PNC
Piano nazionale per gli investimenti complementari al PNRR
Ministero dell'Università e della Ricerca

FIT4MEDROB

D4.1.1

REPORT ON THE REGULATORY FRAMEWORKS ANALYSES #1

Piano Nazionale Complementare (PNC) – Decreto Direttoriale n. 931 del 6 giugno 2022 – Avviso per la concessione di finanziamenti destinati ad iniziative di ricerca per tecnologie e percorsi innovativi in ambito sanitario e assistenziale

Project identifier: PNC0000007

Start date: 01/12/2022

Duration: 44 months

Website: www.fit4medrob.it

Editors: Francesca Gennari, Federica Casarosa, Vanessa Battiato, Irina Carnat, Andrea Chiappetta, Georgios Christou, Emilia Giusti, Matteo Greco, Paola Merli and Camilla Signoretta, (research affiliates, PhD students and assegnisti fellows, Scuola Superiore Sant'Anna Pisa)
PIs: Giovanni Comandé , Maria Gagliardi, Elena Vivaldi (Scuola Superiore Sant'Anna Pisa)

Due date of deliverable: 31/05/2023
Actual submission date: 31/05/2023
Date of resubmission: 15/05/2024
Version: 2.0

DISSEMINATION LEVEL OF DELIVERABLE		
PU	Public, fully open, e.g. web	**X**
CO	Confidential, restricted under conditions set out in Partners Agreement	

HISTORY OF CHANGES

VERSION	SUBMISSION DATE	CHANGES
1	31/03/2023	First version
2	09/05/2024	Transferred in the new format, further clarified links in the Initiative, further English proof-reading and sent to upload in the platform

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This D4.1.1 deliverable, titled "Legal gaps and enablers of biorobotic devices and allied digital technologies" is the product of the first six months of work (M6) of Activity 4, Mission 1 of the Fit4MedRob project. Its objective is to draw up a map of the legal roadblocks and issues that arise when trying to design and to create new and sustainable biorobotic devices and allied technologies. This is perfectly coherent to the Fit4MedRob project vision: if a new generation of biorobotic devices and allied technologies needs to be developed, it is of the utmost importance to have a full overview of the legal and regulatory blocks and challenges ahead.

To do that, the A4 group worked on a three-fold methodological approach. Given that the majority of the A4 members are legal experts and researchers, the most obvious course of action was to select which EU and national legislative acts or proposals could impact the creation of new biorobotic devices. The following step was to analyse and comment them. This was the guiding principle of the top-down approach (2.1). At the same time, the A4 group took advantage of the unique opportunity to work with other researchers from the same project but from other activities (mainly Activity 1 and 2) specialised in medicine, bioengineering and other applied sciences which are functional to the development of biorobotic devices and allied technologies. This occasion was particularly important because it gave the A4 group a unique opportunity: not only was the group able to check whether it was accurate in mapping the relevant EU and Italian legal rules, but also it was able to collect insights about legislative documents that might have not been considered as important because of their more practical and operational character. Some examples of this kind of documents are the following: the update of the National Ethical Committee discipline, which is essential for carrying out clinical trials at a national level[1]. Moreover, the partners pointed out the importance of the in-progress-update of the Machinery Directive, which was included in the initial legislative documents list to analyse, but that was considered maybe less relevant in comparison with other legislative acts such as the Medical Devices Regulation (*infra*-3.4). Further, it was possible to gather this information by circulating a survey-table among the Fit4MedRob participants during the month of March 2023. The contents of this survey-table and its implication for this deliverable are detailed further in this document (*infra*-4 and Annex). Ultimately, the use of two complementary approaches (top-down and bottom-up) made it possible to exactly map the potential and actual sources of legal obstacles for doctors, engineers, and technical experts in biorobotics and allied technologies. However, the amount of relevant legislation found through both the top-down and bottom-up approach and the time constraints for the first release of this deliverable (i.e. peer-review and deadlines) made it clear that there was a choice to make between quantity and quality. The A4 group decided to focus just on some of the relevant national and EU relevant legislative acts and proposals at this moment in time. The choice was in line with the nature of living 'living' document of this deliverable that envisages other releases until the end of the project. *To clarify, in this version of the deliverable (which is already quite lengthy in terms of pages and contents) the different research formations of the A4 activity focussed on some of the EU and national legislative acts but the text already has placeholders for the other documents that need to be analysed and completed in section 3.*

This means that, while reading section 3, in this first version of the deliverable the reader will find:

- a more constitutional law-focussed sub-section on the right to health and the multilevel healthcare delivery in Italy (3.1)
- a synthetic analysis of the Medical Devices Regulation (MDR) (3.4)
- a synthetic analysis of the in vitro diagnostic medical devices regulation (IVDMR) (3.5)
- a synthetic analysis of the Free Flow of Non-Personal Data Regulation (3.6)
- a synthetic analysis of the AI act regulation proposal (3.8)
- a synthetic analysis of the Cyber Resilience act regulation proposal (3.9)
- a synthetic analysis of the NIS I Directive (3.13)
- a synthetic analysis of the NIS II Directive (3.14)
- a first analysis of EU and Italian implementing rules concerning Personal Protective Equipment (PPE) and the application of the guidelines to implement healthcare home assistance from the perspective of Italian insurance law.

The results concerning the application of the bottom-up of the methodology is in section 4 which also details the tools and the process through which it was possible to gather relevant information from the Fit4MedRob partners.

1 All the EU and Italian legislative proposals and acts will be referenced in a complete way in the respective subsections of section 3 of this deliverable.

Section 5 instead is dedicated to summary conclusions which synthetize the work done until now for this version of the deliverable.

References for each of section 3' contributions are in the Bibliography section.

Finally, the annexes show the text of the survey-table and the answers that were given by the Fit4MedRob partners during the month of March 2023.

1 INTRODUCTION

This deliverable 4.1, titled "Legal gaps and enablers of biorobotic devices and allied digital technologies", is the entry point to the tasks carried out by the Activity 4 research group within the framework of Fit4MedRob project. It features a complete and clear exposition of the core objectives of the whole activity.

For clarity's sake, it is worth reminding that Activity 4 is comprised in Mission 1 of the Fit4MedRob project. While Mission 1 covers the general themes of Clinical translation and innovation, Activity 4 more specifically deals with the Legal, Ethical and Policy acceleration aspect (LEPA) of the whole Fit4MedRob project.

A4 activity's targets constitute a smooth and logical transition from Activity 1 and 2 of the same mission 1, which were respectively focussed on a preliminary survey of patients and health-sector operators' needs. Alongside Activity 3, which primarily deals with health technology assessment procedures, Activity 4 starts from the results of the previous activities and focuses on the legal roadblocks stemming from the application of the biorobotic and allied digital technologies legal framework (see *infra*-2. Methodology). Moreover, in the second iteration of this deliverable there will also be a part concerning solutions to the mapped legal obstacles.

Activity 4 objectives were set after ascertaining that the current rules concerning sustainability and clinical evidence for biorobotics were not enough to face the challenges of the climate crisis: this unprecedented environmental crisis makes it necessary to re-think about social and economic sustainability to preserve the planet, and to integrate these new necessities with an ever-evolving state of the art of biorobotics and allied technologies. What is needed, instead, is that biorobotic devices and allied digital technologies need to be designed, developed, and deployed in a legal and policy framework that is sustainable and able to support their seamless uptake, with clear protocols and identified payers, in each of the possible scenarios. A4 aims to systematically identify and suggests new paths to solve the current roadblocks at regulatory, policy, and socio-economic levels. Moreover, it aims at connecting with the upcoming effort to set up an EU dataspace and the continuously evolving regulatory framework (e.g., Clinical Trials Regulation and Medical Device Regulation, Artificial Intelligence Act, Machinery Products Regulation, Product Liability Directive, civil liability rules etc.).

Activity 4 will disentangle the gaps and overlaps that emerge from the implementation of new provisions and their eventual combination with actual liability regimes, reimbursement approaches and financial coverage, at national and regional levels. In addressing the ethical and legal dimensions it combines top down (desk research) and bottom up (interviews, roundtables, simulations and focus groups) approaches with a continuous engagement of stakeholders by *(i)* mapping the EU, national, and regional hard and soft law regulations, and *(ii)* comparing them with the law in action in each considered context, leveraging on comparative law and policy analysis methodologies. Within this methodological backdrop the research will inevitably cover the following topics: compensation coverages, personal and non-personal data management, ethical and legal clearance, risk management from medical malpractice, medical liability, insurance, personal injury damages compensation.

This deliverable is structured as follows.

After this first introduction (1), there will be a methodology section in which there will be an explanation of the strategies adopted to gather and analyse data concerning medical devices (at large) legislation and to list down the legal obstacles experienced by the health-care service operators and biorobotics product manufacturers while trying to be compliant with the relevant policies and legislative acts (2).

Section 3 will instead involve a preliminary analysis of the first regulatory frameworks (3). As it will be shortly explained, it will be a first analysis as for time constraints it was impossible to analyse and comment all the legislative framework theoretically applicable to biorobotics devices and allied technologies. Hence, this first iteration of the deliverable focussed on the constitutional aspects of the protection of the right to health in Italy (3.1); on medical devices conformity procedures at large (3.4, 3.5); on the possibility to re-use non personal data collected by the medical devices (3.6); on the proposed conformity regime for AI algorithms (3.8) and on cybersecurity at large (3.9, 3.13, 3.14). Subsequently, section 4 concerns a detailed explanation of the application of the bottom-up analysis of the legal roadblocks starting from the partners experiences and challenges with some of the legal frameworks. To conclude, in section 5 there will be some preliminary conclusions. At the end of this deliverable, there is a bibliography dedicated section, and it is also possible to read the feedback of the partners who took part in the survey concerning their legislative obstacles and hurdles that they had to face while deploying their services to patients.

2 METHODOLOGY

The methodology applied to this deliverable is three-fold.

The A4 group firstly applied a combination of a top-down (2.1) and bottom-up (2.2.) approach to identify both the relevant legal acts or proposals and the problems of the manufactures and technical experts in this field. The first method was adopted by A4 researchers to map all the relevant legislative frameworks in theory applicable to biorobotic devices and allied technologies.

The second method was instead more interactive and involved Fit4MedRob partners inputs to focus on the most pressing and practical legal obstacles with the objective to create better legal rules. Moreover, in the last paragraph of this section it will be explained the 'living document' character of this deliverable (2.3). The fact of it being a work in progress depends on the quantity of legislative acts that are in theory applicable to sustainable biorobotic devices and allied technology at the EU level as well as to the need to keep these aspects of the project open to changes and to emerging issues and regulatory interventions/proposals. The number of legislative acts to cover was too extended to be properly studied and detailed within the first milestone of the project (M6). Hence both the list of paragraph 2.2 and the entirety of section 3 concerning the preliminary analysis of the regulatory framework is not final at this stage but it is instead a work in progress that will be completed in the upcoming iterations of this deliverable until the end of the project.

2.1 TOP-DOWN APPROACH

The first level follows a top-down approach and consists in the legislative mapping of the legal frameworks that are relevant for the Fit4medRob project. A first relevant part of the rules applicable to the matter come from the Italian constitutional, national and regional frameworks levels. The second relevant part of the rules applicable to biorobotics devices and allied technologies comes from the original EU level, which was later transposed into Italian national law or that is still at a EU legislative act proposal level but that is relevant for this specific deliverable. Here follows a list of all the identified relevant legislative frameworks. However, it must be stated that this list is complete as far as the theoretical mapping of the state of the art concerning the legislative framework applicable to biorobotics devices and allied technologies to date. In practice, it was not possible to analyse all the documents in this deliverable iteration because of the time-constraints imposed by the deadlines. The interplay between the bottom up and the top down approach is feeding of issues and regulatory frameworks to be integrated.

- The constitutional basis and the interplay with the Italian multilevel healthcare system
- 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 (General Data Protection Regulation, GDPR)
- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Medical Devices Directive, MDR)
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (IVMDR)
- Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 final (AI act proposal)
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL On horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 COM(2022) 454 final (Cyber-resilience act proposal)

- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Health Data Space COM(2022) 197 final (EHDS proposal)
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS I)
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS II)
- Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (Machinery directive)
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products COM/2021/202 final (machinery regulation proposal)
- Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (PLD)
- Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products COM/2022/495 final (product liability directive update)
- National discipline of the Ethical Committees and its most recent updates in the wake of the implementation of the Clinical Trials Regulation EU/2014/536, L 3/2018 and Law of 26, 27 and 30 January 2023
- Italian tort rules applied to biorobotics devices and allied technology
- Italian contractual rules applied to biorobotics devices and allied technology
- Italian insurance rules applied to biorobotics devices and allied technology

2.2 BOTTOM-UP APPROACH

To have a more complete methodology, a better project governance implementation and to increase the mutual trust among the different participants, it was necessary to ask the other Fit4MedRob partners what their problems were in applying the Italian and EU legislation to their daily work and activities. In this way, Activity 4 met two objectives.

The first objective was to check whether the top-down mapping of the legal acts and proposals was comprehensive enough; the second objective was to make sure not to have missed any particular hard or soft law document that could potentially be relevant to this deliverable but that was not within the Activity 4's researchers' fields of expertise. The results of this approach were particularly interesting as the methodology applied involved the distribution of a survey-table for the Fit4MedRob partners to be filled in by 31 March 2023. The survey-table contents and results can be found in section 4 and annex of this deliverable.

2.3 THIS DELIVERABLE AS A LIVING DOCUMENT

This deliverable is a living document. The fact that this deliverable will need more iterations to be completed is also a methodology choice. In a way, it comes as a logical conclusion and evidence that the two previously employed methods, especially the top-down approach work: in fact without the survey-table (see *infra* section 4) and the collaboration of the Fit4MedRob partners Activity 4 maybe would have not focussed as much on the national discipline and update concerning the Ethical Committees. Moreover, it was considered that in the trade-off between quality and quantity the latter should prevail. Hence, the legislative acts and proposals covered in the next section actually were studied in depth and cover mostly the application of the top-down approach methodology. Given the fact that the survey-tables were lastly submitted on 31 March 2023 there was not enough time to develop all the themes that emerged from the filled-in survey-tables before sending this deliverable to peer-review. The issues that could not be included in this version of the deliverable will be included in the next iterations.

3 PRELIMINARY ANALYSIS OF THE FIRST REGULATORY FRAMEWORKS

3.1 THE RIGHT TO HEALTH AND THE MULTILEVEL HEALTHCARE DELIVERY[2]

3.1.1 Introduction

As already mentioned, Activity 4 aims to remove the obstacles that today's regulatory framework and the current division of competences between the different levels of government have fuelled.

In the following, we will try to illustrate the existing hard and soft law interventions at EU, national and regional level, highlighting for each one the most critical profiles and areas for reform.

The intention is (a) to try to ascertain whether there are suitable supranational references towards which national legislation on the subject can be oriented and (b) to analyse the problems that the competition between State and regions generates.

