fundación Telefónica: Conecta Empleo is an online training platform developed by Fundación Telefónica in Spain. It provides a wide range of courses and resources to improve digital skills and enhance employability. The platform covers topics such as basic digital skills, coding, data science, and entrepreneurship.

Orange's Social Tariff (Tarifa Social): Orange, one of the major telecommunications providers in Spain, offers a Social Tariff program to help individuals with limited financial resources access internet connections. This program provides discounted rates for eligible individuals and aims to bridge the digital divide by making internet access more affordable.

D-Generation Pact: The Generation D Pact is a commitment between more than 50 administrations and public entities, companies, associations, foundations, social agents, the third sector and the media to provide citizens with digital knowledge and skills. The objective is to create a cohesive, coordinated and complete ecosystem to make visible and involve Spanish society in the digital transformation process, in order to close the digital skills gap, raising the percentage of the Spanish population with these skills from 70% to 100%. In order to make the offer of courses and initiatives more visible, a collaborative web portal has been set up for the members of the project, which will serve as a loudspeaker for all the digital skills initiatives carried out in Spain. Dissemination and awareness-raising campaigns will also be carried out, and RTVE (National Public Broadcasting Corporation) will play an important role in the broadcasting of content on digital skills at prime time, as well as the broadcasting of specific programming on all of the Public Broadcasting Corporation's media.

Belgium

Digital Wallonia: Digital Wallonia is an initiative in Belgium that promotes digital inclusion and offers online training resources. It provides access to a variety of courses, tutorials, and webinars covering digital skills, coding, entrepreneurship, and more. The platform aims to support individuals in developing their digital competencies.

Belgian Digital Agenda: The Belgian Digital Agenda is a government initiative that promotes digital transformation and digital inclusion. It provides information and resources on various digital topics, including digital skills development. The agenda highlights the importance of digital literacy and offers guidance on training programs and initiatives available in Belgium.

These online training materials and public aids help individuals enhance their digital skills, gain confidence in using digital technologies, and overcome barriers to online participation. They offer accessible and self-paced learning opportunities that can be beneficial for individuals seeking to improve their digital proficiency.

It’s important to note that these examples are not an exhaustive list, and there may be additional online training platforms and public aids available in each country. Exploring official government websites, telecommunications providers, and digital inclusion initiatives can provide more information on specific online training materials and public aids tailored to the needs of individuals in Estonia, France, Spain, and Belgium.

Considering the importance of public aid mechanisms such as the Spanish Social Tariff for ensuring equal access to internet for all types of population’s groups, it is worth mentioning the existence of further instruments as such in the other countries:

Estonia

KredEx Internet Subsidy: The Estonian government, through the KredEx foundation, provides an Internet Subsidy program to support low-income families and individuals in accessing affordable internet services. Eligible applicants can receive financial assistance to cover part of their internet service costs.

France

Solidarity Digital (Solidarité Numérique): Solidarity Digital is a French government program that aims to bridge the digital divide and provide support for individuals facing digital exclusion. It offers various resources, including information on low-cost internet offers and financial aid for internet subscriptions for eligible individuals.

Belgium

Internet pour Tous (Internet for All): Internet pour Tous is an initiative in Belgium that promotes digital inclusion and affordable internet access. It works in collaboration with internet service providers to offer reduced-cost internet subscriptions for individuals and families with limited financial means.

It's worth noting that specific eligibility criteria and program details may vary for each social tariff initiative. These programs are designed to ensure that individuals with financial constraints have access to affordable internet services, thereby promoting digital inclusion and reducing the digital divide.

For more information and to determine eligibility for these social tariffs or similar programs, individuals can visit the official websites of relevant government entities, telecommunications providers, or digital inclusion initiatives in their respective countries.

2023 has been designated by the European Union as the European Year of Skills, recognizing the crucial role that skills development plays in shaping a prosperous and resilient Europe. This dedicated year underscores the importance of skills in driving innovation, fostering economic growth, and addressing societal challenges. With rapid technological advancements and evolving labour market needs, it is essential to equip individuals with the necessary skills to thrive in the digital era. By promoting and investing in skills development, the European Union aims to empower its citizens, enhance employability, promote social inclusion, and ensure a competitive advantage in the global landscape. The European Year of Skills serves as a catalyst for policy actions, initiatives, and collaborations at the European, national, and local levels, emphasizing the value of skills as a transformative force for individuals, businesses, and society as a whole.

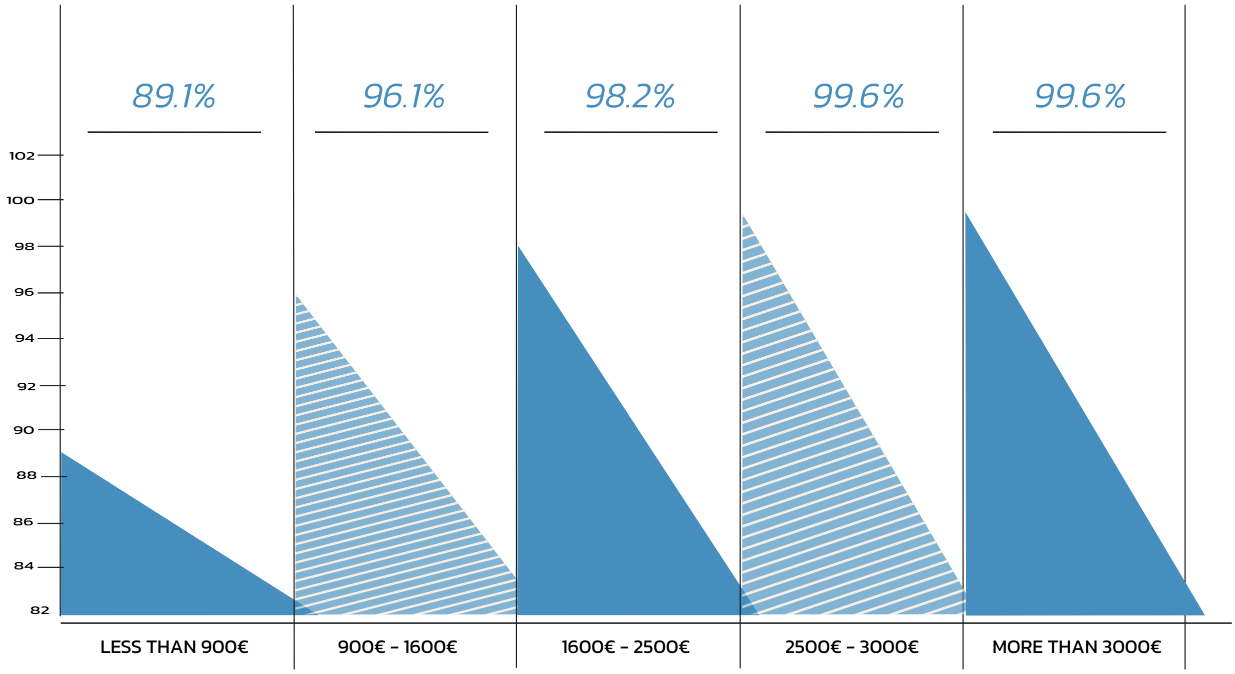
Furthermore, **a key aspect of the European Year of Skills is the recognition of the importance of ensuring equal and accessible access to digital education tools that are adapted to the needs of all population groups**. This includes individuals of different ages, backgrounds, abilities, and geographical locations. By bridging the digital divide and providing inclusive digital education opportunities, the European Union can promote social cohesion and prevent the exclusion of marginalized groups. It is essential to invest in educational resources, training programs, and infrastructure that enable everyone to acquire digital skills and participate fully in the digital society.This emphasis on inclusivity reinforces the principle that

NO ONE SHOULD BE LEFT BEHIND IN THE DIGITAL TRANSFORMATION, FOSTERING A MORE EQUITABLE AND COHESIVE EUROPEAN UNION THAT HARNESSES THE POTENTIAL OF ALL ITS CITIZENS.

CASE STUDY: HOW SPAIN ACCOMPANIED ITS BINDING REGULATION ON DIGITAL RIGHTS WITH PUBLIC POLICY INSTRUMENTS AND STRATEGIES

Data for Spain shows that in 2021, 64% of the population had these competences at a basic or advanced level. However, as in the rest of Europe, there are significant gaps between socio-demographic and socio-economic groups. In terms of age, there is a 58% disadvantage rate for the older population compared to the younger one. In terms of occupational status, there is a 49-point gap between inactive population and students, and in terms of education level, there is a 47-point gap between people without education and those with a high level of education. These variables raise concerns about which population sectors should be targeted by the measures that are implemented.