Indeed, resolving the legal loopholes that inhibit the full deployment of biorobotic devices requires prior awareness of the overabundance of measures that, instead of unravelling existing knots, have complicated the framework. To date, operators in the sector find themselves struggling with regulations that are too often obscure and with an excessively articulated division of competences.

Yet the demand for digital and robotic technologies has reached very high peaks in recent years, and pragmatic responses are now expected from legislation more than ever, also aimed at clarifying the margins of intervention of each institutional actor.

After all, as highlighted by the literature, the Covid-19 pandemic has led to an intensification of the use of new technologies in the health protection sector, due to the need to provide continuity of care. This has also required an adjustment of the organizational and interaction methods between public entities and private providers of services, to *guarantee the paradigm of personalization of care, an element acquired in the national health and social-health system at least from the early years of 2000.*

The broadening of the concept of health, which finds a fundamental foothold in the WHO definition as a "condition of complete physical, mental and social well-being and not exclusively the absence of disease or infirmity"[3] has slowly led to the affirmation, even from one normative point of view and not only from clinical practice, the idea that the satisfaction of this wide and varied right passes through the elaboration of a personalized response to the need expressed by the single person.

A first formal recognition in this sense, at an internal level, concerns the area of social and health care and is contained in the d.p.c.m. 14 February 2001 (Guidance and coordination act in the field of social-health services), where reference is made to the drafting of *personalized projects according to health needs* which require both health services and, at the same time, social protection actions; projects that must be drawn up on the basis of multidimensional assessments, therefore carried out by different professionals[4]. It is a typical operating method of social assistance, which also has its roots in a historic lack of standardization of interventions and services, and which through social-health integration interventions has extended to the operating methods of the protection of health strictly understood.

Personalization and continuity of care, supported by a personalized project which therefore looks at the person's health not as a one-off, but in a medium/long-term perspective, can certainly be strengthened by the development of digital and robotic technologies.

2Although the general structure and discussion is a common effort, this part was produced by Elena Vivaldi, Andrea Chiappetta, Matteo Greco.

3 Preamble to the Constitution of the World Health Organization as adopted by the International Health Conference, New York, June 19-22, 1946 (Official Records of the World Health Organization, no. 2, p. 100).

4 In the same sense see the articles 21 and 22 of the d.P.C.M. of 2017.

Let's think about the importance that assistive technologies have for persons with disabilities, the elderly, and the long-term sick. For example, in the last twenty years, in the field of disabilities, they have made a fundamental contribution: for access to information, for rehabilitation, and, in general, for the improvement of the quality of life and their ability of self-determination.

Moreover, technological development has represented a key element for questioning the disability classification model adopted by the World Health Organization in 1980. This model, called ICIDH (International classification of impairments, disabilities, and handicaps), took as a reference a notion of disability as a psychophysical impairment of the individual. The classification method adopted in 2001, and which took on the name ICF (International classification of functioning, disability, and health), still represents the point of reference for the "positive" classification of human functioning levels. The ICF therefore presents itself as an interactive model between the health condition and the environment, through which both the aspects concerning the person's health (consistently with the medical-rehabilitation model) and the aspects of social participation are placed on the same level (consistent with the social model), relating this picture to the contextual factors (environmental and personal). *Taking into account the context in which the Fit4medrob project intends to move, it should be highlighted that among the latter, in particular among the contextual factors of an environmental nature, technologies that "compensate" for disability are expressly placed.*

The change of perspective with respect to the previous system lies precisely in the fact that the ICF constitutes a classification method that proposes a common language, suitable for describing the functioning situations of all people (not just people with disabilities) in relation to different scenarios that may occur during life. According to this model, disability is the consequence or result of a relationship between health conditions, personal factors and environmental factors that represent the circumstances in which the individual lives.

The transition from the first to the second international classification has accompanied the transition from the so-called *medical model of disability to the social model*.

The medical model, characterized by an individualistic imprint, considers disability as "a lack" that leads to a deviation from the standard of functioning of a human being, a lack that must be read and addressed with medical tools and practices. It is therefore based on arguments of a utilitarian nature: medical and rehabilitative interventions aim to recover the functionality of a person. As has been effectively observed, the foundation of the measures implemented is not the protection of the rights of the people to whom they are addressed, but the objective of improving the overall well-being of the society in which they intervene. In essence, it is about transforming people with disabilities into "normals".

The affirmation of the social model highlights the importance given to the context in which the person with disability lives, and therefore enhances the importance of public policies aimed at removing the various types of barriers that prevent the full unfolding of the personality. Public policies whose objective is represented by the affirmation of the catalog of rights proposed within the UN Convention, whose method must be based on participation and whose result must tend to empower the people in favor of whom one intervenes.

The social model recognizes the importance of medical intervention and scientific progress that can improve people's lives, but this intervention is placed in a context in which disability must not remain a tragic event, a private fact that affects only the person and his family. In other words, it means recognizing the importance of other types of intervention: from education to social inclusion, from vocational training to job placement, with a view to planning and personalizing interventions.

In this overall context, the role played by biomedical and engineering sciences does not regress but must become increasingly "refined" and precise, representing one of the forms of knowledge that can contribute to eliminating any form of discrimination and enabling the person with disability to participate, in condition of equality with others, to the life of society.

The benefits linked to the implementation of the use of technologies are accompanied by a series of critical issues that need to be taken into consideration by public decision-makers and which concern the right to health, understood in its dual nature of collective interest and individual right.

Firstly, think of the risk that their use is not aimed at supporting the care relationship but at replacing it or in any case negatively affecting its quality, undermining the person's self-determination and fair access to care. On this profile, it should be noted that the care relationship and the time dedicated to it constitute a fundamental vehicle of the right to health as provided for by art. 1, paragraph 2, of law 219 of 2017 (Rules on informed consent and advance treatment provisions).

Secondly, it is appropriate to highlight the theme of equity in access to care, with respect to the dimension of the right to health as a social right, which must also be guaranteed in the case of the use of new technologies, in a context of great transformations, relevant on the demographic (aging of the population of Western countries) and epidemiological (increase in chronicity compared to acute)
Taking into consideration the exclusive legislative competences of the State, the clause of the essential levels of services concerning social rights, such as the right to health, assumes a pivotal role.
Furthermore, profiles relating to "state security" may come into play, which may assume relevance in relation to the need to guarantee the resilience of digital infrastructures.
These competences condition and limit the concurrent competence of the Regions in the field of "health protection", a matter in which the regional functions assume a decidedly significant weight with respect to the organizational implementation of the provisions at national level, with consequent territorial asymmetry which also affects the service offer.
Based on this premise, the report intends, first, to present a summary reference to the contents of the UN Convention on the rights of persons with disabilities in relation to the use of new technologies, also in connection with the issue of rehabilitation and full and effective participation of persons with disabilities in society, on an equal basis with others.
Then, the essential features of the Italian regional system will be taken into consideration, with reference to the right to health, trying to explore the possible connections and problematic profiles that link the theme of the essential levels of performance to that of robotic technologies in the field of health protection.

3.1.2 United Nations dimension: the impact of robotics technologies on the right to health and the continuity and personalization of care

At an international level there *are relevant documents which provide for and encourage the use of technologies to guarantee people's right to health and the continuity and personalization of care*.
Among these, some international Conventions, which have been ratified by Italy and which therefore enter our legal system through art. 117 paragraph 1 of the Constitution, play a leading role.

In the context in which the Fit4medrob project intends to move, the UN Convention on the Rights of Persons with Disabilities, approved by the United Nations General Assembly on 13 December 2006 and entered into force on 3 May 2008, assumes a central role.
Precisely on the assumptions referred to in the introduction, the United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) places assistive technologies as a fundamental right, as they aim to guarantee equal opportunities, mobility, health and dignity for every person.
To date it is estimated that more than a billion people in the world need at least one assistive technology, but only 10% of these have access to it for various reasons: high cost of some technologies, lack of information, actual availability of products, training insufficient professionals, shortage of TA specialists, inadequate policies or insufficient funding.

> Art. 117, paragraph 1:
> *"Legislative powers shall be vested in the State and the Regions in compliance with the Constitution and with the constraints deriving from EU legislation and international obligations".*

The UNCRPD represents the most recent conventional system on human rights adopted by the UN whose main purpose is to strengthen the protection of people with physical, sensory, mental, and intellectual disabilities.

This aim is also pursued through the establishment of the so-called Committee on the Rights of Persons with Disabilities, competent to receive and examine individual or group complaints, presented by the victims of violations of the rights recognized by the Convention by a State Party.
Precisely to remove the barriers that prevent people with disabilities from fully participating in public and social life, the Convention contemplates some new generation rights, among which a broad concept of accessibility deserves a prominent place, which also contemplates the accessibility of information technologies, communication technologies and robotic technologies.
In the Convention, in fact, there are numerous references to technologies: in the general provision relating to the obligations of the member states (art. 4); in the provisions relating to accessibility (art. 9), personal mobility (art. 20); in the provision relating to freedom of expression (art. 21); in the provision relating to qualification and rehabilitation (art. 26), as well as in that relating to participation in political life (29). Furthermore, article 19, which recognizes the right of independent living of all persons with disabilities, refers more generically to the need for them to be guaranteed access to a series of home, residential or community support services, which may include technological aids.

In all cases the general principles are essentially three:

a) the use of technology as a tool to guarantee or facilitate access to rights

b) the priority for technologies with more accessible costs

c) the importance of accessible information in relation to the technologies available, as a prerequisite for its full use.

It foresees, among the general obligations of the States listed in the art. 4, to undertake or promote the research and development of universally designed goods, services, equipment, and facilities.

Art. 26 – Habilitation and rehabilitation

1. States Parties shall take effective and appropriate measures, including through peer support, to enable persons with disabilities to attain and maintain maximum independence, full physical, mental, social and vocational ability, and full inclusion and participation in all aspects of life. To that end, States Parties shall organize, strengthen and extend comprehensive habilitation and rehabilitation services and programs, particularly in the areas of health, employment, education and social services, in such a way that these services and programs:
   a) Begin at the earliest possible stage, and are based on the **multidisciplinary assessment of individual needs and strengths**;
   b) Support participation and inclusion in the community and all aspects of society, are voluntary, and are available to persons with disabilities as close as possible to their own communities, including in rural areas.
2. States Parties shall promote the development of initial and continuing training for professionals and staff working in habilitation and rehabilitation services.
3. States Parties shall promote the **availability, knowledge and use of assistive devices and technologies, designed for persons with disabilities, as they relate to habilitation and rehabilitation**.

They should require the least possible adaptation and least cost to meet the specific needs of a person with a disability, to promote their availability and to promote universal design in the development of standards and guidelines.

The universal design strategy was born in the field of architecture and then spread to other fields, such as that of information technology, communication, and robotics, and requires **that every design activity must consider the different needs**.

According to article 2 of the Convention:

"Universal design" means the design of products, environments, programs and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design. "Universal design" shall not exclude assistive devices for groups of persons with disabilities where this is needed.

The principles that characterize universal design are:

1. equity of use (the project must be useful for people with different abilities);
2. flexibility of use (the project must accommodate a wide range of individual preferences and abilities);
3. simple and intuitive use (the use of the project must be understandable regardless of individual skills and experiences);
4. perceptible information (the project must communicate the necessary information to the user)
5. fault tolerance (The project must minimize the possibility of negative consequences resulting from accidental actions);
6. reduced physical effort (the project must be able to be used comfortably and with little effort
7. size and space suitable for use (the size and space of the project must allow for easy use beyond the posture, mobility of the body and its size).

Consequently, to the ratification, the UNCRPD constitutes a limit, both for the state and regional legislators. It follows that, according to what the Constitutional court has had the opportunity to affirm in its well-known case-law relating to the relationship between domestic law and international law, the provisions of the UNCRPD can be evoked as parameters interposed in the judgement of the constitutionality of Italian laws. So, the Italian law in contrast with the UN Convention could be declared unconstitutional for violation of the art. 117, paragraph 1.
Since the Convention's ratification, the Constitutional Court has constantly evoked the principles contained in the UNCRPD whenever the rights of persons with disabilities have come to the fore, but it has also emphasized that the Convention **has no direct effect**: achieving the goals set out in it requires the necessary intervention of Parliament.

Constitutional Court, judgement no. 2/2016:

Nonetheless, the Convention has important interpretative effects, given that secondary law (in particular, regulations and directives) must be interpreted in accordance with the provisions of the UN Convention, according to what was stated to the Court of Justice, for the first time, in the Ring case and Werge[5].
The European Union also played an active role in the UN Convention process from the very beginning, issuing a

It takes the form of "obligations of results": the contractual instruments are limited, in fact, to outlining certain objectives, reserving to the States Parties the task of concretely identifying - in relation to the specificities of the individual legal systems and the correlative and undisputed margin of regulatory discretion - the means and ways necessary to implement them.

communication as early as 2003 expressing its support for the adoption of an international Convention by the United Nations[6]. Subsequently, the EU signed the UN Convention in 2007. Ratification was completed almost three years later and the first Disability Strategy 2010-2020 was drawn up in 2010.
In the last one, the Strategy 2021-2020, the EU affirm that technologies constitute an enabler of rights and a prerequisite for the full participation of persons with disabilities on an equal basis with others.

The Commission will examine by 2023 the functioning of the internal market for assistive technologies to identify need for further action as diverse rules in the Members States on product eligibility and certification may harm the competitiveness of prices.

3.1.3 The Italian legal framework for the development of biorobotics: State and Regions in healthcare protection.

3.1.3.1 Brief overview on the Italian regionalism

Constitutional Law No. 3 of 2001 radically reshaped the framework of relations between State and Regions, leading to a significant expansion of regional legislative competences with respect to the previous regime.
The main constitutional reference is Article 117 Cost. The current version of the article includes two lists of subject-matters and a third group considered as residual, which covers all the subject-matters not listed before.

- The first list, contained in Paragraph 2, enumerates the subject-matters falling under the exclusive legislative competence of the State, namely subject-matters in which the State is entitled to state principles and detailed rules valid, uniformly, throughout the national territory.
- The second list, contained in Paragraph 3, enumerates the so-called "concurrent subject-matters": in this second group, the State may only define the fundamental principles, while the regions are entitled to adopt the substantive regulations.
- The third group, on the other hand, includes all the subject-matters not listed in the first two catalogues: here Regions have exclusive legislative competence, under the only limitation of respecting the Constitution and the constraints deriving from EU law and international obligations.

Consequently, in this new framework the general regulatory competence no longer belongs to the State but to the Regions. In addition, one should consider that the exercise of legislative power in concurrent subject-matters is not subordinated to the previous definition of the fundamental principles by the State: the regions may regulate within the limit of the fundamental principles deducible from the legislation in force.
This is a scenario in which it becomes crucial to have some juridical tools aimed at balancing competing instances, such as: national unity and local autonomy, regional differentiation and equal access to fundamental rights. In this sense, to ensure a certain degree of uniform implementation of fundamental rights, the 2001 reform attributed to the State the exclusive competence to define the basic levels of benefits concerning civil and social rights that have to be guaranteed throughout the national territory (article 117, Paragraph 2, lett. m.).
According to the Constitutional Court, this is a prerogative that allows the State to interfere in all subject-matters, even those falling under exclusive regional competence.