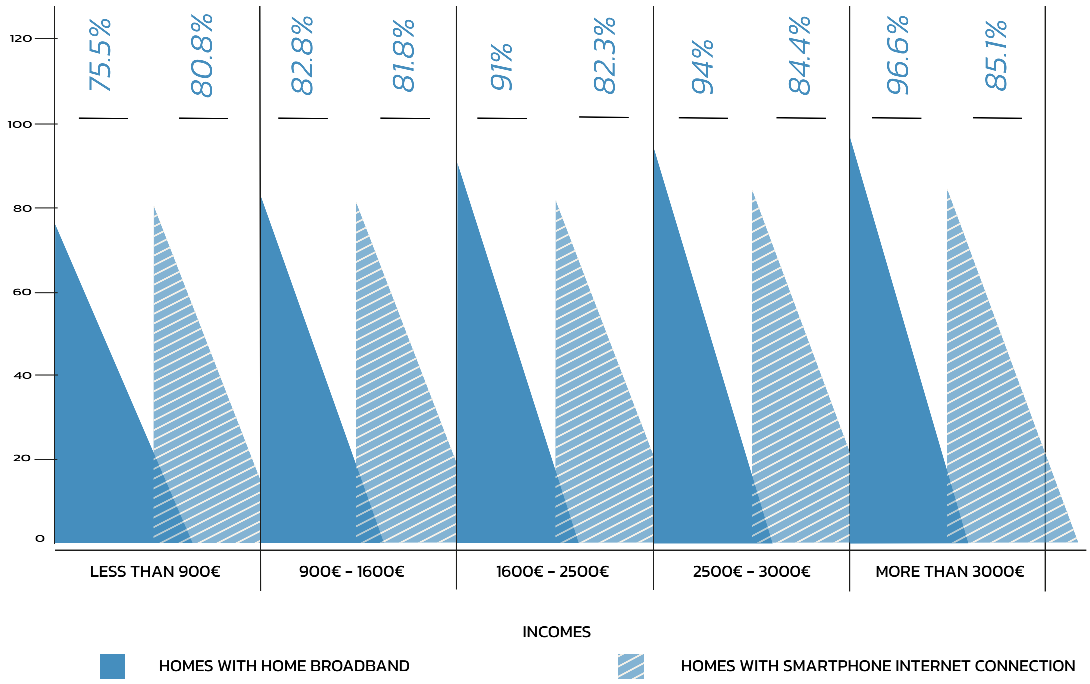
POPULATION'S SCALE ABOUT GLOBAL DIGITAL CAPABILITIES BY SOCIODEMOGRAPHIC STRATUM IN SPAIN



Moreover, population groups that accumulate several of the unfavourable indicators (living in rural areas, belonging to the elderly population, etc.) should be taken into consideration.

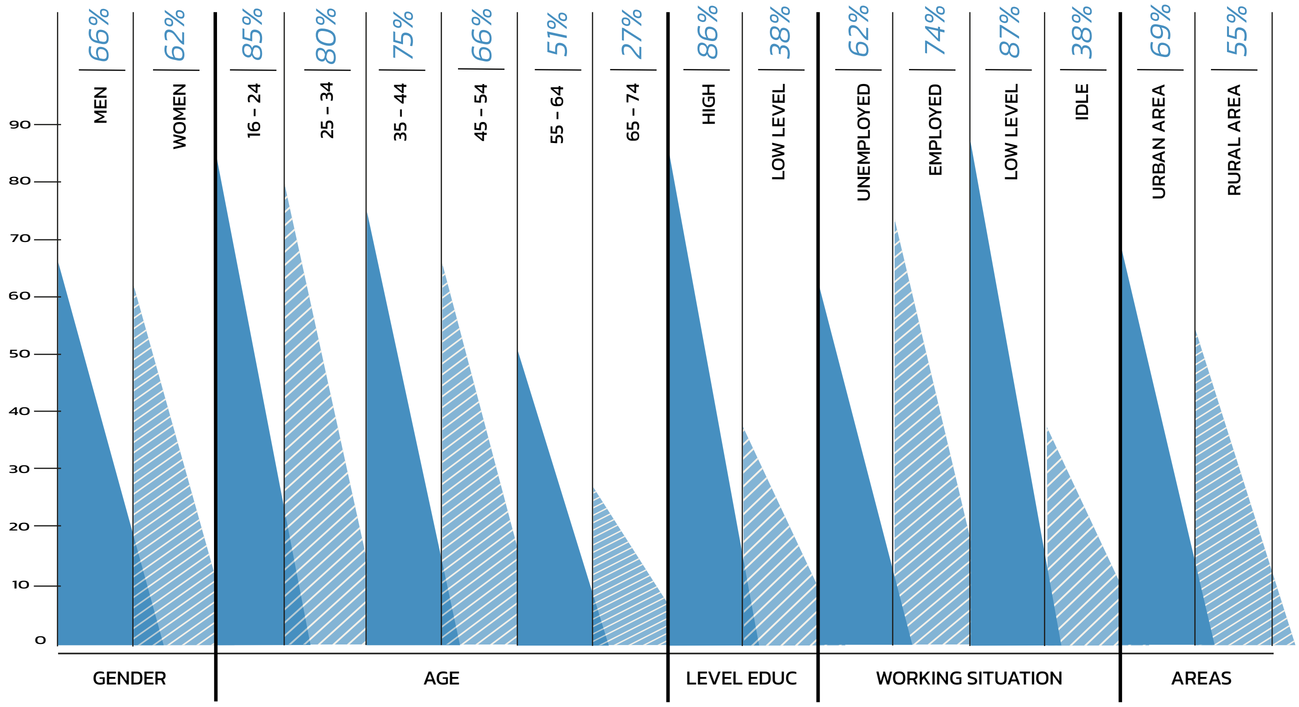
Other factors such as lack of economic resources make access even more limited. The digital divide based on income is linked to the concept of affordability, which is the ability of a citizen to pay for internet access based on their income level. The cost of internet access is a contentious issue and a frequent topic of disagreement among operators, regulators, and user associations. This report cannot comment on these conflicts, as the data provided by various statistical entities generally do not include comparisons of prices but rather adoption percentages, which is what we will focus on.

SPANISH HOMES WITH INTERNET CONNEXION'S SCALE BY INCOME.



It was expected that income would be a substantial factor in quantifying the digital divide, which proves to be confirmed by the data: The percentage of homes with incomes above 2,500 euros is almost 10 points higher than of those with incomes below 900 euros, while the percentage of households that do not have home broadband access due to economic reasons is almost 25% for those with the lowest incomes, but drops to 9% for those with higher incomes.

HOME'S SCALE ABOUT DIGITAL CONNEXIONS BY SOCIOECONOMIC STRATUM IN SPAIN



This is why impactful measures are necessary to prevent economic class, age, or regional origin from being determinants in our prospects.

When it comes to the Spanish state action regarding accessibility, we should focus on the *España Digital 2026* plan (*Spanish Digital 2026 plan). This is an ambitious project the Spanish government has developed after the COVID-19 pandemic created the necessity of* using new technologies in the personal and working spheres. It is dependent of an even wider plan of action *Plan de Recuperación*, both dependent of the Ministry of Economic Affairs and Digital transformation. This is wide plan which contemplates several sectors of action and intervention targets.

Furthermore, it is important to mention that this plan of action is strongly financed by the EU *Next Generation* funds, it complies with the 2030 agenda and has a budget of 20.000 million for all the subplans and actions. For the propose of this analysis we will just focus on the intervention directly focused on people's accessibility to the online world. Regarding the latter, we will go over the next big plans of action, which are included as part of the big 8 plans the project *España 2026* contemplates:

1. Plan de Digitalización de las Administraciones Públicas 2021 -2025. (*Digitalisation plan for Public Adminstrations 2021-2025).*

2. Estrategia de Impulso a la Tecnología 5G. *(Strategy for 5G technological advance)*

3. Plan Nacional de Competencias Digitales. (*Plan for National Digital Competences)*

4. Plan para la Conectividad y las Infraestructuras Digitales de la sociedad, la economía y los territorios. (*Plan for connectivity and Digital Infrastructure of society, economy and territories)*

These plans are tremendously wide and cover a lot of sectors of action, but we will only shed light on the ones more directly affecting people's accessibility. Furthermore, Spain's territorial administrative distribution divide the country in 17 regions each with specific plans and objectives, but we will follow on the ones mentioned above, which may overlap with regional government ones, but still are focused nation-wide.

1. Digitalisation Plan for Public Administrations 2021 -2025

This plan follows the recommendations of the European Commission report *Digital Transformation for Transport, Construction, Energy, Governments and Public Administrations,* so in that sense this approach is consistent with the European tendencies and is also backed with European funds. The objectives the plan seeks need to be pointed here for a deeper understanding of how is helping citizens access to the administration:

- Accessible, secure, reliable and efficient digital services.
- Democratization of the access to emerging technologies[1].

The action axis 1 contemplates 4 measures directly focused on access: app Factory, user experience improvement, GoTechLab (to improve and facilitate citizen access) and new digital identity (facilitation of the identification process citizens have to do before the public administration). These are the 4 citizen-focus measures out from the 17 this plan contemplates, which helps provide a better access to digital services.

2. 5G Technology Strategy

As with the latter plan, this second strategy plan is also in line with the European Commission's approach which is expressed in the *Action Plan for 5G in Europe*. The direct effects of this strategy over the accessibility concerns are not that direct, but still play a crucial role, even if more indirectly.

It is important to highlight its objectives in order to have a clear perspective of what the plan aims to achieve:

1. Support economic recovery and job creation.
2. Reinforce economic, social, and territorial cohesion, closing the social, economic or gender digital divides.
3. Provide the country with the necessary connectivity to increase its resilience in face of future crises.
4. Promote sustainable development.
5. Contribute to the transformation of the productive sectors and the transition towards a new economic, ecological, and social model.
6. Promote the consolidation of Spain as one of the leading countries in technological deployment and in R+D+I for the development of applications on new digital technologies in Europe, especially 5G.

[1] https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Plan_Digitalizacion_AAPP/Objetivos.html

The monetary provisions for this plan are 2.000 million euros, part of it is coming directly from European funds, precisely from *Europe Facility (CEF2)*. As this project does not target people directly, for the propose of the analysis we will just mention that this plan is provided with 15 specific measures tackling connection infrastructures improvements and the development of 5G technology (Ministerio de Asuntos Econonómicos, 2020, p. 9). This might not be relevant at first, but access is also related to how good and fast the online connection works. This boosts citizen online relation with the administration and helps businesses to work in a competitive and efficient way (Ministerio de Asuntos Econonómicos, 2020).

3. National Digital Skills Plan

This plan, as with the latter two, is also carried out by the Ministry of Economic Affairs and Digital Transformation. The expected budget of this project is 3.750 million euros, part of it is coming from *Next Generation* funds, *Social European Fund*, *Digital Europe* and *Digital Education Plan 2021-2027*. This plan objectives are also worth commenting as they give a clear picture of the aim of the administration in this matter is (Ministerio de Asuntos Econonómicos, 2020a):

- **Goal 1:** guarantee digital inclusion, leave no one behind in the process of digitization and progress in the development of basic citizenship skills.
- **Goal 2:** reduce the digital gender divide, increasing the number of ICT female specialists.
- **Goal 3:** ensure the digitization of education and the acquisition of skills for the education of teachers and students at all levels of the educational system.
- **Goal 4**: guarantee the acquisition of advanced digital skills both to the employed and unemployed, to improve their employability conditions. For instance, for the employed and busy, so that they learn to adapt to the continuous new demands of their working life, with emphasis on the groups most affected by the digitization and robotization of tasks.

These four latter parts, belong to the axis and line of action structure, but this plan also contemplates other specific strategies regarding advanced skills for employed population and education sector.

Just to mention some of them we can point out the following:

- *Plan de choque por el empleo joven 2019-2021* (*Youth employability shock plan 2019-2021):*

  https://www.sepe.es/HomeSepe/dam/SiteSepe/contenidos/personas/encontrar_empleo/pdf/Plan-de-Choque-Empleo-Joven-2019-2021.pdf

- *Plan de modernización de la Formación Profesional* (*Modernisation plan for professional education)*

  https://www.todofp.es/dam/jcr:5d43ab06-7cdf-4db6-a95c-b97b4a0e1b74/220720-plan-modernizacion-fp.pdf

- *Digitalízate +* (*Digitalise yourself + plan):*

  https://digitalizateplus.fundae.es/digitalizate/1/43

- *Plan Reincorpora-T* (*Reincorporate yourself plan):*

  https://www.sepe.es/HomeSepe/dam/SiteSepe/contenidos/personas/encontrar_empleo/reincorporate/PLAN-REINCORPORA-T-PRESENTACION.pdf

- *Programas para internacionalización de la empresa ofrecidos por ICEX España Exportación e Inversiones (Incentives for internationalisation of bussinesses offered by ICEX Spain):*

  https://www.icex.es/es/todos-nuestros-servicios/visitar-mercados/agenda-de-actividades

- *Escuelas conectadas* (*Connected schools):*

  https://www.red.es/es/iniciativas/escuelas-conectadas

- *Internet segura for kids* (*Secure internet for kids):*

  https://www.incibe.es/menores

- *Iniciativas desarrolladas por el Instituto Nacional de Tecnologías Educativas y de Formación del profesorado (INTEF)* (*Incentives developed by the National Institute of Educational Technologies and training of teaching staff):*

  https://intef.es/

This plan is the most complete when it comes to accessibility and skill development. As it is mentioned in this executive report, the initiatives are broad and open to let administrations develop the measures in their own way (Ministerio de Asuntos Econonómicos, 2020b).

Finally, these previously mentioned plans we have explored, all tackle the accessibility issue in different ways, providing citizens with a wide range of skills to overcome the problems posed by the digital and online world. The cooperation of European funds and institutions combined with the Spanish national government approach, provides the project *España Digital 2026* with strong tools to reduce the digital divide.

HOW IS PROMOTED IN THE STATE A HEALTHY USE OF DIGITAL TOOLS (THAT MEANS DEALING WITH THE DIFFICULTY OF DISCONNECTING AND FINDING A GOOD ONLINE/ OFFLINE BALANCE)

The use of technology does not only imply advantages. Indeed, in practice, the emergence of diseases triggered by unconscious and improper use of these technologies is becoming more and more frequent. This is a latent problem that undoubtedly represents one of the great challenges facing all countries today, given its difficult solution and its enormous extent. In what follows we will try to analyze the means followed by France, Spain, Belgium and Estonia to avoid this problem and promote a healthy use of new technologies, as well as to cure and face it.

Starting with **France**, in 2016, France regulated the right to disconnect from the workplace, imposing the obligation on companies to have a negotiated agreement with their employees to define response timetables for messages, calls, or emails outside of working hours. Several laws have also been enacted to combat the spread of false or defamatory information. Examples of these include the Law on Combating Information Manipulation (Law nº 2018-1202), enacted on December 22, 2018, which enables judges to remove fake news during electoral periods and the Avia Law/ Law on Combating Hate Speech on the Internet (Law nº 2020-766), passed on June 24, 2020 but partially vetoed by the French Constitutional Council, which compels to remove hate speech, such as homophobic, racist, and paedophilia-related content, with millionaire fines and also enhances the effectiveness of user reporting mechanisms. In other sphere, the Advertising Regulation Authority (ARPP) is a public French institution which can assess consumer complaints regarding advertising. It ensures the ethics of advertisements and advertising campaigns and has been continuously updated in order to be able of controlling online publicity.

As part of the France Relance Plan, driven by the Ministry of Economy, Finance, and Industrial and Digital Sovereignty, French citizenship is being helped to adapt to the new digital reality through three different approaches aimed at specific groups. Firstly, a digital hybridization plan for secondary education in France was implemented in 2022. Students are being taught into a safe use of the Internet and on how to take advantage of the new digital tools. Secondly, the France Connect infrastructure has been in development in order to provide public organizations with trained professionals that help to implement the digitalization of daily procedures. Lastly, since 2022, 4,000 digital advisors have been deployed to teach the population most affected by the digital gap through centres and associations, helping them develop skills such as protecting against scams, verifying online information, managing and securing personal data, and becoming informed about addictive digital practices.

In **Spain**, the need to provide a solution to all the problems that, from a medical point of view, can be generated by technological development, fundamentally in the most vulnerable people, has not been overlooked. In fact, last year, 2022, the General Secretariat for Digital Health, Information and Innovation for the SNS, which is part of the Ministry of Health, published the digital health strategy, the implementation of which seeks to provide a response to all these problems. In fact, such is the importance given to it that it has been included as an essential part of Article 43 of the Spanish Constitution, which recognizes the right of all persons to health protection, including in the digital sphere.

In any case, from a normative point of view, the Law 16/2003 on the cohesion and quality of the SNS and Law 33/2011, on General Public Health, are key, together with article 43 of the EC to which we have already referred. This strategy also pursues an aspect that is key to its effectiveness, since it not only focuses on increasing the autonomy and decision-making capacity of patients, but also goes further by seeking the development of SNS professionals to be able to cover all these cases and deal with their enormous and evident complexities.

Without wishing to undertake an exhaustive analysis of the digital health plan developed and implemented by the Spanish National Health System (which can be obtained from the document published by the Ministry), the fundamental objective of the SNS Digital Health Strategy (ESD-SNS) is “to contribute to maintaining the Spanish population in good health and to strengthen the SNS through the transformation capacity of digital technologies aimed at people, health professionals, health service provider organisations and other related agents” in order to obtain the greatest possible benefit from digital technologies, increasing coordination between the functions that make up the comprehensive framework of health protection: promotion, prevention, care and rehabilitation, in addition to including aspects of teaching and research.

In this sense, it is clear about the need to promote the performance of the public health system by means of instruments that support the work of professionals and the generation of value processes together with the costs and the opinion and preference of patients, which makes it a realistic and easily implementable strategy that values the economic requirements that its implementation entails. In addition, it also aims to improve decision making in the NHS, providing it with interoperable and quality information, and a Data Space that allows its secondary use for the generation of scientific knowledge and for the evaluation of services, and adapting the progress of the healthcare system to the demands of today’s society, through innovation policies oriented towards 5P healthcare (Population, Preventive, Predictive, Personalized and Participative), foreseeing that in any case, the incorporation of digital technologies into the NHS must catalyze its transformation towards this new paradigm and translate into new and better services in line with the needs of the population, more adapted to each person, with greater autonomy and decision-making capacity for patients and compatible with the sustainability of the system.

By way of summary, its strategic lines of action include:

1. Development of Digital Public Services in the healthcare sector.

2. Promote the interoperability of health information, at national and international level, at the service of both health surveillance and health interventions of any kind, facilitating decision-making by health authorities, managers and professionals.

3. Extension and reinforcement of data analytics and exploitation of information for the “business intelligence” of the NHS.

It seems clear, therefore, that Spain has maintained a tendency to integrate the use of both preventive and curative mechanisms to deal with the problems arising from the extension of technologies from the public resources and organizations themselves. However, from a personal point of view, we consider that this country still has a long way to go in this area, since it seems clear that although the strategy developed can contribute to a good degree to the solution of the negative effects of the misuse of technology and the implementation of these in the medical field, nothing is foreseen from the point of view of prevention, which is undoubtedly the most important pillar in the interest of uprooting the problem.

Regarding **Belgium**, the Belgian government collaborates with associations and private entities to promote the Digit-All Plan. This program aims to transform society and economy in Belgium, making them more resilient to digital change. Among its initiatives, we see the establishment of a volunteer network called "123Digit" to assist and teach those individuals who are vulnerable to the digital transition, guiding them in the use of new devices. The plan also proposes activities to promote digital skills among young children.

Additionally, in Belgium, the right to disconnect has also been regulated as a requirement for companies of a certain size to negotiate an agreement with their employees that establishes the extra work hours during which workers must be accessible for company communications. (*Loi portant des dispositions diverses relatives au travail* October 3rd, 2022, Art. 16).