Finally, this kind of competences' distribution system lends to the emergence of quite a few "grey zones", due to the unavoidable uncertainty connected to the criterion of the nominal listing of subject-matter. For this reason, the Constitutional Court has always played a fundamental role in the resolution of the possible conflicts. In certain cases, when it is possible to identify an area of competence that is predominant over the others, the Court resolves the conflict by entrusting the legislative power to the level of government competent in the prevailing subject-matter.

> Constitutional Court, no. 282/2002: The Constitutional Court has specified that the basic levels of benefits concerning civil and social rights do not represent *"a matter in the strict sense, but a competence of the state legislator capable of investing all matters, with respect to which the legislature itself must be able to lay down the necessary rules to ensure the enjoyment of guaranteed services for everyone, throughout the national territory, as the essential content of these rights, without the regional law being able to limit or condition them".*

When, on the other hand, the use of this last criterion is not possible, the Court requires the application of the principle of sincere cooperation, by using cooperative decision-making mechanisms, such as the agreement in the State-Regions Conference.

3.1.3.2 The State's legislative competences

Legislative powers in the area of health protection

With the constitutional reform of 2001, "health protection" was included as a subject-matter of concurrent competence. This means that the state law is responsible for establishing the fundamental principles of the subject-matter, while the regions are responsible for the detailed regulation.

In order to provide a clearer representation of the concrete articulation of State competence in this subject-matter, it is useful to start from the distinction between the right to health regulation and the aspects relating to the organization of services required to satisfy it.

With reference to the aspects concerning **the right to health**, the Constitutional Court tends to attribute to the State's competence to regulate the fundamental principles any provision that contributes to defining the substantive characteristics of this right.

In this sense, the concept of "fundamental principles" gains a peculiar meaning, since it cannot always be assimilated to the notion of "general principles": according to the constitutional jurisprudence, in fact, all aspects of the subject-matter that cannot be differentiated on a regional basis are classifiable as "fundamental", if they involve rights whose protection must necessarily 'be given under conditions of fundamental equality throughout the national territory' (Const. Court, no. 338/2003). On the basis of these considerations, the Court admitted even extremely detailed state regulation, despite the nature of concurrent competence of "health protection" subject-matter.

The definition of the right to health, as we have seen, also includes the exclusive competence of the State to set the basic levels of benefits (called, in healthcare sector, "basic levels of care"). This is a fundamental competence since it contributes to defining how this right must be uniformly guaranteed throughout the national territory.

The indication of health services to be guaranteed under equal conditions to all citizens has the function of making equal not only the right but also the manner in which it is fulfilled.

Moving on to the **organizational dimension of the services aimed at satisfying the right to health**, the State's competence to establish the fundamental principles in this matter also covers the organizational aspects of healthcare services. On this point, the Constitutional Court has clarified that the subject-matter "health protection" also includes the organization of healthcare activities, in all those cases in which the organizational dimension is capable of impacting on citizens' health: in other words, when the organizational aspects constitute the functional and operational framework aimed at guaranteeing the quality and adequacy of the services provided (Const. Court, no. 181/06 and no. 207/10). They are all those aspects that affect the fundamental structure of the healthcare system, such as, for example, the relations between public and private operators, the coordination among the various institutional actors, and the organization of healthcare services. In this last area, however, the State's competence has always been strictly defined, otherwise the regional regulatory power would be compressed excessively, violating the constitutional provisions.

Therefore, when the request of equality is satisfied (uniform definition of the right to health and of the services considered essential to satisfy it, together with the fundamental aspects of the healthcare organization), the regulation of the other more specific profiles represents the space within which regional autonomy can move (Const. Court., no. 62/2020).

Health protection activities are many and varied. In particular, they involve a large number of public actors from all levels of government. Such a complex panorama of functions and actors calls for intensive planning activities. For this reason, multi-annual forms of planning represent one of the main instruments through which the State exercises its competence in health matters.

The main planning instrument is the **National Health Plan (NHP)**. In the NHP, the State establishes the general guidelines of the National Health Service and outlines the strategic objectives to be achieved, in agreement with the regions. According to the provisions of Legislative Decree (D.lgs) no. 502/1992, the National Health Plan is prepared by the Government on the proposal of the Minister of Health, taking into account the proposals coming from the

Regions; it is subsequently adopted by Decree of the President of the Republic after deliberation by the Council of Ministers, in agreement with the Unified Conference.
Originally, the plan was the place where basic levels of care (BLCs) should be defined. However, since 2001, the definition of BLCs has been separated from the Plan: as will be explained in more detail in the next chapter, nowadays they are defined in an autonomous decree, subject to the agreement with the Regions.
In any case, today the NHP appears to be strongly neglected (the last one expired in 2008) in favor of other moments of connection between State and regions in the management of healthcare. In recent years, in fact, other forms of coordinated planning have become increasingly important, including the Health Pact, which will be discussed in section 1.4.

Deficit Plans Return and Commissioner

Regional autonomy in the field of health protection, in particular in the management of the health services, may be limited by the public expenditure limits set by the State. This is a function that can be traced back to the subject of concurrent competence 'coordination of public finance'. The Constitutional Court has repeatedly affirmed that the state law may legitimately impose spending restrictions to the regions in order to ensure the unitary balance of general public finance, in light of national objectives, influenced by EU obligations (Const. Court, no. 52/2010). In other words, these spending limits and objectives represent fundamental principles of the subject 'coordination of public finance' and for this reason are suitable for binding regional autonomy, also in the health sector.

> Constitutional Court, no. 123/2011: *"The dispositions providing for agreements between the State and the regions to cover financial deficits are aimed at containing public health expenditure and, therefore, are expressive of a related principle of public finance coordination".*

In this perspective, the so-called **Deficit Plans return** represent one of the instruments through which the State implements its public finance coordination function.
The operational programs for the reorganization, requalification, and strengthening of the Regional Health Service (**Deficit Plans return**) are envisaged by the Law no. 311/2004 and they figured as attachments to agreements signed by the Ministers of Health and the Ministers of Economy and Finance with the single Regions. Therefore, Regions with financial deficits are subject to the Deficit Plans Return, which must contain both measures aimed at re-establishing the economic-financial balance and measures aimed at guaranteeing the correct provision of the basic levels of benefits, in compliance with the national plans and with the current dPCM setting the basic levels of care. The Deficit Plans Return shall continue according to three-year operational programs, which may be renewed until their objectives are achieved. Starting from 2007, the first Deficit Plans Return began to be signed which progressively involved ten Regions: Lazio, Abruzzo, Liguria, Campania, Molise, Sicily, Sardinia, Calabria, Piedmont and Apulia. Liguria and Sardinia completed their Deficit Plans Return at the end of the three-year period 2007-2009; Piedmont at the end of the three-year period 2013-2015. The other seven regions (Lazio, Abruzzo, Campania, Molise, Sicily, Calabria, Apulia) are still subject to their Deficit Plans Return.
Moreover, the Article 120 Cost. provide that "the Government can act for bodies of the regions […] whenever **such action is necessary to preserve legal or economic unity and in particular to guarantee the basic level of benefits relating to civil and social entitlements**". In application of this provision, in healthcare sector, state law provided the Commissioner procedure.
Commissioner procedure starts with a decision of the Council of Ministers when, during the periodic assessments of the Deficit Plans' implementation, serious branches are detected, capable of jeopardizing the protection of national economic unity and BLCs. The Commissioner adopts all the measures indicated in the plan as well as any

further regulatory, administrative, organizational and management act or measure necessary for the complete implementation of the plan. Moreover, with the Commissioner's designation, various sanctioning measures are activated, including the automatic increase of IRAP and IRPEF tax rates.
Commissioner procedures have been activated for five Regions: Lazio, Abruzzo, Campania, Calabria and Molise. To date, Abruzzo, Campania, and Lazio have ended their procedures, while Calabria and Molise remain under commissioner.

3.1.3.3 The Regions' legislative competences

3.1.3.3.1. Legislative powers in the area of health protection

The current constitutional model identifies the Regions as the main territorial hub of the national health care system.
In fact, the management of the regional health care is ensured through the allocation of regulatory, policy, planning, programming, support, monitoring and auditing powers to the regional bodies.
Regions are thus now recognized as a decisive player in the process of implementing the services to be provided in the social and health care field.
After all, the incidence of the regional dimension in the organization of the National Health System has already been sharply pointed out in the Art. 1 of Legislative Decree no. 229/1999 (so-called *Bindi Decree*) in the part that states:

*"The health protection as a fundamental right of the individual and an interest of the community is guaranteed, with respect for the dignity and freedom of the human person, through the National Health Service**, as a complex of the welfare functions and activities of the Regional Health Services and other functions and activities carried out by bodies and institutions of national importance"**.*

Then, the enhancement of the role of the Regions found the highest recognition thanks to the Constitutional Law no. 3/2001, which, by intervening in the overall structure of Title V of the Constitution, has redefined - as mentioned above - the criteria for the division of legislative powers between State and Regions.

Today, if the art.117, Paragraph 2, lett. m), of the Constitution assigns exclusively to the State the task of determining the basic levels of benefits concerning civil and social rights to be guaranteed throughout the national territory, **the art. 117, Paragraph 3 includes the subject of "health protection" among the matters subject to concurrent legislation**. So, while the State is concerned with defining the basic principles of this matter, the Regions have **the power to define the detailed legislation in the field of the health protection**.
This theoretical model of allocation of legislative powers has undergone some adjustments over the years due to the multiple judgement by which the Italian Constitutional Court has tried to clarify the boundaries of intervention of each level of government.

Constitutional Court, no. 282/2002: *"The new wording of Art. 117, third Paragraph, of Constitution compared to the former wording of Art. 117, first Paragraph, **expresses the intent of a clearer distinction between the regional competence to legislate in these matters and the state competence, which is limited to the determination of the fundamental principles of regulation**".*

It is precisely the Constitutional Court that has clarified that the matter "health protection" introduced by Constitutional Law no.3/2001 is very broad and is capable of encompassing each profile affecting the right to health. It follows that the management profiles of the regional health care, the organization of the pharmaceutical service and the appropriateness of therapeutic practices fall within the subject matter.
Thus, the Constitution allows the Regions to regulate – directly or indirectly – all aspects that aim at health protection.

Constitutional Court, no. 270/2005: *"In the new constitutional framework, characterized by the inclusion within the scope of concurrent legislation first and foremost of* ***the subject matter "health protection" there can be no doubt that as a rule all public entities operating in these subjects under the jurisdiction of the Regions are the subject of the corresponding regional legislative power*** *(which must, moreover, take place, of course, within the framework of the fundamental principles determined by the State legislator), since their provision and regulation represents one of the possible organizational options for achieving the goals chosen by the constitutionally responsible entity in the subject matter or subjects concerned".*

However, the constitutional reform has not completely marginalized the role of the State, which because of the requirements of uniformity maintains its centrality.
In fact, the constitutional jurisprudence after 2007 **has progressively enhanced the *centripetal tendencies*** by reaffirming the position of the State as the only "bearer" of the unity of the legal system.

Constitutional Court, no. 271/2008: *"The limit of exclusive State's competence over basic levels as opposed to concurrent legislative competence over health protection may be relatively mobile and depend concretely on the legislative choices".*

These tendencies of the Constitutional Court have contributed to a weak picture of the distribution of legislative competences in the field of the health care, so much so that today it cannot be clearly said how far the State can go in defining the fundamental principles of the matter.

The distinction between "fundamental principles" (remitted to State's competence) and "detailed regulations" (attributed to regional power) is not always easy to grasp, and this does not facilitate the relationships between the different sources of legislative production.

This uncertainty often leads the Constitutional court to **tolerate excessive State's interference in the name of uniform nationwide protection of the health-good** (over all, Const. court, no. 338/2003) **or the need to contain the public spending** (over all, Const. court, no. 294/2009).

> Constitutional Court, no. 338/2003: *"The boundary between permissible and impermissible therapies directly and necessarily affects the fundamental principles of the subject matter, which are remitted to state competence, since it involves rights whose protection cannot fail to be given under conditions of fundamental equality throughout the national territory"*.

The inevitable interconnection between the subject of "health protection" and multiple other matters reserved for exclusive State's competences (e.g., international prophylaxis rather than environmental protection and civil law) makes the margins of intervention even more indefinite and, as a result, the perimeter of regional attributions even more 'vulnerable'.
This prompted the Constitutional Court to develop the **prevalence criterion**, according to which when more than one subject matter intersects, legislative power rests with the body competent in the subject matter most affected by the regulation.
But the point on which the mechanism of the allocation of legislative competencies becomes most engulfed is related to the connection between the subject of health protection with that of determining the basic levels of benefits (as mentioned above, of exclusive state power). In fact, the two subjects are not separated by previously identifiable boundaries.
The State in the matter of BLCs is empowered to place comprehensive regulation, and the dividing line between the two spheres of competence is given, on a case-by-case basis, precisely by the concrete exercise of state power.
In order to prevent the full exercise of state competence in the determination of basic levels from reflecting an emptying of regional attributions in the area of health protection, the Constitutional Court has identified a tempering to guarantee the involvement of the regions: **the need to submit state determinations to the evaluations of specific liaison bodies between State and Regions by virtue of the principle of loyal cooperation**.
On these premises it must be inferred that **the implementation of robotics and domotics tools applied to the health sector passes, for the updating of the basic levels of care, from the state competencies and, for the financing and concrete application in regional health facilities, from the indefectible involvement of the Regions**.

3.1.3.3.2. Legislative powers in the area of social assistance

With the reform of the Title V of the Constitution, the subject of "social assistance" became the exclusive competence of the Regions.
The constitutional reform has deprived the State of the power of planning, reserving to it only the definition of basic levels, thus marking the beginning of a new phase for almost all Regions called upon to implement a timely legislation to reorganize the regional welfare system. This phase is characterized by increasing autonomy and independence from the central State.
Therefore, it is up to the Regions to regulate, through their own laws, the principles, the guidelines, the organization and provision, through municipalities, of the following social goods and services:

- Professional social service and social secretariat for information and counseling;
- Social emergency response service;
- Home care;
- Residential and semi-residential facilities for persons with social fragility;

- Community-based residential reception centers.

Constitutional Court, no. 296/2012: "The Constitutional court considers the system of welfare social assistance *"profoundly changed by the constitutional reform introduced by Constitutional Law No. 3 of 2001, which gave the regions residual-type legislative competence in the field of social services, as reiterated by the constant case law of this Court, which has affirmed that* ***all activities relating to the arrangement and provision of services, free and paid, or of economic benefits intended to remove and overcome situations of need and difficulty that the human person encounters in the course of his or her life****, excluding only those insured by the social security system and health system,* ***fall within the more general scope of social services attributed to the residual legislative competence of the Regions****".*

Regions are also concerned with allocating state funding to local governments and planning sector goals in so-called Social Plans.
The concrete determination of the basic levels even of social rights is up to the State, which is therefore called upon to define both the basic levels of benefits (Italian acronym: LEP) and the basic levels of social assistance (italian acronym: LIVEAS).
Therefore, the State is responsible for ensuring the maintenance of adequate uniformity of treatment in terms of the rights of all citizens, while the Regions retain wide discretion in social policy choices.

3.1.3.4 The existing coordination mechanisms.

As anticipated, the complex division of legislative powers in the field of health protection has led to an appreciation of the importance of coordination mechanisms between the different levels of government, conceived as venues better suited to achieve a political synthesis and not to compress the space for intervention of the Regions.
So, the collaborative module between the state and regions is the cornerstone of the system of health competences.
The recognition of the State's exclusive competence on the subject of basic levels of care and the involvement of the Regions in the definition of detailed regulations in the more general matter of health protection requires necessary tempering from time to time in order to avoid the paralysis of the system or the marginalization of regional entities.
In fact, as the Constitutional Court has repeatedly clarified, the competence over BLCs cannot lead the State to appropriate the regulation of profiles not strictly related to health or social services.
To avoid this danger and reconcile the reasons for the uniform exercise of services throughout the Country with the powers constitutionally assigned to the autonomies, the law-system makes use of the concertative instruments in which State and Regions are forced into dialogue in order to reach agreements.

Constitutional Court, no. 169/2017: The Court points out that while it is not in doubt that *"the determination of BLCs is an obligation of the state legislator, its projection in terms of regional needs necessarily involves the regions,* ***so the physiological dialectic between these subjects must be marked by loyal cooperation****".*

The mechanisms of state-region linkage fully respond to the logic of loyal cooperation between institutional subjects that is expressly recognized in Article 120, Paragraph 2, of the Constitution. Whenever an interest is involved that transcends that of the individual territorial entity, collaborative procedures come into play in order to be able to devise overall strategies that take on the general interest.

The most important and widely used collaborative mechanism is the State-Regions Conference, established by Law no. 400/1988.

Therefore, the Conferences system today plays a crucial role in the harmonization of legislation.

The Constitutional Court over the years has increased the specific weight of the Conferences system, entrusting it with a strategic political role in multiple administrative and regulatory proceedings.

The moments of necessary liaison between State and Regions in the social-health field are now so many that **they occupy a preponderant space in health planning, as well as in the distribution of resources**. This is because the use of agreements or opinions, implemented through the State-Regions Conference system, is necessary whenever "health legislation is at the intersection of matters attributed by the Constitution to state and regional legislative power, without any material area being identifiable that can be considered clearly prevailing over the others" (Const. Court, no. 50/2008).

Art. 12, par. 1, Law no. 400/1988: *"The Permanent Conference for Relations between the State, Regions and Autonomous Provinces of Trento and Bolzano is established at the Presidency of the Council of Ministers, with tasks of information, consultation and liaison, in relation to general policy directions likely to affect matters of regional competence, excluding general directions relating to foreign policy, defense and national security, and justice".*

Art. 12, par. 5, Law no. 400/1988: *"The Conference is consulted:*

(a) on the general lines of regulatory activity directly affecting the regions and on the determination of national economic planning objectives;

(b) on the general criteria relating to the exercise of state policy and coordination functions inherent in the relations between the state, regions, autonomous provinces and infra-regional entities;

(c) on other matters on which the President of the Council of Ministers deems it advisable to acquire the opinion of the Conference".

The most important product referred to the policy synthesis activity of the State-Regions Conference is the Health Pact. This is a three-year financial and programmatic agreement between the government and the Regions that links health spending to planning.
By entering into the Health Pact, the parties agree to commonly define service financing choices and pursue the goal of improving the quality of services or increasing the suitable of services.

Constitutional Court, no. 31/2006: The Court points out that while it is not in doubt that *"The Conferences system represents* ***one of the most qualified forums for the elaboration of rules intended to complement the parameter of loyal cooperation****".*

Regions also commit to controlling spending in every strategic area (e.g., hospital care, personnel governance, reorganization of regional networks). Only strict compliance with the measures set out in the Health Pact can enable Regions to access any increases in regional health service funding.
The incidence of the State-Regions Conference in the processes of health system development is also evidenced by the necessary agreement that it must provide on the draft decree by which the Minister of Health defines the maximum tariffs for each service included in the BLCs.
The multiple attributions recognized to the State-Regions Conference testify to how the criteria for the division of competencies between State and Regions are excessively complex and unsuitable for defining a priori the respective areas of intervention.
Inevitably, therefore, the road to full affirmation of biorobotics also passes through the Conferences system.

3.1.3.5 The role of the State and the Regions in social and healthcare investments provided by the NRRP

The Decree-Law No. 77 of 2021 is concerned with defining the governance of the NRRP and the active involvement of the Regions in the implementation of the measures and investments provided for in the Plan, through the establishment of specific technical bodies linking the Presidency of the Council of Ministers and implementing bodies.
The topic is of absolute relevance to the social and health sector since the NRRP devotes two specific Missions (5 and 6) to "Cohesion and Social Policies" and "Health."

3.1.3.5.1 Mission 5 (Cohesion and Social Policies)

Specifically, Mission 5 of the Plan (Cohesion and Social Policies) plays a very prominent role within the NRRP, aiming to ensure:

- the support for **gender equalities;**
- **combating discrimination**;
- the encrease in **youth employment**;
- the **territorial rebalancing** and **development of the South** and inland areas.

To achieve these purposes, the Mission allocates 19.85 billion euros, an amount equal to 10.34 percent of the total PNRR amount.
The mission is made explicit in three components that respond to the European Commission's Recommendations No. 2/2019 and No. 2/2020, and will be accompanied by a series of reforms that support and complement the implementation of investment:

- M5C1: Employment policies;

- M5C2: Social infrastructure, families, communities and the Third Sector;
- M5C3: Special interventions for territorial cohesion.

Component 1, with 6.66 billion euros allocated, aims to transform the labor market with tools that facilitate labor mobility, improve workers' employability and raise the level of protections through training.
Thus, interventions designed to:

- strengthen active labor market policies;
- strengthen employment centers;
- promote the creation of women's enterprises;
- promote the acquisition of additional skills by the younger generation.

A fund of 11.22 billion euros is dedicated to the **second component** of Mission 5, aimed at enhancing the social dimension of health, urban planning, as well as housing policies.
The general objectives of this component can be summarized as follows:

- strengthen the role of territorial social services and family policies, with special reference to children, the elderly and people with disabilities;
- improving protection and inclusion systems for people experiencing extreme marginalization and housing deprivation;
- Integrate national policies and investments to ensure a multi-pronged approach that addresses both the availability of more affordable public and private housing and urban and land regeneration;
- Recognize the role of sports in social inclusion and integration as a tool to counter the marginalization of local individuals and communities.

The **third component** of Mission 5 has 1.98 billion euros and is overall aimed at strengthening policies for the South and inland areas, with measures to improve the quality of education, health and social services.
The interventions attributable to this mission pursue the general objectives of:

- strengthening the National Strategy for Internal Areas;
- economic and social valorization of property confiscated from the mafias;
- strengthening tools to combat school dropout and social-educational services to minors;
- reactivation of economic development through the improvement of the service infrastructure of the SEZ Areas functional to increase the competitiveness of the companies present and the attractiveness of investments.

3.1.3.5.2 Mission 6 (Health)

Mission No. 6 assumes a crucial role in the NRRP, given the universal value of health, its nature as a fundamental public good, and the macro-economic relevance of public health services.
The Covid-19 pandemic has made certain critical aspects of a **structural nature affecting the National Health Service** (NHS) even more evident, so that this Mission **constitutes a unique opportunity to synergistically address all problematic profiles** and to align, once and for all, services with the care needs of patients in every area of the country.
The Mission aims to:

- improve the infrastructure and technological endowments available to the NHS;
- promote research and innovation;
- develop the professional-technical, digital and managerial skills of staff.

To achieve these purposes, the Mission allocates 15.63 billion euros.
More specifically, **the interventions are based on the importance of being able to rely on appropriate leveraging of state-of-the-art technologies, high digital, professional, and managerial skills, new processes for performance and care delivery**, and more effective linkage between research, data analysis, care, and its planning at the system level.
The mission is expressed in two components:

- M6C1: Neighborhood networks, facilities and telemedicine for community health care;
- M6C2: Innovation, research and digitization of the National Health Service.

Component 1, with 7 billion euros allocated, aims to pursue a new and innovative healthcare strategy that will enable the country to achieve adequate quality standards of care.
Ascribed to this area of funding are interventions designed to:

- strengthen the NHS by aligning services with the needs of communities and patients;
- strengthen outreach health facilities and services;
- develop telemedicine by overcoming the fragmentation and lack of homogeneity of health services offered throughout the country;
- develop advanced telemedicine solutions to support home care.

A fund of 8.63 billion euros is dedicated to the **second component** of Mission 6, aimed at strengthening the relationship between research, innovation and health care by updating the research policies of the Ministry of Health.
The general objectives of this component can be summarized as follows:

- developing public health **that enhances investment in the health system in terms of human, digital, structural, instrumental, and technological resources**;
- strengthen scientific research in biomedical and health fields;
- strengthen and innovate the technological and digital structure of the NHS at the Central and Regional levels to **ensure a significant evolution of health care modalities, improving the quality and timeliness of care**;

3.1.4 Biorobotic Technologies as Basic Levels of Care (BLC)

3.1.4.1 The general legal framework on Basic Levels of Care (BLCs)

The **National Health System** is the set of functions and activities, with national relevance, provided by each Regional Health System, financed by the State.

As mentioned above, the concept of "basic levels" was introduced at the constitutional level by the Constitutional Law no. 3 of 2001, in order to define an exclusive legislative competence of the State. This specific subject matter gives to the State the power (and the duty) to fix the basic levels of benefits relating to the right to health, valid throughout the national territory, specifically named **"Basic Levels of Care" (BLC**).
Pursuant to article 1 of Legislative Decree (D.lgs.) no. 502 of 1992, healthcare services that offer scientific evidence of a significant benefit for individual or collective health, in relation to the financial resources employed, may be identified as BLCs. Therefore, services, activities, and treatments that do not effectively meet the healthcare needs of patients are excluded, as well as those healthcare services that do not guarantee an efficient use of resources with respect to the manner in which they are organized and delivered, in the presence of other forms of services aimed at satisfying the same needs.
BLCs have to be provided by the **National Health System (NHS).** In particular, to ensure the uniform provision of BLCs, it is up to the State to establish how to distribute their costs between the National Health Service and patients: in some cases, the service is provided free of charge, in other cases cost-sharing thresholds (ticket) are set. This

According to the Constitutional Court, "*The measure of citizen co-participation to the costs has to be homogeneous throughout the national territory, "since it would not be acceptable for the concrete offer of a health service falling within the BLCs to be presented differently in the various regions," considering that "the concrete offer includes not only the quality and quantity of the services that must be guaranteed in the territory, but also the thresholds of access, from an economic point of view, of citizens to their use" (no. 203 of 2008). This also applies to special statute regions that bear the cost of healthcare in their respective territories since "the very nature of the so-called BLC, which reflect necessarily uniform protections of the good of health, requires that their regulatory discipline be referred to even the subjects with special autonomy" (no. 134 of 2006*)" (no. 187/2012).

State's prerogative does not allow the Regions to define their own cost-sharing schemes, applicable only throughout the relevant territory.

Financing of the BLCs is ensured through the general mechanism envisaged by D.lgs. no. 118 of 2011 on "fiscal federalism" and it is based on the criterion of "**standard costs**". A "standard cost" represents the ideal amount of money necessary to ensure a specific healthcare service provided as BLC. It is defined in relation to needs (which can also be defined as "standard") to be assessed according to specific indicators.

BLCs have to be adopted by way of a **Decree of the President of the Council of Ministers (dPCM)**[7].

The **procedures for defining and updating** the BLCs are regulated by Article 1, Paragraphs 554 and 559 of Law no. 208 of 2015 (so-called Stability Law 2016). According to this disposition, the dPCM is adopted upon proposal of **the Minister of Health** together with **the Minister of Economy and Finance**, in agreement with the "**Conference for Relations between the State, Regions and Autonomous Provinces of Trento and Bolzano**" and following consultation of the **competent parliamentary committees**, for any subsequent updates to the original dPCM. The second procedure, set out by Paragraph 559, concerns the hypotheses of an update of BLCs that do not imply further burdens for the public finance and that is limited to an amendment of the lists of services that can be provided by the NHS or the identification of measures aimed at increasing the suitability of the delivery of the same services. In this case, the final act consists in a **Decree of the Minister of Health** (instead of a Decree of the President of the Council of Ministers). Here, the State-Regions Conference only expresses an opinion on the draft Decree (whereas the first procedure requires an agreement). Even for this second procedure the opinion of the competent parliamentary commissions shall be required.

The involvement of the Conference is unavoidable for constitutional reasons. More specifically, although the power to determine the BLCs is an exclusive legislative competence of the State, the fact that this competence concerns activities inherent to the subject "protection of health" makes it necessary to involve the Regions through the mechanism of the "agreement".

The Regions, in the light of their legislative competence in the subject matter of "health protection", are responsible for the material implementation of BLCs through their Regional Health Systems (RHS). However, the identification of BLCs not only trace the boundary between what the NHS provides or not for free, or partially for free, but also between the services that all the RHSs have to offer and those that can be provided additionally and autonomously by RHSs, with their own financial resources (so called **extra-BLCs**).

This point is crucial, as it helps to better understand which is the role of the Regions in relation to BLCs. In this way, Regions could adapt the supply of healthcare services to the actual needs of their community. Moreover, the regional framework could be seen as a useful "laboratory" for the experimentation of innovative healthcare services (perhaps also on the basis of national health planning guidelines) that could be adopted as BLCs in the future.

Nevertheless, the regional legislative autonomy in defining the extra-BLCs encounters an important limit when the Region is subjected to a "**deficit Plan Return in health matters"** or when it is under the State commissioner. In these cases, the involved Region cannot guarantee extra-BLC healthcare services. Commissioning procedures have so far

Regione	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Lazio	28/02	11/07												22/07		
Abruzzo	06/03	11/09								15/09						
Liguria	06/03			10/04												
Campania	13/03		28/07											24/01		
Molise	27/03		24/7													
Sicilia	31/07															
Sardegna	31/07			31/12												
Calabria			17/12	30/07												
Piemonte				29/07							21/03					
Puglia				29/11												

In giallo sono riportate le Regione in Piano di rientro, in rosso le Regioni in Piano di rientro e commissariamento.
Le date all'interno delle celle identificano l'inizio/fine del Piano di rientro/commissariamento.

Source: Report Osservatorio GIMBE 2/2022. *Livelli essenziali di assistenza: le disuguaglianze regionali in sanità.*

7 Article 6, DL no. 407/2001.

Figure1

been activated for five regions: Lazio, Abruzzo, Campania, Calabria and Molise. To date, Abruzzo, Campania and Lazio have emerged from commissionership, while Calabria and Molise remain under commission.
BLCs were defined, for the first time, by the dPCM of 29 November 2001, which played the role of **classifier** and **nomenclator** of healthcare services. The decree had a basically recognitive character and it was limited to a generic description of what was already envisaged by regulatory acts in force at the date of its adoption.
The 2001 dPCM was integrally substituted by the **new dPCM of 12th January 2017**: it became the primary source for defining the healthcare services ensured to all citizens through the use of public resources, made available by the NHS. The new dPCM gives a picture of how the NHS is structured. In particular, it offers a division of healthcare services (falling under the BLCs) into **three macro-areas**:
(a) Collective prevention and public health;
(b) District Assistance;
(c) Hospital care.