Lastly, on September 5, 2018, Belgium introduced the Law on the Protection of Individuals with regard to the Processing of Personal Data. This law aligns the GDPR with Belgian national legislation and provides enhanced privacy protection for citizens. In relation to the protection of public security in cyberspace, Belgium has various organizations responsible for supervising and enforcing compliance with laws that prevent cyberbullying in different areas. Entities such as the Institute for Equality of Women and Men (Institut pour L'Égalité des Femmes et des Hommes) or the State Security Service (Sûreté de l'État) participate in and monitor cases of cyberbullying according to their nature.

With regard to **Estonia**, the country is once again surprising for its progress, ranking among the top countries with policies specifically designed to promote the healthy use of technologies. And as we have analyzed in one of the previous sections that the implementation of technology by the Estonian government is carried out from the early stages of school, this is an extremely relevant fact also in relation to the issue that concerns us now, since it seems clear that the fact that the use of technologies is included as a basic part of education implies that citizens learn to make good use of them from the earliest ages. In fact, this is an issue that is included and contemplated in the Estonian digital agenda 2030, which is committed to the development of plans aimed at the development of society focusing on an extensive and substantial digital transformation strategy, in order to achieve a sustainable and healthy development for users, providing solutions to all the problems that may arise, including health problems. We refer to section 5.f for more information on the measures adopted by this country.

WHAT KIND OF PUBLIC FREE RESOURCES ARE AVAILABLE FOR PEOPLE LEARNING NEW DIGITAL SKILLS AS WELL AS THEIR RIGHTS.

Digital media proliferation and globalized interconnectedness have transformed life in all its aspects. Having digital skills has thus become an imperative need to be able to integrate into this new digital society and take advantage of the many benefits it conceals, without falling into its dangers. Therefore, we now aim to analyze the main tools that, for this purpose, public administrations of the four different countries in question have made available for their citizens to learn new digital skills as well as their rights. It is worth mentioning that, in most cases, these tools also serve for digital education related training, hence, part of those have been analyzed before.

Spain

Starting with Spain, the most important public initiative in our country was born in mid-2019, when the Public Employment Service (SEPE), the Foundation for Employment Training (Fundae) and major technology companies - namely Amazon, Cisco, Cloudera, everis, Accenture Foundation, Telefónica Foundation, Google, Huawei, IBM, LPI-Linux Professional Institute, Oracle and SAP - jointly promoted the creation of a package of training resources in digital skills, free of access, online and free of charge. This initiative responds to the need to promote and train workers in this area to improve their efficiency, work and employability. Thus, a large number of courses are offered, all of them free of charge, as mentioned above, in different languages, with varying difficulty levels and durations, subjects of essential importance (cybersecurity, internet of things, digital marketing, etc.) so that all employees, unemployed, self-employed and Small and Medium Enterprises (SMEs) adapt their activity and skills to the demands of the rapid technological transformation in order to contribute to the development of a new production model; a need that has become even more accentuated after the COVID-19 experience.

Certainly, given the impact that new technologies are expected to have on the labour world, contributing with initiatives of this nature for the development of a new work model must be one of the main objectives of any government, which must ensure progressive adaptation of companies, workers and the unemployed to the new and growing professional digital skills, as the Spanish Ministry of Labour and Social Economy has pointed out, a total of 3.2 million jobs linked to digitalisation are expected to emerge before 2030.

As far as Spain is concerned, we must not forget the important role played in this regard by the Spanish Data Protection Agency, which has articulated its own web portal that allows citizens to obtain information quickly and easily about the digital world, in particular their rights and duties, as well as the submission of complaints and claims through instruments such as the priority channel, that facilitate the fight against cybercrime and promotes digital awareness and inclusion of all citizens.

France

In September 2017, the Mouvement des Entreprises de France (MEDEF) launched the so-called “French Coalition for Digital Skills and Jobs”, whose main objective is to achieve digital literacy in the French population, as well as to promote the development of new digital skills that are essential for integration into the world of work. The MEDEF also seeks to encourage the development of policies that aim at digital skills training for all, mainly through new approaches in education that prepare citizens for new forms of employment from the outset.

Equally important in this country is the so-called Plan national pour un numérique inclusif (National Plan for an Inclusive Digital Economy) promoted by the French Secretary of State for Digital Affairs and the French National Agency for Territorial Cohesion (ANCT) one year after the previous one, September 2018, in the framework of the 2030 objectives proposed by the European Commission’s Digital Decade, which, as we know, aims to achieve the development of digital skills by at least 80% of European citizens during the current decade. The objective, in this case, is to provide secure support for companies in the process of digital transformation, as well as the development of a secure digital society for all citizens that does not lose sight of the essential needs of human beings, with a very large amount of funding that exceeds 55 million euros in total between state, European, local and private contributions.

The French National Plan rests on the four basic pillars proposed by the European Coalition for Digital Skills and Jobs: digital skills for citizens, for the working population, in education and advanced skills for professionals in the information and communication technologies (ICT) sector. From there, the initiatives that have been developed aim to support all citizens in their participation in the digital society, in particular those social groups that, due to special circumstances, have been left out of the transformation process, in order to promote the use of digital technology for all. It also seeks to improve existing digital infrastructures and, fundamentally, the current vocational education and training (VET) systems in order to direct them towards the development of the digital skills that will dominate the labour market in the not so distant future.

Other initiatives to be highlighted include the promotion of the PIX online public service, which was previously mentioned, which offers a tool for self-assessment of one’s own digital competence, as well as the use of digital passes and credentials in the country; the promotion of digital resilience, particularly among civil servants and professionals in the care sector; and, finally, coordination between the different territorial entities and the population. The aim is to achieve digital inclusion for at least one third of the French population in the next 10 years.

Belgium

Belgium, in third place, has followed very similar steps to the two countries mentioned above. In November 2021, the Belgian National Coalition for Digital Skills and Jobs - made up of several federal and regional government departments, the professional federations Agoria, VBO and Federgon, the training institutions Syntra and Technifutur, and technology companies such as UQALIFY and Nalantis - launched a platform called "Digiskills Belgium", which brings together a multiplicity of initiatives and training opportunities to bring digital skills to all levels of society in order to bridge the digital divide at national level. This initiative also responds to the need to match the professional skills of the population with the emerging technological demands of the world of work, in order to meet the immense opportunities offered by digitalisation. This initiative also seeks to reduce the number of jobs that have been left vacant due to the lack of these skills among the working population in order to increase the level of employment throughout this decade.

The objectives of the platform are essentially fourfold. First, to inform in a simple and unified way about the different training opportunities available to interested citizens in order to achieve an efficient and visible learning system. All the initiatives that are promoted in this sense should be reflected on this website, which will be the only one available for this purpose. Second, to support all sectors of the population seeking to qualify or update their skills and knowledge to the new, growing and changing requirements of the labour market in order to improve their employability, performance and effectiveness. Thirdly, to simplify the financial funding regime for all such projects by unifying and processing them together on a single platform. Fourth and finally, to achieve the e-inclusion of all Belgian citizens by providing digital information and best practice recommendations.

Alongside this initiative, the Belgian government has also been aware of the need for a particular initiative to ensure the inclusion of women in the digital sector. To this end, it has set up the BeDigitalTogether website for the development of a dedicated national strategy for the years 2021-2026 to improve the representation of women in sectors where women are underrepresented, such as Science, Technology, Engineering, Mathematics and Information and Communication Technologies.

Estonia

Finally, Estonia is one of the most digitally advanced societies in Europe and the world. Certainly, the e-Estonia initiative launched in the second half of the 1990s was a pioneer in the promotion of digital education, digital labour market and digital citizenship, as well as the necessary infrastructure to make this possible. Within this framework, the Look@ World Foundation was created in 2001 with governmental support, which from very early on has played an important role in making the entire Estonian population digitally literate by providing free computer training, raising digital awareness and popularising the use of the Internet and Information and Communication Technologies (ICTs) in sectors such as education, science and culture. The e-Estonia initiative has achieved an unparalleled model of a digital state based on cooperation between public administrations, the private sector, citizens, educational and academic institutions.

Along these lines, in 2015 Estonia set itself the goal of digitising all educational material in both schools and universities. It provided teachers with high quality digital training so that they could start teaching this type of knowledge in schools.

In addition, the Estonian government invested large amounts of funds in the development of school internet connections, in the purchase of devices for teachers and in support for the creation of digital teaching materials. Thus, 100% of Estonian schools have been using smart tools for the daily work of young people for years in order to facilitate teaching.

Also worthy of special attention when referring to Estonian resources is the Estonian model of e-democracy, which allows for public input in political debate, improving the transparency and efficiency of the latter's actions, for example, through the portal for citizens' initiatives to Parliament (Rahvaalgatus.ee), which has converted three out of every 15 initiatives sent by this means into law. The digital society and digital rights are undoubtedly a daily reality for the people of this small Baltic country, which has led its latest initiatives to share its model and knowledge with second countries. To this end, it has created the Education Nation for international cooperation and extension of its successful educational model.

WHAT KIND OF EXISTING METRICS MEASURE THE ENVIRONMENTAL IMPACT OF DIGITAL PRODUCTS AND SERVICES IN THE COUNTRY

The President of France introduced Law No. 2021-1485 on November 15, 2021, with the goal of minimizing the environmental impact of the digital industry within the country. This law encompasses the findings and recommendations of the research mission conducted by the Committee on Planning and Sustainable Development from December 2019 to October 2020. Its objective is to provide guidelines for individuals, professionals, and public entities involved in the digital sector, promoting the growth of an environmentally conscious and responsible industry in France (Rabouille, 2022).