3.1.4.2 The macro-areas defined by the dPCM of 12th January 2017 and biorobotic technologies.

As mentioned above, the types of healthcare services included in the BLCs are divided into three macro-areas:
1. **Collective prevention and public health**, which includes activities and services provided to promote public health. This area includes activities for monitoring, preventing, and controlling infectious and parasitic diseases, including vaccination programs; activities for the protection of health and safety in life environments; activities for monitoring, preventing, and protecting health and safety in workplaces; animal health and veterinary urban hygiene; food safety; activities for monitoring and preventing chronic diseases, including the promotion of healthy lifestyles and organized screening programs; nutritional monitoring and prevention; and medical-legal activities for public purposes.
2. **District assistance** which represents the second macro-area of BLCs and is structured into nine sub-areas of services: a) primary health care; b) territorial health emergency; c) pharmaceutical assistance; d) integrative assistance; e) ambulatory specialist care; f) prosthetic assistance; g) thermal assistance; h) domiciliary and territorial social and health assistance; and i) residential and semi-residential social and health care.
3. **Hospital care** which represents the third macro-area of BLCs and is divided into the following kinds of services: a) emergency room; b) ordinary acute hospitalization; c) day surgery; d) day hospital; e) rehabilitation and long-term care; f) transfusion activities; g) cell, organ and tissue transplant activities; and h) poison control centers.
Many services included in these macro-areas aim to satisfy the specific needs of the Project's target groups, namely **patients with reduced sensorimotor and/or cognitive functions requiring rehabilitation, assistance, and/or support**. Biorobotic technologies could play a fundamental role in order to provide the best response possible to their needs.
Therefore, this section aims to provide a clear representation of which kind of activities classified as BLCs are more prone to innovations in the field of biorobotic. This is a fundamental step to foster the introduction of biorobotic technologies within the services provided as BLCs.
From this prospective, the most relevant activities concern rehabilitation services and prosthetic assistance.
Rehabilitation is a process whereby a person with disability is brought to the best possible level of autonomy on a physical, functional, social, intellectual, and relational plan.
A distinction can be made between two kinds of activities: **a) rehabilitation health activities**, which include assessment, diagnostic, therapeutic and other procedures aimed at overcoming, containing or minimising disability and the functional limitations (*e.g*. moving, walking, talking, dressing, eating, communicating, working, etc.); **social rehabilitation activities** which include actions and interventions aimed at ensuring to the patient the maximum possible level of participation in social life, containing the negative effects of their disability condition.
Rehabilitation activities can be provided in the following sub-areas: ambulatory specialist care and integrative assistance, related to the macro-area "District assistance"; ordinary acute hospitalization, day surgery, day hospital and rehabilitation and long-term care, related to the macro-area "Hospital care".

In the field of **District assistance**, the NHS has to ensure the services listed in **the nomenclator provided in Annex 4** of the dPCM, which also includes many rehabilitation activities that could be delivered using new rehabilitation robots (end-effectors, rehabilitation exoskeletons, gait trainers, etc.).

Updating the nomenclature, in order to integrate rehabilitation robots within the rehabilitation services ensured by the NHS, could play a pivotal role toward a broader diffusion of such biorobotic technologies. This would be able to ensure an expansion of the protection of the right to health, in a universal perspective, therefore untied from insurance schemes, linked to employment-type welfare models.

In more detail, the nomenclator includes, for each service: the identification code, the definition, any delivery methods aimed to guarantee patient safety, any notes referring to conditions of deliverability or indications for proper prescriptions.

The manner in which these services may be provided is regulated autonomously by each Region and Autonomous Province.

The dPCM encourages and promotes the delivery of BLC services in a **domiciliary regime**. In particular, the NHS guarantees domiciliary health care services for people who are not self-sufficient or in frail conditions. The costs of this kind of service are entirely covered by the NHS for the first thirty days after the hospital discharge and 50% for the following days. The remaining 50% is covered by the Municipality, which has the right to ask the user to cover part of the quota with its resources (on an ISEE basis), according to regional and municipal regulations.

If domiciliary health assistance is not possible, the NHS guarantees patients who are unable to be treated at home the opportunity to be hosted in a residential institution that offers them all the care they need. In fact, adequate accommodation is necessary in order to guarantee domiciliary assistance; it is important to have the support of people (family members, friends or professionals) who can ensure the satisfaction of the patient's main daily needs, including aid with personal mobility. When these conditions are not met, the local health agency may approve admission to a residential institution that can guarantee adequate care (medical, nursing, rehabilitation and assistance) for all patient needs.

Domiciliary, residential, and semi-residential assistance activities also include social services. **Integrative assistance** is aimed at guaranteeing continuity between health treatment and rehabilitation activities, ensuring at the same time social care. Specific care pathways are defined to achieve this objective. The NHS guarantees uniform access to health and social services, ensuring a multidimensional needs assessment from a clinical, functional, and social point of view. The patient's therapeutic and rehabilitation needs are defined in the Individual Assistance Plan (PAI), which is drawn up by a multidimensional assessment unit. The regions and autonomous provinces ensure the uniform organization of these services with reference to procedures and the multidimensional assessment.

In all these cases, the use of biorobotic technologies could play a pivotal role in reducing the use of residential institutions and ensuring that the patient is treated at home. Additionally, providing domiciliary social and health services using biorobotic technologies could ensure better continuity in assistance. Moreover, the strengthening of domiciliary services is a fundamental objective of the National Recovery and Resilience Plan (NRRP). In this perspective, the Plan stresses that independence and autonomy of elderly/disabled persons at home could be better guaranteed through the integration of domiciliary healthcare with social interventions, by reducing the risk of inappropriate hospitalization; and this will be possible only if the opportunities offered by new technologies are fully exploited.

Furthermore, in the field of “District assistance”, specifically in the sub-area of “rehabilitation and long-term care”, the dPCM provides that the NHS guarantees a number of healthcare services that can be provided in hospital under the conditions laid down in Article 44. Among these services are also included several rehabilitations one. The identification of the proper hospitalization setting is based on the specialist doctor's assessment, who prepares the rehabilitation project and defines the objectives, methods and times for completing the treatment, activating the domiciliary, residential and semi-residential territorial services for the rehabilitation needs after the discharge.

The last relevant class of healthcare services qualified as BLCs is **prosthetic assistance**. The dPCM of 2017 states that the NHS must guarantee healthcare services that involve the provision of prostheses, orthoses, and technological aids as part of a rehabilitation-assistance plan aimed at preventing, correcting, or compensating for functional impairments or disabilities resulting from pathologies or injuries, enhancing residual abilities, and promoting the autonomy of the patient.

The nomenclature of Annex 5 contains the following kind of devices: a) prostheses and orthoses made or fitted to measure by a qualified professional, additional devices and services for the maintenance, repair, adaptation, or replacement of components of each prosthesis or orthosis; b) technological aids of continuous manufacture or mass

production that do not require fitting by a qualified health professional; c) technological aids of continuous or serial manufacture, ready for use.
Introducing new biorobotic technologies into the nomenclature of Annex 5 could be crucial in promoting their spread and development. For example, thought-controlled prostheses could be introduced to restore lost prehensile or locomotion functions of individuals with limb amputations. The 2017 dPCM's illustrative documentation shows that several innovative services have already been introduced, especially in the field of information and communication technologies, in favor of people with very great functional limitations (so-called ICT-Information Communication Technologies aids), as well as the introduction of digital technology hearing aids for the prescription of which, however, a precise hearing loss range has been indicated.
The procedure for prosthetic assistance includes the following stages: a) formulation of the individual rehabilitation plan, b) prostheses prescription, c) authorization, d) delivery, e) testing, and f) follow-up. The regions specifically regulate this procedure, avoiding unnecessary requirements for the patients or their relatives. The individual rehabilitation plan is formulated by the specialist doctor in collaboration with a multidisciplinary team based on the patient's needs. Regions may provide for the establishment of regional or company lists of prescribing doctors.
The individual rehabilitation plan must contain: a) the indication of the pathology or injury that caused the disability; b) a functional diagnosis showing the specific disability; c) the description of the treatment plan with an indication of the expected outcomes in relation to the use of the prosthesis in medium and long term; d) the kind of device and any necessary adaptations or customizations; e) how and when the device may be used, the possible requirement for assistance or supervision in its use, the possible contraindications and the limits of its use with regard to the functional response; f) the indication of how the program will be followed up and how the results obtained with respect to those expected. In exceptional cases, for patients with extreme disabilities, local health agencies may ensure access to prostheses, orthoses, or aids not included in those listed in the nomenclature, in accordance with the procedures established by Regions and Autonomous Provinces, and on the basis of specific criteria and guidelines[8].
Finally, it should be noted that the provision of healthcare services is always conditioned by the **suitability assessment**. Social and health services are suitable when it meets patients' needs, their efficacy is scientifically demonstrated and they satisfy the principle of economy in the use of resources. In other words, the principle of suitability plays a fundamental role since it acts as a "watershed" between what can be guaranteed by the NHS, and what the NHS is not required to provide[9].
The relevance of the principle of suitability is particularly evident with regard to innovative therapies and technologies, such as biorobotic technologies: they are generally expensive (although they may generate virtuous mechanisms and ultimately savings in the long term) and their effectiveness may be based on unconsolidated scientific evidence, precisely due to their innovative nature.

3.1.4.3 The mechanism for updating

The Law no. 208/2015 required the establishment of the mechanism for updating the Basic Levels of Care.
In particular, the *National Commission for the updating of the Basic Levels of Care and the promotion of the appropriateness in the National Health Service* has been set up to guarantee the systematically and continuously updating of the services.
The Commission is appointed and chaired by the Minister of Health and sees the participation of members of:

- Regions;
- The Italian National Institute of Health (italian acronym: ISS);
- Italian medicines Agency (Italian acronym: AIFA);
- National Agency for Regional Health Services (Italian acronym: AGENAS);
- Ministry of Economy and Finance.

It began its work on 28th July 2020 with the stated aim to create a National Health Service (NHS) always in step with the technological and scientific innovations and the needs of the citizen.
The update requests of the services included in the Basic Levels of Care may be submitted to the Commission by:

8 Article 18, Paragraph 8.

9 I.e., the so-called "Caso Di Bella" (Const. Court, no. 185/1998).

- Citizens or patient organizations;
- Ministry of Health or Institutions supervised (AIFA; AGENAS; ISS);
- Healthcare companies and local health authority;
- University hospitals;
- Health care technology companies.

The Commission has received:

- 9 update requests for the triennium 2017-2018;
- 56 requests in the year 2019;
- 122 requests in the year 2020;
- 62 requests in the year 2021.

The updating of each service is realized by Decree of the Minister of Health and the State-Regions Conference expresses a favorable opinion on the draft decree.
The mechanism has revealed weak points where investments and improvements will be needed to make the system more efficient.
In fact, the legislative framework does not contain accurate references to the timeframe in which complete the exam of the request and to the criteria for assessing the addition of new services.
Not being provided clear and even valuation parametres, the works of the Commission are absolutely discretionary.
The only criterion that inspires the assessments of the Commission is the principle of suitability.
This principle imposes the choice of services which are compatible with the resources of the Healthcare local authorities and with the financial and organisational rules of the hospitals.
It follows that only suitable services can be inserted into the Basic Level of Care.
However, the services included in the Basic Level of Care cannot be granted to the citizens until after the identification of the maximum tariff for their provision.

3.1.4.4 The issue of tariff updates

The Legislative Decree no. 502 of 30 December 1992 identifies the method and criteria for defining the healthcare rates.
In particular, the article 8, Paragraph 1, provides that the Minister of Health, by special Ministerial Decree, *a)* establishes the classification systems which define the service or performance unit to compensate and *b)* outlines maximum tariffs to be paid for the accreditate structures.
Such estimates need to comply with the principles of economy and efficiency and shall take into the standard cost of the services already available or previously identifiable.
With the same Ministerial Decree are defined also the general criteria by which Regions adopt own tariff system.
Consequently, these tariffs are used as twofold reference for the assessment supporting: *a)* the adequacy of the resources at the disposal of the National Healthcare System and *b)* the weight of the regional finances in order to guarantee the health care.
Then, according to the Paragraph 7 of the same article, it is expected that by Decree of the Minister of Health, after the agreement within the State-Regions Conference, shall be governed **the way of remunerating the prosthetic and special-outpatient assistance included in the Basic Levels of Care**.
This measure represents the most important thread in the development of the health care systems because it allows to update the type of services, including technologically advanced performance.
The adoption of this Ministerial Decree (also called Tariffs decree) essentially enables the periodic funding of the Italian National List of assistive devices eligible for provision through the National Health Service.
In fact, **only the setting of the tariff plan can allow the provision of services, so that the "new" Basic Levels of Care remain locked without the prior adoption of the Tariffs decree.**
It follows that the services included in the Basic Levels of Care cannot be evenly provided in all Regions until after the approval of the relative tariffs.

The required steps to define the new tariffs of the prosthetic and special-outpatient assistance are two:

1. The first takes place at the national level and becomes concrete in the adoption of a specific decree of the Minister of Health;
2. The second, that involves the Regions through the State-Regions Conference, supposes an agreement over the national tariff for each service.

Therefore, in the procedure for the updating of Basic Levels of Care it is necessary the convergence of all levels of government (statal and regional).
The article 1, Paragraph 420, of the Law no. 205/2017 expressly stated that the adoption of the tariffs decree should have happened no later than 28th February 2018.

However, the Ministry of Health presented a first version of the decree only in the January 2022 and the State-Region Conference rejected it; in the September 2022 an amended version of the decree was defined but the State-Region Conference has postponed the scrutiny due to the reluctance of some Regions.

In the meeting of 28th September 2022 of the State-Regions Conference, the agreement on the draft tariffs decree was withdrawn from the items of discussion.

The existing coordination mechanisms between State and Regions have still not found an agreement and in we are attended since 28th February 2018 of the emanation of the tariffs decree.
So, on one side there are the Regions who have the opportunity to provide additional services with their own resources; on the other side there are the Regions (Abruzzo, Calabria, Campania, Lazio, Molise, Apulia and Sicily) who are subjected to the Plan Return and could provide only the services indicated in the "old" Basic Levels of Care set in 2001.
Because of that delay, the health care system remains anchored to outdated services and cannot accept the advances in scientific research.
Within the services introduced by the dPCM 12th January 2017, but not yet operational due to the lack of the maximum tariffs, there are highly technological services.
To confirm this, just consider that were not fixed the tariffs for the hadrontherapy, the enteroscopy with micro camera, the stereotatic radiotherapy, the home automation systems, the control sensors or the voice recognition systems.