This legislation was one of the first stepping stones for environmentally conscious action within the digital sector. About a year later, BEREC (Body of European Regulators for Electronic Communications) published a statement on how ICT must be mindful of the digital sector's impact on the environment. This was done in order to set a standard as other countries ventured into similar national legislation as well as to ensure that the green transition of the sector would be as ambitious and effective as possible. The March 2022 publication specified a number of measures to be carried out. These included improving the reliability of available data, encouraging transparency of digital products, promoting good digital practices and minimizing the sector's environmental footprint (BEREC, 2022).

However, it is important to remark that the aim is not solely to halt digitization or limit its ecological impact but rather to combine its development with social and economic needs. This would build novel and clear environmental requirements. The main issue lies in the fact that the digital sector already accounts for 3% to 4% of the world's greenhouse gas emissions; and while this figure is relatively low compared to other industrial sectors, its ecological impact could increase significantly if nothing is done to limit it, given the projected annual growth of digitization (2022).

Measuring the environmental impact of digital products and services can be complex, but there are several existing metrics and approaches that can help assess their environmental footprint. Some of which are the most used:

- **Carbon footprint:** This metric calculates the amount of greenhouse gas emissions, usually measured in carbon dioxide equivalent (CO2e), generated by a digital product or service. It considers factors such as energy consumption, server infrastructure, data transmission, and end-user devices (Beauvisage, 2022).

- **Energy consumption:** This metric focuses on the amount of energy required to power the digital infrastructure, including data centers, servers, and network equipment. It includes both direct energy use (e.g., electricity consumed by data centers) and indirect energy use (e.g., energy required to manufacture and operate devices) (Beauvisage, 2022).

- **Water usage:** Although digital products and services primarily consume electricity, digital products and services can indirectly contribute to water consumption through the energy generation process, their manufacturing processes or cooling requirements of data centers. Tracking water usage helps assess the overall environmental impact (Beauvisage, 2022).

- **E-waste generation:** This metric focuses on the volume of electronic waste generated by digital products and services when they become obsolete or reach the end of their life cycle. It considers factors such as device lifespan, recycling rates, and disposal practices to understand the environmental consequences of electronic waste accumulation. Proper disposal and recycling of electronic waste are crucial to minimizing environmental harm (Beauvisage, 2022).

• **Material footprint:** This metric measures the resources required for manufacturing digital devices, such as smartphones, tablets, and computers. It assesses the environmental impact of raw material extraction, processing, and manufacturing stages. In addition, assessing the efficiency of material use can provide insights into resource consumption, waste generation, and potential environmental impacts (Beauvisage, 2022).

• **Life cycle assessment (LCA):** LCA is a comprehensive approach that evaluates the environmental impact of a digital product or service throughout its entire life cycle, including raw material extraction, manufacturing, distribution, usage, and end-of-life disposal. It considers multiple environmental indicators, including energy consumption, emissions, and resource depletion (Beauvisage, 2022).

• **Product Lifetime:** The lifespan of digital products, such as smartphones, laptops, and servers, affects their overall environmental impact. Longer-lasting devices reduce the need for frequent replacements and associated resource consumption. To counter planned obsolescence and promote longer product lifetimes, initiatives such as product durability standards, repairability requirements, and consumer awareness campaigns have emerged, preventing the product lifecycle from falling below minimum efficiency standards. Governments and organizations have been advocating for policies and regulations that discourage premature obsolescence and encourage sustainable product design, repairability, and recycling (Beauvisage, 2022).

• **Renewable energy usage:** Tracking the percentage of renewable energy sources powering the digital infrastructure provides insights into the environmental friendliness of the sector. It encourages the transition to cleaner energy sources and reduces reliance on fossil fuels (Beauvisage, 2022).

These metrics help assess and compare the environmental impact of digital products and services in a country. For instance, some of them are explored in the '*Pour un numérique soutenable'*, report made by Autorité de Régulation des Communications Électroniques et des Postes (ARCEP), which is the French regulatory authority for electronic communications and postal services. They facilitate decision-making processes for individuals, businesses, and policymakers, enabling the adoption of more sustainable practices and technologies (Beauvisage, 2022).

FOURTH SECTION

WHAT IS MISSING? PUBLIC SURVEY QUESTIONS TO BETTER UNDERSTAND THE NEEDS OF EU CITIZENS

1 - Relationship between digital identity and digital rights

2 - The impact of digital identity on European citizens' digital rights

3 - Challenges and opportunities for ensuring digital rights in the context of digital identity

4 - Types of digital identity

5 - Analysis of the development of digital identity in the European context

A pragmatic review of measures for the development of digital identity in Europe

Review of measures for the development of digital identity in Spain

Review of measures for the development of digital identity in Estonia

Review of measures for the development of digital identity in Belgium

Review of measures for the development of digital identity in France

Analysis and evaluation of best practices

Conclusions

MEASURES FOR THE DEVELOPMENT OF OUR DIGITAL RIGHTS (ELECTRONIC ID)

Digital identity and digital rights are closely linked. Digital identity is essential for citizens to be able to exercise their digital rights and reap the benefits of digital technologies, such as access to online services, participation in the digital society and protection of their privacy and personal data. However, there may also be risks to digital rights associated with digital identity, such as misuse of personal data, risk of discrimination and lack of control over one's digital identity. It is therefore important to understand the relationship between digital identity and digital rights and how these rights can be secured in the context of digital identity.

RELATIONSHIP BETWEEN DIGITAL IDENTITY AND DIGITAL RIGHTS

Digital identity is a key element for the exercise of European citizens' digital rights. Digital identity is necessary to access online services, to carry out transactions and to participate in the digital society. For example, digital identity is used to access public services online, such as filing tax returns, accessing healthcare and education online. It is also used to access private online services, such as e-commerce and social networking.

However, the use of digital identity can also pose risks to digital rights. Misuse of personal data, lack of privacy and discrimination are risks associated with digital identity. It is therefore important to ensure that citizens have control over their digital identity and that their digital rights are respected in the context of digital identity.

THE IMPACT OF DIGITAL IDENTITY ON EUROPEAN CITIZENS' DIGITAL RIGHTS

Digital identity can have a significant impact on the digital rights of European citizens. On the one hand, it can improve access to digital services and participation in the digital society. On the other hand, it can increase the risk of discrimination, lack of privacy and misuse of personal data.

One of the biggest risks associated with digital identity is the misuse of personal data. Digital identity requires the collection and use of personal data, and the misuse of this data can have a significant impact on the privacy and security of citizens. In addition, digital identity can be used for discrimination, as information about digital identity can be used to make discriminatory decisions in the provision of services.

It is therefore important to ensure that citizens have control over their digital identity and that their digital rights are respected in the context of digital identity. This may include measures to ensure privacy and security of personal data, transparent and non-discriminatory access to digital services and protection against misuse of personal data and discrimination.

CHALLENGES AND OPPORTUNITIES FOR ENSURING DIGITAL RIGHTS IN THE CONTEXT OF DIGITAL IDENTITY

Digital identity poses several challenges and opportunities for securing the digital rights of European citizens. One of the main challenges is to ensure the privacy and security of personal data in the context of digital identity. It is necessary to implement technical and legal measures to ensure that citizens have control over their personal data and that their rights regarding the processing and use of this data are respected. In addition, it is important to establish security protocols that prevent the breach of citizens' digital identity.

Another important challenge is to ensure accessibility and equity in the use of digital identity. Digital identity should not be a tool exclusive to certain groups or sectors of the population, but should be available to all citizens. There must be a guarantee that all citizens can obtain their digital identity easily and securely.

On the other hand, digital identity can also be an opportunity to secure citizens' digital rights. A secure and trusted digital identity can ensure access to digital services and reduce the digital divide, allowing citizens to enjoy the benefits of the digital age. In addition, digital identity can be used for identity verification in online transactions, which can improve security and reduce fraud.

TYPES OF DIGITAL IDENTITY

There are different types of digital identities, depending on the domain in which they are used and the data associated with them. Some of the most common types of digital identity are:

- **Government digital identity:** this is the digital identity issued by the government to its citizens, such as the electronic ID in Spain or the eID in Belgium.
- **Corporate digital identity:** this is the digital identity that a company grants to its employees to access certain resources or services.
- **Social digital identity:** is the digital identity that is created in social networks or online communities.
- **Financial digital identity:** this is the digital identity associated with online financial transactions, such as shopping in online shops or online banking.

Also, based on the eIDAS regulation, we can classify identity as follows:

1. **Low:** This level refers to basic verification of the user's identity, such as name and date of birth, and is mainly used for low-risk online services.
2. **Substantial:** This level requires more rigorous verification of the user's identity, using additional information such as an identity document or credit card, and is used for online services that require a higher level of security, such as online banking.
3. **High:** This level involves the most rigorous verification of the user's identity, with additional security measures such as biometrics and multi-factor authentication. It is used for critical online services, such as e-signing legal contracts and filing tax returns.

On the other hand, the same regulation describes three types of digital identity representation through the use of electronic signatures, classifying them as follows:

1. **Simple electronic signature:** this is the most basic type of electronic signature and can be created by anyone. It does not provide any guarantee of authenticity or integrity of the signed data and is therefore not suitable for high-risk or critical transactions.
2. **Advanced electronic signature:** this type of electronic signature uses an identity authentication method that ensures that the signatory is who he/she claims to be. In addition, it is uniquely linked to the signatory and the signed data, which guarantees the integrity of the data. Advanced electronic signatures are suitable for important and critical transactions.
3. **Qualified electronic signature:** this is the most secure type of electronic signature and offers the highest level of guarantees. A qualified e-signature must be created using a secure electronic signature creation device and is based on a qualified certificate issued by an accredited trust service provider. Qualified e-signatures are suitable for very critical transactions, such as the signing of large contracts or the filing of tax returns.