The consequences are that:

- the Basic Levels of Care updated with the dPCM of 2017 are not yet functional uniformly throughout the country;
- the further updating of the Basic Levels of Care is stationary because the addition of new services could not produce effects.

We can therefore conclude that the effective admission of the robotics and domotics technologies in the national and regional health care system cannot be separated from the adoption of the tariffs decree.

3.1.4.5 The monitoring procedure

The **Guarantee System (GS)** represents the instrument through which the Italian Government ensures the delivery of BLCs under conditions of quality, suitability and uniformity. It was introduced in 2000 with the D.lgs. no. 56/2000.
It defined a set of approximately 100 indicators. The overall evaluation methodology includes a weighting system that assigns a reference weight to each indicator and assigns scores based on the region's level of achievement relative to national standards.
The **BLC Committee** is the responsible subject of the process. It was established by the Minister of Health's Decree of 21st November of 2005. In particular, until 2019, its monitoring activity was carried on through the use of the so-called "**BLCs Grid**," which was a set of indicators throw which it is possible to catch the performance of each RHS and framing the possible territorial inequalities. In 2019[10], with the introduction of the **New Guarantee System (NGS**), the BLCs Grid was replaced by a new set of 22 indicators, called "**CORE**". In order to be "compliant" with the BLC, each Region has to reach a score of 60/100 in each BLC macro-area. The remaining 66 new NGS indicators not belonging to CORE are part of the so-called "**NO CORE**" subset. The list of CORE subset indicators can be reviewed annually by the BLC Committee.

BLC COMMITTEE COMPOSITON:

- **4 representatives** from the Ministry of Health (one of whom acts as coordinator);
- **2 representatives** from the Ministry of Economy and Finance;
- **1 representative** from the Department for Regional Affairs of the Presidency of the Council of Ministers;
- **7 representatives** from the Regions designated by the Conference of the Presidents of the Regions and Autonomous Provinces**.**

Article 116, Paragraph 3, Cost.: "*Additional special forms and conditions of autonomy, related to the areas specified in art. 117, Paragraph three and Paragraph two, letter l) - limited to the organizational requirements of the Justice of the Peace - and letters n) and s), may be attributed to other Regions by State law, upon the initiative of the Region concerned, after consultation with the local authorities, in compliance with the principles set forth in art. 119*".

3.1.4.6 The differentiated regionalism

Article 116, Paragraph 3, of the Constitution provides that state law may attribute to regions 'further special forms

and conditions of autonomy' on the basis of an agreement between the state and the Region concerned.

The subject matters on which the "further special forms and conditions of autonomy" can be activated are:

- **All subject-matters of concurrent legislative competence** (Article 117, Paragraph 3, Const.);
- **The following subject-matters of exclusive state legislative competence:**
  - organisation of peace justice (Article 117, second Paragraph, lett. l) Const.);
  - general rules on education (Article 117, second Paragraph, lett. n), Const.);
  - protection of the environment, the ecosystem and the cultural heritage (Article 117, second Paragraph, lett. s) Const.).

10 With the DM 12th March 2019.

The allocation of new legislative and administrative functions is subject to the definition of the 'basic levels of benefits' (BLB) concerning civil and social rights that must be guaranteed throughout the national territory, pursuant to Article 117, second Paragraph, lett. m) of the Constitution.

The "Cabina di Regia" shall

a) carry out a recognition of state legislation and administrative functions exercised both by the State and Regions in each of the subject-matters listed in Article 116, Paragraph 3, of the Constitution;

b) carry out a recognition of the historical State expenditure in each region over the last three years, with reference to the matters referred to in Article 116, Paragraph 3, of the Constitution, and to the individual administrative functions exercised by the State

To this end, Law no. 197/2022 (Budget Law for 2023) has set up a committee, named "Cabina di Regia", for the determination of the BLBs under the Presidency of the Council of Ministers.
Within six months from the conclusion of the activities, the "Cabina di Regia" shall prepare one or more draft decrees of the President of the Council of Ministers by which the BLBs and the related standard costs and needs are determined, also separately, in the subject matters mentioned by Article 116 Const.
The subordination of the mechanism of differentiated regionalism to the prior definition of BLBs and BLCs could abstractly entail the advantage of encouraging and accelerating the procedures for updating and financing individual benefits, including encompassing even the most advanced technological tools. In practice, it will depend on how the Committee succeeds in operating.
To date, the provision has never been fully implemented. In the final part of the 17th legislature, Emilia Romagna, Lombardy and Veneto began negotiations with the Government that led to the subscription, on 28 February 2018, of three separate "preliminary" agreements. With the start of the 18th legislature, all three regions which signed the so-called pre-agreements expressed to the government their intention to broaden the range of subject matters to be transferred. In the meantime, other regions, although they have not signed any pre-agreement with the Government, have expressed their willingness to undertake a path to obtain additional forms of autonomy (Piedmont, Liguria, Tuscany, Umbria, Marche and Campania).
Health protection is one of the subject matters most affected by the preliminary agreements. In particular, the Regions have requested 'greater autonomy' in the following areas: human resources management (with regard to the removal of specific constraints on expenditure and on free-professional activity); training of specialized medical workers (in particular, through special agreements with the universities); determination of the system of tariffs, reimbursement, remuneration and co-participation; governance system of the companies and bodies of the regional health system; establishment and management of supplementary health funds.
However, the possibility for affected regions to demand additional competencies with regard to services previously defined in the BLCs could cause new distorting inequalities in the health protection and in the use of new technologies.
In fact, if BLCs were truly updated and new biorobotic technologies included, the differential regionalism on these services could reward some "privileged" Regions at the expense of all others.
In a scenario in which the constitutional right to health is conditioned by 21 regional health systems that still generate inequalities in the offer of healthcare services, there is a real risk that regional differentiation could lead to the "destructuring of the National Health System"[11].
In other words, without the concrete guarantee of BLBs and without specific financial constraints, differentiated regionalism risks to legitimize the gap between the North and the South, violating the constitutional principle of equality in the enjoyment of the right to health, due to the close relationship between the guarantee of the latter to the organization of health services.

11 Balduzzi R., Servetti D., Regionalismo differenziato e materia sanitaria, in Rivista AIC, 2/2019, p. 12.

3.1.5 Conclusions

The reflections produced in the previous Paragraphs aim to underline various critical aspects whose resolution is crucial to the full application of the robotics and domotics technologies in the fields of social and health services.

Below, we try to highlight the issues related to the reform of the basic levels of care by identifying possible prospects of getting out of the current situation at stake:

- Input mode of the biorobotics technologies within the macro-areas of the BLCs: the development of technology requires continuous adjustments of the healthcare system so that it's appropriate to adopt periodic checks of the areas of activities.
- The constraint of the principle of suitability in the mechanism for updating: the robotics and domotics technologies, by their nature, entail high costs which should not be compatible with the principle of suitability.

It's therefore necessary the introduction of the assessment criteria that encourage and privilege the scientific progress.

The updating of the services may keep in step with the times only if there will be no aprioristic limits in the choice of the 'new' BLCs.

- The absence of a measure that imposes time limits for the updating procedures: the services' updating process must take place within certain times. The works of the Commission should follow well-defined processes so as to offer prompt response to the requests.
- The 'lock' of the updates consequently to the non-agreement on the tariffs decree: the subordination of the provision of services to the determination of maximum tariffs provokes a serious restriction of citizens' rights. It is absolutely essential to guarantee the contextual definition of the new services and of their costs.
- The distorting consequences of the arrangement of the Plan return applied to the deficit Regions: the system of the Plan return does not allow the Regions who are experiencing hardship to ensure the updated health services. This mechanism creates inequalities and harms even more the Regions in economic difficulty.

It is hoped that this discipline can be reformed allowing investments controlled in such a sensitive area. Otherwise, who guarantees the BLCs in these Regions?

3.2 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 (General Data Protection Regulation)

3.3 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

3.4 REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 5 APRIL 2017 ON MEDICAL DEVICES, AMENDING DIRECTIVE 2001/83/EC, REGULATION (EC) NO 178/2002 AND REGULATION (EC) NO 1223/2009 AND REPEALING COUNCIL DIRECTIVES 90/385/EEC AND 93/42/EEC

3.4.1 Executive Summary

The medical devices sector has vastly developed over the past 20 years. The MD Directive (MDD) 93/42/EEC[12] and Active Implantable MDD (AIMDD) 90/385/EEC[13] were the European Union's regulatory model until recently, first published in 1993 and 1990 respectively and have now been replaced by the MD Regulation (MDR) 2017/745[14] which entered into full application on 26th May 2021 after a transition period of three years, extended in early 2020 for a fourth year due to the COVID-19 crisis. While the regulation does not fundamentally change the conformity process for medical devices, it does seek to address weaknesses in it, particularly in the realm of surveillance and transparency, however it does so with an overly complex transitionary period that is currently open to fundamental operative flaws that put the seamless supply of medical devices, as well as innovation in the medical devices sector of the European Union at risk.

3.4.2 Background

The regulation of Medical Devices was preceded by two directives, The Medical Devices Directive (MDD) 93/42/EEC and Active Implantable Medical Devices Directive (AIMDD) 90/385/EEC. Under Annex IX of the MDD, the first step was to classify the actual device. The regulation provided 18 rules to classify medical devices. According to these Rules, medical devices are classified by their intended purposes. These rules would identify the risk value of the device and classify them into class I, I-measuring, I- sterile, IIa, IIb and III., which would then decide the conformity assessment process. The manufacturer would then proceed with the conformity assessment process with certain options available depending on the risk classification of the device, provided they are not custom made or intended for a clinical investigation under Article 11 of the directive:

- For Risk Class III devices: Annex II or III coupled with Annex IV or Annex V
- For Risk Class IIa devices: Annex VII coupled with Annex IV or Annex V or Annex VI or Annex II.
- For Risk Class IIb devices: Annex II (minus point 4) or Annex III coupled with Annex IV or Annex V or Annex VI
- For Risk Class I devices: Annex VII

Compliance for most risk classifications under the directive essentially boiled down to certain requirements: a 1) Quality Management System (ISO 13485); 2) Technical file, including a design file for the highest risk classifications; 3) Hiring of a Notified Body for assessment and certification; 4) Appointing of an EU authorized representative for regulatory affairs not sales and marketing[15]. The technical file comprised of:

a) Classification justification;

12 Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, Document 31993L0042, ELI: http://data.europa.eu/eli/dir/1993/42/oj

13 Consolidated text: Council Directive of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (90/385/EEC), Document 01990L0385-20071011, ELI: http://data.europa.eu/eli/dir/1990/385/2007-10-11

14 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.), ELI: http://data.europa.eu/eli/reg/2017/745/oj

15 Yvonne Halpaus, 'Medical Device Directive 93/42/EEC CE-Marking What Manufacturers Need to Know & Do', 2015, QNET LCC, at p2

b) General Information about device and suppliers and sub-contractors; c) Translated Labels and Instructions for use and use of EU Symbols;
c) Risk assessment in accordance with ISO14971 latest issue;
d) Essential requirements may include biocompatibility, flammability, EMC/LVD, software standards and other test reports;
e) Evaluation of clinical data;
f) Procedures: for vigilance, post marketing review, translations etc.
g) Declaration of Conformity; etc.

The manufacturer would then appoint a representative, whose role was to share information with the competent authorities to prove that a device conforms with the MDD as well as register the device and keep the technical file available to the competent authorities.

During the 2000s, it was becoming increasingly concerning that the MDD and its sister regulation for IVDs, the IVDD, were becoming outdated. Medical technology was quickly advancing and evolving rapidly, including MDs. A scandal broke down involving Poly Implant Prothese (PIP) Breast Implants, which resulted in severe injuries and deaths due to the manufacturer using industrial grade silicone to make breast implants. While this was in violation of the regulations at the time, the medical device safety framework lacked sufficient checkpoints to prevent it from happening. The Medicines and Healthcare Regulatory Authority had completely failed to safeguard women who had received these implants despite first receiving a report of potential problems with PIP implants nearly a decade before the scandal had broken out, including a case of premature rupture of both implants in the same patient[16]. In light of this scandal, the EU introduced the IVDR[17] as well as the EU Medical Device Regulation (EU MDR) to try and prevent such a tragedy from happening again[18], and that case as well as others, such as Johnson & Johnson recalling toxic on-metal hip system were the cited reasons for the new regulations introduced by the EU by the European Medicines Agency[19]. A notable aspect of the MDR was the sheer lobbying pressure that it received from the industry during the deliberation period[20], particularly from MedTech, the largest trade association of the industry. This led to several of the stricter amendment options were rejected, such as additional requirements for premarket clinical trials and a transfer of the responsibility for certifying high-risk devices to the European Medicines Agency[21].

The MDR was passed on 5 April 2017 and entered into force on 25 May 2017, replacing both the Active Implantable Medical Devices Directive from 1990 (AIMDD; 90/385/EEC) and the Medical Device Directive from 1993 (MDD; 93/42/EEC). The new regulation was due to become fully applicable on 26 May 2020 after a three-year transition period but was postponed by a year due to the Covid-19 pandemic[22]. Since they are regulations of the European Union, they become binding in all member states automatically after being adopted by the European Parliament and the Council of the European Union, unlike a directive which requires adoption by the national parliaments of each member state to take into force.

Much like its sister regulation, the IVDR, all devices on the market will need to be recertified in order to stay on the market, though some medical devices with certificates issued by notified bodies under the directives may continue

16 Victoria Martindale, Andre Menache, 'The PIP scandal: an analysis of the process of quality control that failed to safeguard women from the health risks', May 2013, Journal of the Royal Society of Medicine

17 Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.), OJ L 117, 5.5.2017, p. 176–332, ELI: http://data.europa.eu/eli/reg/2017/746/oj

18 Laura Maher, Niki Price, 'Ultimate Guide to IVDR for In Vitro Diagnostic Medical Device Companies', November 2022, Greenlight Guru

19 Zaide Frias, 'Update on EMA role in implementation of new legislation for medical devices (MDR) and in vitro diagnostics (IVDR)', 20 November 2019, Annual PCWP/HCPWP meeting with all eligible organisations

20 Which lasted from 2008 to 2013

21 S. Bowers, D. Cohen, 'How lobbying blocked European safety checks for dangerous medical implants' 2018

22 Kosta Shatrov, Cart Rudolf Blankart, 'After the four-year transition period: Is the European Union's Medical Device Regulation of 2017 likely to achieve its main goals?', December 2022, Elsevier Health Policy, Volume 126, Issue 12, Pages 1233-1240, at 1234

to be placed on the market until 27 May 2024[23]. The big initial change of the MDR is the increase in scope. The scope of the MDR has been expanded to include certain products that were previously not covered by the MDD, such as certain aesthetic products, software, and devices that incorporate nanomaterials[24]. The MDD previously classified software and specific groups of products without an intended medical purpose as consumer goods instead. This was likely a response to the PIP scandal that preceded it. Specifically, the MDR[25] defines a medical device as:

(1) 'Medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations, and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means.