ANALYSIS OF THE DEVELOPMENT OF DIGITAL IDENTITY IN THE EUROPEAN CONTEXT

A pragmatic review of measures for the development of digital identity in Europe

In Europe, there are several legislative measures that have been implemented or are being considered for the development of digital rights in relation to citizens' digital identity. Some of these are mentioned below:

1. **Regulation of digital identity:** The European Union has established a legal framework for digital identity through the eIDAS Regulation (Regulation (EU) No. 910/2014), which regulates the electronic identification and authentication of citizens, businesses and public administrations. In addition, the creation of a European framework for digital identity has been proposed, allowing citizens to have complete control over their personal data.
2. **Interoperable digital identity solutions:** Interoperable digital identity solutions are being developed at European level, allowing citizens to use their eID credentials across different public and private services, without having to register for each service separately. These solutions allow for greater efficiency and convenience in the use of digital services. The biggest example of this is the proposed eIDAS regulation2 which foresees the creation of a "digital identity wallet" that would allow European citizens to control their digital identity and use it in any online service in the EU. In addition, the proposal also establishes security requirements for electronic identification and authentication to ensure that personal and confidential information is protected.
3. **Personal data protection:** The protection of personal data is fundamental to the development of the citizen's digital identity. In Europe, the General Data Protection Regulation (GDPR) has been established, which sets the rules for the protection of personal data and guarantees citizens' right to privacy. Furthermore, the European data strategy foresees the review and update of the current EU data protection regulation, the General Data Protection Regulation (GDPR), to ensure that it remains adequate in today's digital environment, as one of the main objectives of the strategy is to promote the secure and responsible use of data, while fostering innovation and competitiveness.
4. **Digital skills education:** It is important for citizens to have digital skills to be able to use digital services efficiently and safely. Therefore, digital skills education programmes are being developed, ranging from teaching basic skills to training in emerging technologies.
5. **Citizen participation:** Citizen participation is essential for the development of the digital citizen identity. Citizens must be involved in the process of designing and developing digital services and in making decisions about the use of their personal data.

These measures are just some of the initiatives being taken in Europe to develop digital rights in relation to citizens' digital identity. It is important to continue working in this direction to ensure that citizens have access to efficient and secure digital services, and that they have control over their personal data.

In addition, in June 2021 the European Commission presented a proposal for a Regulation on European Digital Identity (EID) that aims to establish a common legal framework for digital identity across the EU. This proposal seeks to establish a secure, private and portable digital identity system for EU citizens, allowing them to access digital services easily and securely across the EU, using an electronic ID issued by their own Member State. The European Digital Identity Regulation is still in the approval process and is expected to enter into force soon.

Review of measures for the development of digital identity in Spain

Spain is one of the leading European countries in the development of digital identity and has extensive legislation in this area. Law 59/2003, on Electronic Signatures, establishes the legal framework for the use of electronic signatures and guarantees their functional equivalence with handwritten signatures on paper. In addition, the National Security Scheme (ENS) regulates the security measures that must be applied in the management of information in the field of public administration, with the aim of guaranteeing the confidentiality, integrity, availability, authenticity and traceability of the information and electronic services provided.

On the other hand, the National Interoperability Scheme (ENI) establishes the technical and organisational requirements to be met by public administration systems and applications to ensure interoperability and efficiency in the provision of e-services. Within the framework of the ENI, the Cl@ve platform has been developed, which allows citizens to use a unique digital ID to access public administration e-services.

The Spanish government is also working on the development of a digital identity based on Blockchain technology, through the European Blockchain Services Infrastructure (EBSI), which would allow citizens to have greater control over their personal data and guarantee their privacy and security. The use of advanced electronic signatures and electronic seals is also being promoted to guarantee the authenticity and integrity of electronic documents and services provided online.

Likewise, in February 2021, the governments of Spain and Germany reached an agreement to collaborate in the development of a European digital identity that could be used throughout the European Union. This agreement took place within the framework of the European Council of Ministers of Economy and Finance (ECOFIN) and is based on the European Commission's initiative to develop a legal and technical framework that allows European citizens to use their digital identity throughout the EU.

The objective of this agreement is to work towards the creation of a common digital identity solution that respects the fundamental rights of citizens and guarantees the privacy and security of personal data. To this end, Spain and Germany have committed to collaborate in defining the technical and security requirements needed to ensure the interoperability of existing digital identity solutions in both countries, and to work together on the development of new solutions if necessary.

In addition, the agreement between the two countries also includes collaboration on the development of a common digital infrastructure and the promotion of digital transformation in the EU, with the aim of improving competitiveness and efficiency in the digital single market.

It should be noted that this initiative is part of the European data strategy and the European Commission's objective to create a secure and sustainable single market for data. European digital identity is seen as a key element for the development of this digital single market and for improving the protection of European citizens' digital rights.

In short, Spain has solid digital identity legislation and measures in place to ensure the security, efficiency and interoperability of e-services provided by the public administration. The country is constantly evolving in this area and is working to further improve and develop its legal and technical framework for digital identity.

Specifically in Spain, there are several initiatives and regulations in relation to citizen digital identity and digital rights. Some of the most relevant initiatives are the following:

1. Ley Orgánica de Protección de datos y de Garantía de los Derechos Digitales, which was passed in March 2018 and establishes the rights and duties of citizens in the digital sphere: https://www.boe.es/eli/es/lo/2018/12/05/3/con
2. The Law on Information Society Services and Electronic Commerce (LSSICE), which establishes the obligations of information society service providers and users in the digital sphere: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
3. The DNIe (electronic National Identity Card), which is an identity document that allows for online identification and electronic signature: https://www.dnielectronico.es/
4. The Cl@ve platform, which allows citizens to identify and authenticate themselves online with different public and private bodies using a single digital identity system: https://clave.gob.es/clave_Home/clave.html.
5. The Action Plan for the Development of e-Government 2020-2025, which sets out the lines of action to improve digital public services and digital identity in Spain: https://avancedigital.mineco.gob.es/programas-avance-digital/Documents/EspanaDigital_2025_TransicionDigital.pdf
6. Law 59/2003 of 19 December 2003 on electronic signatures, repealed by Law 6/2020 of 11 November 2020, regulating certain aspects of electronic trust services: https://www.boe.es/eli/es/l/2020/11/11/6
7. National Security Scheme (ENS) developed in Royal Decree 311/2022, of 3 May, which regulates the National Security Scheme: https://www.boe.es/eli/es/rd/2022/05/03/311
8. National Interoperability Scheme (ENI) developed by Royal Decree 4/2010, of 8 January, which regulates the National Interoperability Scheme in the field of e-Government: https://www.boe.es/eli/es/rd/2010/01/08/4/con
9. Framework collaboration agreement between Spain and Germany for the technical development of decentralised digital identity solutions: https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210729_np_ecosistema.aspx / https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/210901_np_esp_ger_declaration_signed.pdf
10. Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565
11. Law 40/2015, of 1 October, on the Legal Regime of the Public Sector: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566

Review of measures for the development of digital identity in Estonia

In Estonia, citizen digital identity is a fundamental part of society and is supported by the government. The Estonian government launched the digital identity programme in 2002 and since then, it has evolved into a comprehensive digital identity system that is used to access a wide range of public and private services online.

Its advanced digital identity system is among the most advanced in the world and is known as "e-residenciy" and is a reference model for digital identity throughout Europe.

Estonian e-Residency is based on the concept of "secure identity and electronic authentication", which enables citizens and businesses to conduct online transactions securely and conveniently. Digital identity in Estonia is regulated by the Digital Identity Act, which sets out the requirements for the creation and use of digital identity, as well as the rights and responsibilities of users.

Among the digital identity development measures in Estonia is the implementation of the digital identity card, which is issued to all Estonian citizens and permanent residents. This digital identity card is a personal identification document that also serves as an electronic signature and a means of online authentication. The Estonian digital identity system is based on an electronic identity card containing a digital signature and a cryptographic chip that stores personal data.

Another important measure is the government's online service portal, known as "e-Estonia". This portal provides access to a wide range of government services online, including business registration, tax payment and filing, and access to medical records.

In addition, Estonia has pioneered the use of Blockchain technology for the storage and protection of digital identity data. For example, Estonia's e-Residency programme uses Blockchain technology to ensure the authenticity and integrity of users' digital identity data.

Estonia has developed highly advanced legislation and development measures for digital identity, which have led to the creation of a secure, convenient and efficient digital identity system. This approach has been central to the development of digital rights in Estonia and has been recognised as a reference model for digital identity across Europe.

The Estonian government has also created initiatives to encourage the use of the digital citizen identity, allowing foreign citizens to obtain an Estonian digital identity and access the same online services as Estonian citizens, prompting companies and entrepreneurs from all over the world to take up electronic residence in Estonia because of the ease and security of online transactions with the administration necessary to carry out their business activities.

Specifically in Estonia, there are several initiatives and regulations in relation to citizens' digital identity and digital rights. Some of the most relevant initiatives are as follows:

1. Estonian Digital Identity Act: https://www.riigiteataja.ee/akt/120062022057
2. "Estonia's E-Residency Program", Estonia.eu, https://e-estonia.com/e-residents/about/.https://e-resident.gov.ee/
3. Estonian Digital Services Platform (X-Road) https://e-estonia.com/solutions/interoperability-services/x-road/
4. "Could Estonia be the first 'digital' country? ", BBC News, https://www.bbc.com/future/article/20171019-could-estonia-be-the-first-digital-country
5. eGA strategy 2025 https://ega.ee/wp-content/uploads/2015/01/eGA-strategy-2025-external.pdf
6. e-Estonia. e-Governance in practice https://ega.ee/wp-content/uploads/2022/05/e-Estonia-la-e-gobernanza-en-la-practica-compressed.pdf

Review of measures for the development of digital identity in Belgium

In Belgium, digital citizen identity is a topic of interest for both government and citizens. The Belgian electronic identity card is a document that meets the requirements of electronic identification and is used to access government and private sector online services.

The Belgian electronic identity card contains the holder's personal information, such as name, address and date of birth, as well as a digital signature and a photograph. It is used to authenticate the holder's identity when accessing online services, such as tax declarations, social security services and online voting.

In addition, the Belgian government has established a legal framework for digital citizen identity, as an EU member country, by legally recognising electronic signatures since 2000, with the Laws of 20 October 2000 and 9 July 2001, established after the adoption of the EU Directive in 1999. This EU Directive was replaced by EU Regulation No. 910/2014 in 2014, eIDAS.

Privately, there is an initiative driven by the major Belgian banks through the itsme e-platform, which allows secure online identity verification and authentication.

In terms of initiatives to promote the use of digital citizen identity, the Belgian government has established training and awareness programmes for citizens and the private sector on the importance and benefits of digital identity.

1. "Electronic Identity Card: https://www.agii.be/thema/vreemdelingenrecht-internationaal-privaatrecht/verblijfsdocumenten/elektronische-vreemdelingenkaarten/elektronische-eu-kaart
2. "Electronic Identification and Signature", https://www.ibz.rrn.fgov.be/fr/documents-didentite/eid/
3. "Digital Government Factsheets - Belgium", European Commission, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Belgium_2019_1.pdf
4. Electronic ID cards in Belgium: the keystone of eGovernment: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/belgium
5. Itsme: https://www.itsme-id.com/en-BE/why-itsme

Review of measures for the development of digital identity in France

In France, digital identity is regulated by various laws and regulations.

On the one hand, there is the "France Identité Numérique" initiative, which aims to provide a secure and unified digital identity for French citizens. The platform was launched in November 2020 and allows French citizens to create a secure online account that enables them to access public services online and carry out online procedures with the government.

In addition, in 2016 the law "Pour une République numérique" (For a Digital Republic) was passed, which establishes a series of rights and principles to ensure the protection of the digital rights of French citizens, including the right to access the internet, the right to privacy and personal data protection, the right to net neutrality, and the right to online transparency and accountability. Also, in combination with this, the European Union's Data Protection Act 2018 has been incorporated into French law, providing greater protection of personal data online.

Specifically, the creation of this law by the digital republic was a pioneering event in Europe in terms of citizen participation, in which the use of technology and data in French society was decided. The open participation process started in 2015 and lasted several months, during which citizens, experts and civil society organisations were able to provide their input through a digital platform called "Consultation Citoyenne" (Citizen Consultation).

The platform allowed anyone with internet access to provide input on issues such as data protection, transparency in public information, net neutrality and digital accessibility, among others. In addition, public debates and targeted online consultations were held to engage different interest groups. Citizen participation allowed for the collection of a large number of contributions and suggestions that were integrated into the drafting of the law. Among the main measures of the law are the right to personal data portability, the promotion of open source software in public administration, the protection of corruption whistleblowers and the prohibition of so-called "digital commons" (such as internet access) from being private and commercialised.

On the other hand, the French e-identity system, called FranceConnect, was also launched in 2016 and allows citizens to use a single account to access multiple government online services, such as tax declarations, subsidy applications and medical records. In addition, the system is designed to meet the highest security and privacy standards, with two-step authentication and protection of the user's personal data.

France is also developing the sovereign identity project "Mon Compte Formation", which seeks to give citizens full control over their personal training data and certifications. This would allow citizens to share their certifications securely with employers and other organisations.

The following links provide access to the various sections that the French government has dedicated to the initiatives described above.

1. Law "Pour une République numérique": https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033202746/
2. Public consultation on the French digital republic: https://www.republique-numerique.fr/project/projet-de-loi-numerique/consultation/consultation
3. "FranceConnect, Agence Nationale des Titres Sécurisés: https://www.franceconnect.gouv.fr/
4. Mon Compte Formation", Ministère du Travail, de l'Emploi et de l'Insertion, https://www.moncompteformation.gouv.fr/

Analysis and evaluation of best practices

The promotion and protection of digital identity and digital rights in Europe has become a key issue for the European Commission and many Member States. Many European countries have implemented data protection laws and regulations similar to the GDPR, which has led to increased protection of European citizens' personal data.

However, there is still much to be done to ensure that European citizens have control over their own digital identity and that their digital rights are protected. Digital identity and digital rights need to be addressed as interrelated issues, and further work is needed to develop initiatives and practices that protect both.

There is a need to continue exploring new approaches to digital identity and digital rights, and to work towards finding effective solutions to ensure the privacy and security of personal data online. EU initiatives, such as the digital identity strategy, are a good start, but further work is needed to improve the protection of European citizens' digital rights. In this regard, it is important to highlight some outstanding initiatives and experiences in promoting and protecting digital identity and digital rights in Europe.

Firstly, the European initiative of the General Data Protection Act (GDPR) has been an important milestone for the protection of privacy and security of personal data online. This regulation has allowed European citizens to have greater control over their personal data, granting them new rights, such as the right to data portability and the right to be forgotten.

Another major initiative is the European Digital Identity (EID) project, which aims to create a common EU-wide digital identification system, enabling European citizens to access public and private services in a secure and efficient manner. This project also aims to ensure the privacy and security of citizens' personal data.

In addition, there are several initiatives in different European countries that have been recognised for their commitment to the promotion and protection of citizens' digital rights. For example, in Spain, the Spanish Data Protection Agency is responsible for guaranteeing the protection of the personal data of Spanish citizens and companies. Also in France is the CNIL, the National Commission for Information Technology and Liberties, which is responsible for ensuring respect for the digital rights of French citizens.

As regards the evaluation of best practices in the promotion and protection of digital identity and digital rights, there are several initiatives that have evaluated the impact of these initiatives. For example, the European Commission has conducted several evaluation reports on the implementation of the GDPR and the EID initiative. In addition, there are international organisations, such as the Electronic Frontier Foundation (EFF), which evaluate the protection of digital rights in different countries.

Furthermore, the use of Blockchain in the construction of digital identity systems can enable the creation of a safer and more efficient digital single market by ensuring interoperability and security in data exchanges. In addition, it can reduce reliance on centralised intermediaries and improve the privacy and security of personal data.

Conclusions

Digital identity is a complex concept that has evolved in parallel with the development of digital technologies. In Europe, digital identity and digital rights are closely related, and the protection of digital rights is a major challenge in the context of digital identity.

European laws and regulations seek to protect digital rights, and there are outstanding initiatives and experiences that show good practices in the promotion and protection of digital identity and digital rights in the region. However, there are still many challenges to overcome and opportunities to explore.

It is essential to work on improving the privacy and security of personal data online, and to find effective solutions to ensure the protection of European citizens' digital rights. To this end, it is necessary to continue to explore new approaches and to work together to implement effective measures to protect digital identity and digital rights.

> **DIGITAL IDENTITY AND DIGITAL RIGHTS ARE THEREFORE KEY ISSUES IN THE DIGITAL AGE IN WHICH WE LIVE, AND IT IS IMPORTANT TO ADDRESS THEM IN AN EFFECTIVE AND COLLABORATIVE WAY TO ENSURE THAT THE RIGHTS OF EUROPEAN CITIZENS ARE PROTECTED IN THE DIGITAL WORLD.**

FIFTH SECTION

GENERAL CONCLUSIONS AND BIBLIOGRAPHY

1 - Literature review

2- Data sets

3 - Use of resources

4 - European resources

5 - Bibliography

-LITERATURE REVIEW:

Barrio Andrés, M. B. A. (2021). Formation and evolution of digital rights. Carlos Antonio Agurto Gonzalés. ISBN: 978-956-392-922-5. Ediciones Olejnik.

Boto Álvarez, B. A. (2018). Personal data processing: Between French privacy protection and the single digital market. General Journal of Administrative Law, (49). https://digibuo.uniovi.es/dspace/bitstream/handle/10651/51129/Tratamiento%20de%20datos%20personales_entre%20la%20protecci%C3%B3n%20francesa%20de%20la%20vida%20privada%20y%20el%20mercado%20digital%20%C3%BAnico..pdf?sequence=2

Committee of Ministers of the Council of Europe. (2014, April 16). Guide to Human Rights for Internet Users. CM/Rec(2014)6.

European Commission. (2021, June 4). Data protection in the EU. https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

European Commission. (n.d.). Press corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163

European Commission. (2010, November 4). A comprehensive approach on personal data protection in the European Union. COM (2010) 609 final.

European Commission. (2022, January 26). European Declaration on Digital Rights and Principles for the Digital Decade. COM(2022) 28 final.

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights. BOE No. 294, 06/12/2018.

Political Constitution of the United Mexican States [Mexico], February 5, 1917. Amendment of June 11, 2013. DOF (Official Gazette of the Federation) of 06/11/13.

Ramos, F. (2014). The new data protection regulation and the European lobby battle. DPO & it law. https://www.dpoitlaw.com/el-nuevo-reglamento-de-proteccion-de-datos-y-la-batalla-europea-de-los-lobbies/

Spanish Constitutional Court. (1998, May 4). STC 94/1998. BOE No. 137, June 9, 1998.