The following products shall also be deemed to be medical devices:

- devices for the control or support of conception;
- products specifically intended for the cleaning, disinfection or sterilisation of devices as referred to in Article 1(4) and of those referred to in the first paragraph of this point."

Crucially, the MDR continues on to provide 71 definitions of different medical device classifications. This is a stark increase to the mere 11 definitions used in the MDD to classicfy devices. The MDR now classifies devices into four major risk classes: I, IIa, IIb, and III – according to the risk they constitute to the health of patients and consumers, with class I representing the devices that pose the lowest risk. Notably however, the MDR also refines and expands upon the rules of classification, resulting in a total of 22 rules over the MDD's 18. Some medical devices have been additionally assigned to a higher risk class, such as most software products, which have been assigned as class IIa devices under the MDR[26].

The MDR also introduces the concept of an economic operator. This collective term is used to describe following stakeholders[27]: legal manufacturers, authorized representatives, importers, distributors, or natural and legal persons who combine or sterilize system or procedure packs. The MDR then expands the duties of these economic operators alongside the entire supply chain. Under Articles 10 and 11 of the regulation, manufacturers from non-EU countries need to appoint an authorized representative who is located within the EU and is fully legally liable for defective devices alongside together the manufacturer. Notably however, the MDR also assigns duties to importers and distributors, who now have duties ranging from verifying and ensuring the conformity of medical devices with the MDR, to keeping a register of and notifying other economic operators about complaints, recalls, and withdrawals that a medical device may be subjected to[28]. This is a substantial change from the MDD, where distributors have no

23 Ibid

24 Art. 2 & Annex XVI

25 MDR Article 2 (1)

26 At 11, p

27 MDR, Article 2(35)

28 Articles 13 and 14 respectively

obligations and importers had only the duty of keeping the technical documentation of a device available in case that neither the manufacturer nor their authorized representative was based in the European Union.

Additionally, the MDR also seeks to strengthen the procedure for designating notified bodies. Much like its preceding regulation, Notified Bodies are mostly private, for-profit organizations that charge fees to manufacturers for assessing the conformity of a medical device with the requirements of the MDR. The designation of these Notified Bodies has been the responsibility of the member states in which they are situated under the MDD. The MDR changes this procedure. The procedure is now carried out by a joint assessment team consisting of three experts – one from the European Commission and two from member states other than the state in which the applying conformity assessment body is located. The MDR also establishes a new body named the Medical Device Coordination, which then shares experiences and exchanges views on issues relating to notified bodies, and drafts technical recommendations, which is considered before the designation of the Notified Body. The Notified Bodies still retain their abilities to delegate certain activities of conformity assessment of the MDR to subcontractors, much like the MDD allowed them[29].

Some of the most crucial changes that the MDR introduces relate to the classification and conformity assessment. The MDR creates a new advisory body, which is appointed by the European Commission, which is comprised of an expert panel comprising clinical and technical experts[30]. This body has the ability to modify the requirements related to the conformity assessment of medical devices such as by developing common specifications or providing manufacturers with advice on their clinical development strategy, but also has the ability to give opinions regarding the classification of certain high-risk devices. While these opinions are non-binding, notified bodies must still nevertheless justify their decision should they choose to disagree with the panel's opinions[31]. Clinical evaluations are still a requirement for manufacturers to bring new devices in the market, and much like the MDD, it is possible for a manufacturer to conduct a clinical evaluation by demonstrating the equivalence of the technical, biological, and clinical characteristics of a device to those of a predicate one, with implantable class IIb and III devices generally requiring device specific clinical data[32]. Annexes XV and XIV also require that manufacturers must submit a clinical investigation report that includes a critical evaluation of both the positive and negative findings they have generated in a clinical investigation, as well as a requirement to document and conduct clinical evaluations through the establishment and update of a clinical evaluation plan[33].

Finally, the MDR crucially enhances the post market surveillance of medical devices. To facilitate a more coordinated information effort in that regard, as well as a more transparent environment, the EU has additionally set up EUDAMED, as part of both the IVDR, as well as Regulation 2017/745. EUDAMED will act as a central repository for information on medical devices and in vitro diagnostic medical devices (IVDs) placed on the EU market, including their manufacturers, distributors, and authorized representatives and will facilitate the exchange of information between national competent authorities, the European Commission, and economic operators such as manufacturers, importers, and distributors[34]. EUDAMED will consist of six interconnected modules that cover different aspects of the medical device regulatory process, including registration of economic operators, registration of devices, certificates, clinical investigations, vigilance, and market surveillance. The database will allow authorized users to access information about medical devices and IVDs, including their technical specifications, conformity assessment, clinical evidence, post-market surveillance, and adverse events reporting. The implementation of EUDAMED was initially planned for May 2020, but due to technical difficulties, it has been delayed. The European Commission has proposed a phased implementation of EUDAMED, with some modules being available before

29 Under Art. 37 & Annex VII respectively

30 Art. 54–55, Art. 106 & Annex IX

31 At 11, p1235

32 At 11, p1235

33 Ibid

34 Laura Maher, pp 12-13

others[35]. The new implementation date is expected to be announced soon. Once EUDAMED is fully operational, it will play a critical role in ensuring the safety and effectiveness of medical devices and IVDs in the EU market by providing a comprehensive and transparent database for regulators, manufacturers, and other stakeholders. Through EUDAMED, the MDR aims to "identify any need for taking additional preventive actions and to promote collaboration between economic operators after devices have been placed on the market. To meet this aim, manufacturers must create post-market surveillance plans to inform competent authorities and notified bodies about (non-)serious incidents and undesirable side-effects, as well as feedback and complaints provided by users and economic operators under Articles 83-84 and Annex III[36]". The MDR strongly encourages manufacturers to conduct their post-market surveillance in a proactive manner as to identify unknown side-effects or potential misuse that devices may have[37].

3.4.3 Impact and Challenges

Unfortunately, the new MDR is not without its growing pains. As mentioned above, on 27 May 2024 all certificates issued under the former two directives will expire, requiring all devices on the market with such certificates to require an entirely new certification under the MDR. But as of July 2022, MedTech reported that the vast majority of medical devices on the market had yet to transition to MDR compliance, despite having less than two years remaining until the deadline of 26th of May 2024[38]. This included certificates that have not been issued yet for "more than 85% of the > 500,000 devices estimated to be covered by (AI)MDD certificates"[39]. Some scholars estimate that a full transition "will probably take even longer than this to complete, and devices certified under the former directives will continue to be used during this time and perhaps for decades if they are put into service or made available on the market on 26 May 2025 at the latest[40]," which is why there has been a reluctance in assessing the impact of the MDR currently.

A big contributor to this problem seems to be the time taken to certify. Industry respondents in the MedTech survey indicated that while for some this process can be relatively fast, taking only six months, for the vast majority of manufacturers the process quoted by notified bodies was usually 13 to 18 months[41]. This was especially the case for new devices as well as class III devices. Access to notified bodies is generally difficult, with five of the old notified bodies withdrawing from the market, likely due to the more stringent requirements imposed by the MDR[42], with only 20 of the existing 56 notified bodies having been designated under the MDR by 2022[43]. Unpredictable certification time resulting in longer cycles, combined with the lack of binding conformity assessment timelines, responsiveness from the notified body can be devastating for innovation and supply in the European Union's medical device industry. MedTech's survey reveals that since 26 May 2021, 101 companies participating in the survey have already chosen to launch 4,306 new devices outside of the European Union (instead of the EU)[44]. Since 2021, it seems that the geography of preference for a first regulatory approval since 2021 is the USA, with large companies now more likely to prioritise the USA over the EU for new approvals for medical devices[45], with EU based SMEs also

35 MediCept, 'Eudamed Update: Implementation is Paused, MDR Compliance is Not', 29 April 2021

36 At 11, p1235

37 Annex XIV

38 MedTech, 'MedTech Europe Survey Report analysing the availability of Medical Devices in 2022 in connection to the Medical Device Regulation (MDR) implementation', 14 July 2022, at p6

39 Ibid

40 At 11, p1235

41 Ibid, p8

42 Oriel STAT A MATRIX Blog. 'Status of EU Notified Bodies Designated to EU MDR 2017/745 and IVD 2017/746', 21 April 2021

43 At 11, 1237

44 At 27, p17

45 Ibid

now indicating that EU and USA are now prioritised equally for new products, which in essence means that half of EU based innovation will benefit USA-based patients first, rather than ones in the European Union[46].

This is particularly impactful towards SMEs, where only 6% of their devices planned to be transitioned to MDR have been certified under the new regulation, compared to 16% of MDR certified devices planned to be transitioned by large companies, and only 7% of SMEs certificates (TF and QMS) have been issued under MDR, compared to an overall average of 13% as of 2022 according to the MedTech survey[47]. The survey also reports that while SMEs account for 26% of the total number of devices expected on the market by 26 May 2024 (or 18% of devices requiring a certificate, i.e., those in Class Ir/Is/Im/IIa/IIb/III), SMEs will require 40% of the total certificates needed. In addition, as discussed in the previous section, SMEs lag behind larger companies in terms of submitted applications for MDR certification, with At least 15 % and up to 30% of SMEs report having no access to an MDR-designated Notified Body yet[48]. Despite SMEs being seen traditionally as the backbone of the European industry[49], due to their characteristics and limited resources, they tend to lack the financial capability to enter new devices into the market as compared to large firms, as well as conduct independent clinical tests[50]. While the MDR does make some concessions for SMEs through exemptions such as from the obligation to directly employ a person responsible for regulatory compliance under Article 13, as the survey suggests, implementation of harmonized strategies has proven very difficult for SMEs regardless. This could have drastic results on the industry, leading to potential shortages of vital medical devices from the market and their temporary reduction of availability from the European Union health sector[51].

Despite the negative implications and growing pains of the MDR, it is difficult to ignore the potential positive impacts that it will likely have, particularly on the primary goal it set out to achieve, namely increasing patient safety. The creation of EUDAMED allowing for the aggregation of post-market data on potential adverse effects, detection and prevention can become a lot more proactive and faster in the future, as soon as stakeholders overcome their insufficient familiarity with the database itself[52]. But crucially while the substantial equivalence test that was retained from the MDD has long been criticized by scholars for providing the wrong incentives by deterring manufacturers from gathering new clinical evidence[53], or a series of incremental changes nevertheless leading to a new device that are substantially different from the original one[54], the MDR still may reconcile this through its more stringent post-market surveillance. While such an effort on the side of manufacturers has not been observed by scholars yet, stricter requirements might encourage manufacturers to work towards an improved patient safety in the EU healthcare sector. Some scholars, however, still remain sceptical about the effectiveness of post-market surveillance. Shatrof and Blankart state that on the long term, “postmarket evidence is mostly irrelevant for assessing the safety and effectiveness of medical devices currently on the market because many of these are continuously modified and replaced, making the data collected on the parent device less valuable[55]”. In addition, they state that “many health professionals regard adverse events as natural and reporting these as unnecessary, unfeasible, or even futile, and, often, industry does not respond to safety issues”, and that “many users also do not have sufficient knowledge of adverse event reporting systems, even in large hospitals”[56]. Finally, they state that

46 Ibid

47 Ibid, p15

48 Ibid

49 MedTech Europe. The European Medical Technology Industry in figures; 2019.

50 C. Sorenson, M. Drummond, ‘Improving medical device regulation: the United States and Europe in perspective’, Milbank Q, 92 (1) (2014), pp. 114-150

51 N. Martelli, D. Eskenazy, C. Déan, J. Pineau, P. Prognon, G. Chatellier, et al, ‘New European regulation for medical devices: what is changing?’, Cardiovasc Intervent Radiol, 42 (9) (2019), pp. 1272-1278, 10.1007/s00270-019-02247-0

52 At 11, 1237

53 At 39

54 At 11, p1237

55 Ibid

56 Ibid

since the interpretation of problem report and registration is the responsibility of competent authorities in each member state, the response's effectiveness will naturally vary across each of the countries[57].

Another majorly cited problematic feature of the MDR regard the ambiguity of the MDR. As a matter of fact, this is one of the top 5 indicated challenges with notified body that industry body MedTech had found in their survey, citing "fragmented/ non-harmonised interpretations of the same requirements of the MDR among Notified Bodies and within Notified Bodies", and "fragmented/ non-harmonised interpretations of MDCG guidelines", as reasons 4 and 5[58]. Shatrof and Blankart elaborate on this and state that "while the MDR generally adds precision to the regulation of medical devices, the text of the regulation uses many ambiguous terms, such as "sufficient clinical evidence" (e.g., regarding the safety, performance, and benefit-risk ratio of devices; Art. 61), "substantial modifications" (e.g., concerning the design of clinical investigations; Art. 75), and "reasonable period" (e.g., concerning the withdrawal of defective devices from the market; Art. 95)[59]." Article 2 simply does not specify these terms, which leaves room for various interpretations on the side of the Notified Bodies, with an uncertain effect on patient safety and the harmonization of standards[60]. While the two scholars believed that the Medical Device Coordination Group, competent authorities and expert panels would provide sufficient guidance documents to remedy this issue, the MedTech survey indicates that these remain fragmented. MedTech has reported that the MDCG guidance documents can slow down the certification process and lead to rework of the submitted applications and cite that "more than 1 in 5 companies have reported a delay in certification due to a publication of new or revised MDCG guidance. Almost half of all delays led to some level of reworking[61]". They also specify that these delays were caused by three particular documents, out of the 45 cited by respondents:

- MDCG 2021-24 Guidance on classification of medical devices[62]
- MDCG 2020-5 Clinical evaluation – Equivalence: A guide for manufacturers and notified bodies[63]
- MDCG 2020-6 Guidance on sufficient clinical evidence for legacy devices[64]

They further specify that respondents cite "delayed or missing (such as PSUR), guidance is treated "as a law" (sometimes in opposition to the MDR legal text) or guidance does not provide the needed clarity[65]", which further complicates the issue of ambiguity in guidelines in the regulatory assessment process of the MDR.

3.4.4 Policy Recommendations

It is undeniable that the implementation of the MDR in the EU is having a serious effect on the EU medical device market, in both positive and negative regards. First and foremost, the most important shortcoming of the MDR to address is access to notified bodies, which as discussed, remains incredibly difficult, resulting in severe and unpredictable delays, which put the seamless availability of medical devices and the prioritization of innovation in the EU healthcare sector at risk. This was thankfully partially addressed already by the European Commission through the proposal 2023/0005 (COD), amending the transitional provisions of the EU Medical Devices Regulation

57 Ibid

58 At 27, p8

59 p1237

60 Ibid

61 At 27, p19

62 MDCG 2021-24 Guidance on classification of medical devices (October 2021)

63 MDCG 2020-5 Clinical evaluation – Equivalence: A guide for manufacturers and notified bodies

64 MDCG 2020-6 Clinical evidence needed for medical devices previously CE marked under Directives 93/42/EEC or 90/385/EEC

65 At 27, p19

(MDR) and the sister regulation, In Vitro Diagnostic Medical Devices Regulation (IVDR)[66]. The Commission acknowledges that "despite considerable progress over the past years, the overall capacity of conformity assessment ('notified') bodies remains insufficient to carry out the tasks required of them", and that "many manufacturers are not sufficiently prepared to meet the strengthened requirements of the MDR by the end of the transition period[67]". The proposal will seek to extend the deadline of the transitionary period "from 26 May 2024 until 31 December 2027 for higher risk devices (class III and class IIb implantable devices except certain devices for which the MDR provides exemptions, given that these devices are considered to be based on well-established technologies) and until 31 December 2028 for medium and lower risk devices (other class IIb devices and class IIa, class Im, Is and Ir devices)[68]". This extension is subject to certain conditions, such as the devices must continue to conform with the MDD, and must not undergo substantial changes. Needless to say, the industry has welcomed this proposal[69], but it is noted that this is only an extension and does not actually fix the fundamental issues regarding Notified Body availability that was discussed above. But considering the length of the extension of a staggering four years, it could potentially be enough time for the Commission to resolve these issues and create more Notified Bodies to streamline the conformity assessment procedure, as well as make the timeline for it more consistent.