The EU Digital Identity Strategy, published June 2021: https://ec.europa.eu/info/publications/eu-digital-identity-strategy_en

The EU proposal for Digital Identity Regulation, presented in September 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

The eIDAS Regulation (EU Regulation No. 910/2014), which establishes a framework for electronic identity and trust services for electronic transactions in the EU: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

The Verifiable Digital Identity Initiative (VIDI) of the EU, aimed at developing technical and policy solutions to ensure that citizens can control their online digital identity: https://ec.europa.eu/digital-single-market/en/news/verifiable-digital-identity-initiative-vidi

The EU's Digital Single Market Strategy, which includes measures to promote interoperability and portability of digital identity across the EU: https://ec.europa.eu/digital-single-market/en/digital-single-market-strategy

Proposal for Regulation on European Digital Identity (EID): https://ec.europa.eu/info/publications/digital-identity-proposal-regulation_en

DATA SETS:

Eurostat. (2021). Individuals' level of digital skills. Retrieved from: https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I21/default/bar?lang=en&category=isoc.isoc_sk.isoc_sku

Eurostat. (2019). Individuals' level of digital skills. Retrieved from: https://ec.europa.eu/eurostat/databrowser/view/ISOC_SK_DSKL_I__custom_2579363/default/table?lang=en

Instituto Nacional de Estadística (INE). (n.d.). Access to the internet from main dwellings by household size, habitat, household net monthly income, and type of connection. Retrieved from: https://www.ine.es/jaxi/Tabla.htm?tpx=25402&L=0

Instituto Nacional de Estadística (INE). (n.d.). Use of ICT products by people aged 16 to 74. Retrieved from: https://www.ine.es/jaxi/Tabla.htm?tpx=52217&L=0

Instituto Nacional de Estadística (INE). (n.d.). Population using the internet. Retrieved from: https://www.ine.es/ss/Satellite?L=es

-USE OF RESOURCES:

Ministry of Economic Affairs and Digital Transformation. (n.d.). Spain Digital 2025: Digital Transition. Retrieved from: https://avancedigital.mineco.gob.es/programas-avance-digital/Documents/EspanaDigital_2025_TransicionDigital.pdf

Ministry of Economic Affairs and Digital Transformation. (2022, July). Spain Digital 2026. Retrieved from: https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf

Acelera PYME. (n.d.). How to address the digital divide in Spain. Retrieved from: https://acelerapyme.gob.es/novedades/pildora/como-afrontar-la-brecha-digital-en-espana

-EUROPEAN RESOURCES:

European Commission. (n.d.). Digital Education Action Plan. Retrieved from: https://education.ec.europa.eu/es/focus-topics/digital-education/action-plan

-BIBLIOGRAPHY:

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). Official Journal of the European Union L 119, 4th of May 2016.

ARCEP. (2022). Report for a sustainable digital environment. Retrieved from https://www.arcep.fr/uploads/tx_gspublication/rapport-pour-un-numeriquesoutenable_dec2020.pdf

Beauvisage, T. (2022). Measuring Digital Technology's Environmental Footprint: The Figures and Debates. Orange. Retrieved from https://hellofuture.orange.com/en/measuring-digital-technologys-environmental-footprint-the-figures-and-debates/

BEREC. (2022). Draft BEREC Report on Sustainability: Assessing BEREC's contribution to limiting the impact of the digital sector on the environment. Retrieved from https://www.berec.europa.eu/en/document-categories/berec/reports/draft-berec-report-on-sustainability-assessing-berecs-contribution-to-limiting-the-impact-of-the-digital-sector-on-the-environment

Rabouille, F. (2022). Digital Sobriety – Using Digital Technology Sensibly: What Roles Do Companies Have to Play?. Grenoble Ecole de Management. Retrieved from https://en.grenoble-em.com/news-digital-sobriety-using-digital-technology-sensibly-what-roles-do-companies-have-play

Van Dijk, J. (2020). The digital divide. John Wiley & Sons.

Spanish Ministry of Labour and Social Economy initiative web page. Retrieved from https://www.sepe.es/HomeSepe/Personas/formacion/ofertas-formativas/oferta-formacion-estatal.html

AEPD webpage. Retrieved from https://www.aepd.es/es

European Commission - Cybersecurity. Retrieved from https://ec.europa.eu/digital-single-market/en/cybersecurity

ANSSI (France) - Official Website. Retrieved from https://www.ssi.gouv.fr/

National Cybersecurity Institute (INCIBE) (Spain) - Official Website. Retrieved from https://www.incibe.es/

Centre for Cybersecurity Belgium (CCB) - Official Website. Retrieved from https://ccb.belgium.be/

Estonian Information System Authority (RIA) - Official Website. Retrieved from https://www.ria.ee/en

Europol - European Cybercrime Centre (EC3). Retrieved from https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Retrieved from https://ccdcoe.org/

Kwan, C. (2021). Toward an inclusive digital economy for all: Perspectives from an intersectional feminist social work lens. International Social Work, 00208728211009579.

Web page beDigitalTogether. Retrieved from https://www.bedigitaltogether.be/initiatives

Web page DigiSkills Belgium. Retrieved from https://digiskillsbelgium.be/fr/

Web page e-Estonia. Retrieved from https://e-estonia.com/

Ministerio de Asuntos Económicos y Transformación Digital. (2020). 5G Technology Boost Strategy.

Gobierno de España. (2020). Spain Digital 2026.

Ministerio de Asuntos Económicos y Transformación Digital. (2021). National Plan for Digital Skills.

Ministerio de Asuntos Económicos y Transformación Digital. (2021). Digitalization Plan of Public Administrations 2021-2025.

Van Dijk, J. (2020). The digital divide. John Wiley & Sons.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 32(2), 179-194.

Kesan, J. P., & Shah, R. C. (2010). Framing the net neutrality debate. Journal of Information Policy, 1, 6-32.

Cohen, J. E. (2008). What privacy is for. Harvard University Press.

Krämer, J., & Müller, K. (2018). The European Union's General Data Protection Regulation: A law about life and death? European Journal of Information Systems, 27(2), 120-123.

European Union Agency for Fundamental Rights. (2021). The EU Charter of Fundamental Rights: 20 years on. Publications Office of the European Union.

European Data Protection Supervisor. (2019). The EDPS Strategy 2019-2024: Shaping a Safer Digital Future.

Gasser, U. (2018). Digital human rights. In Oxford Handbook of Ethics of AI (pp. 117-128). Oxford University Press.

Van der Sloot, B., & Floridi, L. (2018). The Logic of Personal Data Protection: On the (Im)possibility of Satisfying Everybody. Philosophy & Technology, 31(2), 173-192.

Dubbeldam, M. (2019). E-privacy versus the value of data. Internet Policy Review, 8(3).

Sánchez, A. M. (2019). Digital identity and privacy. Revista de derecho informático, (20), 83-112.

Greenleaf, G. W. (2017). Digital identity and privacy: Some tensions, opportunities and safeguards. Computer Law & Security Review, 33(1), 1-12.

Rosen, J. (2010). The right to be forgotten. Stanford Law Review, 63(7), 387-438.

Gómez-Jordana, L. M. (2019). Digital identity and electronic authentication: A perspective from Spanish and European law. General Journal of European Law, (50), 1-31.

Pitsillides, A. (2020). The GDPR and digital identity in the European Union: A means to achieve privacy by design. Computer Law & Security Review, 38, 105364.

Sartor, G. (2018). Legal identity for all: enabling rights and inclusion through technology. World Bank Publications.

Van der Sloot, B., & Kosta, E. (2019). Respecting privacy through digital identity architectures. Computer Law & Security Review, 35(5), 101233.

Sanz, R. M., & Fuster, G. G. (2018). The privacy risks of digital identity: towards an integrative privacy framework. European Journal of Law and Technology, 9(3).

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law Books.

Taylor, C. (2012). The Routledge Handbook of Identity Studies. Routledge.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. MIS Quarterly, 35(4), 1017-1042.

The eIDAS Regulation (Regulation (EU) No 910/2014), establishing a framework for electronic identity and trust services for electronic transactions in the EU. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

The EU's digital identity strategy, published in June 2021. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9471-2021-INIT/es/pdf

The proposed EU Regulation on digital identity, presented in September 2020. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

The EU Digital Single Market Strategy, including measures to promote interoperability and portability of digital identity across the EU. Retrieved from https://eur-lex.europa.eu/content/news/digital_market.html

Proposal for a Regulation on European Digital Identity (EID). Retrieved from https://digital-strategy.ec.europa.eu/es/policies/electronic-identification

The website of the Belgian Data Protection Authority. Retrieved from https://www.autoriteprotectiondonnees.be/

The Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data in Belgium. Retrieved from https://www.ejustice.just.fgov.be/eli/wet/2018/07/30/2018040581/justel

The General Data Protection Regulation of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

Belgium data protection law. Retrieved from http://www.ejustice.just.fgov.be/eli/wet/2017/12/03/2017031916/justel

Law on the protection of business secrets. Retrieved from http://www.ejustice.just.fgov.be/eli/loi/2018/07/30/2018031595/justel

The annual report of the Belgian Data Protection Authority in 2021. Retrieved from https://www.autoriteprotectiondonnees.be/publications/rapport-annuel-2021.pdf

Law n° 78-17 of 6 January 1978 on data processing, archives and liberties. Retrieved from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

Official website of the Commission Nationale de l'Informatique et des Libertés (CNIL). Retrieved from https://www.cnil.fr/

CNIL report on the protection of personal data in France in 2022. Retrieved from https://www.cnil.fr/sites/default/files/atoms/files/cnil-in-a-nutshell-2022.pdf

Law "Pour une République numérique". Retrieved from https://www.legifrance.gouv.fr/loda/id/JORFTEXT000033202746/_

Funded by the European Union

yourdigitalrights

JÓVENES EUROPEOS FEDERALISTAS ESPAÑA