In regard to the issue of uncertainty of the guidelines provided, MedTech has taken a very vocal stance regarding that. While they agree that such documents are important and welcome their addition, they urge that such documents should stay as guidance documents and should be taken into consideration in varying degrees to devices and device categories, roles "(e.g. Economic Operators), circumstances and that appropriate flexibility is necessary as long as the overall goal is respected[70]". In order to avoid potential delays that arise due to the guidance documents, the urge that "the burden to introduce new unplanned interpretation of the Regulation into the assessment should be minimised and delays to complete the conformity assessment should be avoided[71]", especially as regard to new administrative requirements (such as using certain forms or product codes). In the case that such a guidance document is published during a conformity assessment, where the Notified Body believes that consideration is required, MedTech suggests that the industry should be more involved in that process, and manufacturers should have a say as to whether there is an applicability of the new document, and be able to propose solutions and timelines for implementation of such solutions. In general, there should be a more effective discussion between Notified Body and the manufacturer, particularly in regard to the implementation plan of the guidance documents to facilitate a continuous availability of the medical device[72]. The MDR does not provide for the timing that guidance documents have to be considered by Notified Bodies after completion of the conformity assessment. Therefore, MedTech proposes that newly published guidance documents are considered at the earliest at the time of next periodic re-assessment, and that suspension or withdrawal of a certificate per MDR Art. 56.4/IVDR Art. 51.4 should be considered only in the event that the conformity to the requirements of the Regulations is not met through the principle of proportionality in order to alleviate delay and supply issues caused by document delay[73]. Of course, this is in addition to the comprehensibility issues outlined above. Shatrof and Blankart recommend that in general, future regulation should be written in simpler language with fewer cross-references among articles and annexes in order to make it more accessible[74]. They also recommend an expansion of the definitions included in Article 2 of the

66 Proposal REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards the transitional provisions for certain medical devices and in vitro diagnostic medical devices, Brussels, 6.1.2023, COM(2023) 10 final

67 Ibid. p1

68 Ibid, pp7-8

69 MedTech, 'MedTech Europe welcomes the adoption of amended transitional provisions of the Medical Devices Regulations and calls for continued work to address outstanding implementation challenges', 7 March 2023, MedTech Press Release

70 MedTech, 'Recommendations on the use of Guidance Documents Related to the Medical Device Regulation (MDR) and In vitro Diagnostics Regulation (IVDR)', 28 June 2022, p8

71 Ibid

72 Ibid

73 Ibid, pp8-9

74 At 11, p1239

regulation as to make it easier for stakeholders to understand it, while also echoing the need for more cooperation between stakeholders, Notified Bodies, and the commissions during the whole legislative process.

Finally, a last recommendation could begiven in regard to interdependence. The conformity assessment procedure, as stated above, has not changed too substantially compared to the former directives outside of a reinforced designation and monitoring procedure[75]. This means that the issue of the relationship between Notified Bodies and manufacturers remains a strong issue. As demonstrated by previous studies such as the one conducted by the BMJ, where a fake implant managed to receive approval despite explicitly stating that the device was similar to three controversial implants[76], the industry has close ties to how Notified Bodies function, and often form close ties with them[77]. So much so, that in the US, only a fraction of the approved devices since the regulation first started in 1976 have been subjected to trials, and very few high-risk medical devices that were approved in the US have good quality research-based proof of efficacy and safety[78]. This is largely caused by the fact that Notified Bodies are for-profit, and are essentially contract partners with manufacturers, which raises potential conflict of interest concerns. For example, scholars have criticised the United States Food and Drug Administration's medical device division, accusing it that it is essentially in the control of device manufacturers whose fees contribute one-third of the division's budget[79]. The EU regulatory system is still very much suspect to this. As such, this relationship must be observed closely by the competent authorities, who should not refrain from taking corrective measures if necessary[80]. This can be especially true considering the phenomenon of Notified Bodies withdrawing from the market discussed above, as with more concentration, the stronger the interdependence of notified bodies and manufacturers will become[81].

75 Ibid

76 D. Cohen, 'How a fake hip showed up failings in European device regulation', BMJ, 345 (2012), p. e7090, 10.1136/bmj.e7090

77 At 11, p1239

78 Dhruva SS, Bero LA, Redberg RF. Strength of study evidence examined by the FDA in premarket approval of cardiovascular devices. JAMA. 2009;302(24):2679-2685

79 Lenzer J, Brownlee S. 'The FDA is still letting doctors implant untested devices into our bodies', 4 January 2019, The Washington Post

80 At 11, p1239

81 Ibid

3.5 REGULATION (EU) 2017/746 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 5 APRIL 2017 ON IN VITRO DIAGNOSTIC MEDICAL DEVICES AND REPEALING DIRECTIVE 98/79/EC AND COMMISSION DECISION 2010/227/EU

3.5.1 Executive Summary

As of 2021, 39,844 IVDs were circulated on the market[82]. Out of those, only 8% of them needed a certificate from a Notified Body under Annex II of the IVD Directive which are intended for self-testing[83]. In this environment, Regulation 2017/746[84] of the European Parliament and of the Council on in vitro diagnostic medical devices and repealing Directive 98/79/EC[85] and Commission Decision 2010/227/EU[86], seeks to achieve "a fundamental revision of that Directive is needed to establish a robust, transparent, predictable and sustainable regulatory framework for in vitro diagnostic medical devices which ensures a high level of safety and health whilst supporting innovation[87]." It is noted however, that such a fundamental transition does not come without significant challenges. Particular challenges that are highlighted amongst the industry largely pertain to the complex transition process that is far too lengthy for most businesses, but brutally costly for smaller manufacturers to the extent that it could pose threats to the public health sector in many ways, impacting factors such as innovation and seamless supply of IVDs in Europe.

3.5.2 Background

Within the EU, in vitro diagnostic (IVD) tests were regulated under the 1998 Directive 98/79/EC on in vitro diagnostic medical devices[88] (IVDD)[89]. It affected mainly the pre-market production of CE-IVD marked tests. The vast majority of IVDs in the EU were self-declared by the manufacturers themselves, and as mentioned earlier, only a fraction of them required certification by notified bodies, which were appointed by the national competent authorities in Member States[90]. Crucially however, all IVDs that were compliant with IVDD are not considered to be automatically compliant with the new Regulation, and as such, all will need to go through regulatory approval again, requiring a fresh evaluation by a notified body in order to remain in the market.

The preceding regulation to IVDR, the In Vitro Diagnostic Directive 98/79/EC was introduced in the later part of 1998 and compliance became mandatory on December 7, 2003. The Directive set out the regulatory requirements that

82 MedTech Europe Survey Report analysing the availability of In vitro Diagnostic Medical Devices (IVDs) in May 2022 when the new EU IVD Regulation applies, p6

83 MedTech, 'Transition to EU IVD Regulation (EU) 2017/746 and considerations for non-EU regulatory authorities on managing the impact to product registrations', May 2022,

84Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.), OJ L 117, 5.5.2017, p. 176–332, ELI: http://data.europa.eu/eli/reg/2017/746/oj

85 Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices. Official J Eur Commun. 1998;331:1–37

86 2010/227/: Commission Decision of 19 April 2010 on the European Databank on Medical Devices (Eudamed) (notified under document C(2010) 2363) (Text with EEA relevance), ELI: http://data.europa.eu/eli/dec/2010/227/oj

87 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards the transitional provisions for certain medical devices and in vitro diagnostic medical devices, COM/2023/10 final

88 These typically include devices such as HIV tests, blood gas analysers, immunoassay analysers, etc.

89At 3

90 Dombrink, Isabel, Lubbers, Bart R., Simulescu, Loredana, Doeswijk, Robin, Tkachenko, Olga, Dequeker, Elisabeth, Fraser, Alan G, van Dongen, Jacques J. M, Cobbaert, Christa, Brüggemann, Monika, Macintyre, Elizabeth, 'Critical Implications of IVDR for Innovation in Diagnostics: Input From the BioMed Alliance Diagnostics Task Force', HemaSphere, 6(6):p e724, June 2022.DOI: 10.1097/HS9.0000000000000724, p2

facilitated the free trade within the European Economic Area (EEA), which comprises the 27 European Union (EU) member states and Iceland, Liechtenstein and Norway as members of the European Free Trade Association (EFTA)[91]. The Directive applied to all IVDs sold in the EEA regardless of design or manufacturing origin. If the manufacturer originated outside the EEA they would still be responsible for ensuring that their device met the requirements set out by the Directive. The aim of the IVDD was to specifically address the safety, quality and performance of IVDs and to ensure that IVDs do not compromise the health and safety of patients, users and third parties and attained the performance levels specified by the manufacturer. Under the IVDD, the manufacturer was responsible for ensuring their products complied with the Essential Requirements of the Directive before affixing the CE marking and legally gaining access and free movement within the EEA, with a small minority of the devices requiring approval from an approved Notified Body[92].

The Directive would list out "Essential Requirements" to which all IVDs must comply before being placed on the market. These requirements would address the design, production, labelling and instructions for use. Not all the Essential Requirements will apply to all devices, and the manufacturer would determine which are appropriate for their device according to the manufacturer's intended purpose for their IVD. In addition, manufacturers would demonstrate compliance using an Essential Requirement checklist, which would consider each Essential Requirement and determine whether it is applicable or not. For example, a manufacturer could demonstrate that they have met the Essential Requirements is by complying with the relevant standards, which could include harmonised standards such as ISO 13485 for Quality Management Systems or ISO 14971 for Risk Management, which had been written specially to help manufacturers demonstrate compliance with the IVDD[93]. The Directive grouped IVDs into four categories according to the perceived risk associated with the relative danger to public health and/or patient treatment by an IVD failing to perform as intended. The diagram below from the British Standards Institution's guide to IVDD shows the classification and indicates where a Notified Body is required:

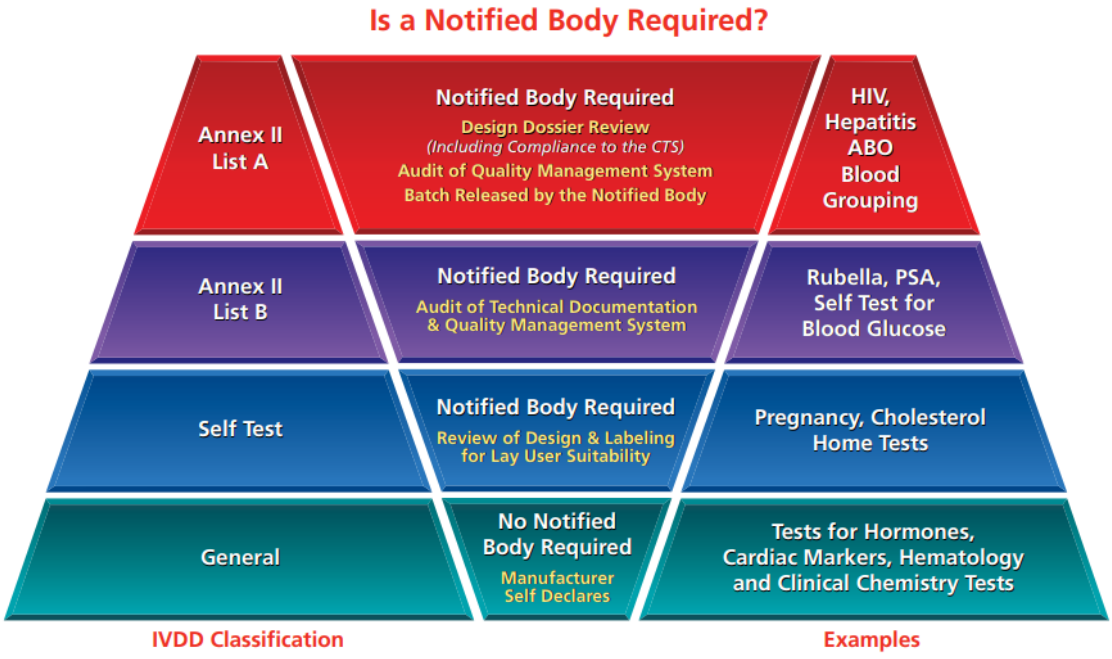

Figure 2

The Directive also included ongoing obligations for the manufacturers of IVDs with regards to experience gained in the post-production phase, including implementation of any necessary corrective actions. The manufacturer was

91 British Standards Institution, 'A guide to the In Vitro Diagnostic Directive', 2012, p2, BSI was An In Vitro Diagnostics Notified Body

92 Ibid

93 Ibid, p3

obliged to maintain a 'Vigilance System' and notify the regulatory authorities of any serious incident which could or had put a patient at risk, or required a product to be systematically recalled. An incident should be reported to the competent authority in the country where the incident has occurred. Manufacturers who did not have a registered place of business in the EU would have to designate an Authorised Representative to perform certain obligations. Such as being the first point of contact for Competent Authorities for issues such as vigilance or compliance cases, where they may be asked to provide documents to the Competent Authority on behalf of the manufacturer.

During the 2000s, it was becoming increasingly concerning that the IVDD was becoming outdated. Medical technology was quickly advancing and evolving rapidly, including IVDs. This would become obvious in 2010 while the IVDD was awaiting review. A scandal broke down involving Poly Implant Prothese (PIP) Breast Implants, which resulted in severe injuries and deaths due to the manufacturer using industrial grade silicone to make breast implants. While this was in violation of the regulations at the time, the medical device safety framework lacked sufficient checkpoints to prevent it from happening. The Medicines and Healthcare Regulatory Authority had completely failed to safeguard women who had received these implants despite first receiving a report of potential problems with PIP implants nearly a decade before the scandal had broken out, including a case of premature rupture of both implants in the same patient[94]. In light of this scandal, the EU introduced the IVDR as well as the EU Medical Device Regulation (EU MDR)[95] to try and prevent such a tragedy from happening again[96], and that case as well as others, such as Johnson & Johnson recalling toxic on-metal hip system were the cited reasons for the new regulations introduced by the EU by the European Medicines Agency[97].

The EU IVDR changes the current IVD registration process in several major ways, adding several more requirements and adopting new classification systems to the regulatory documentation. The major changes according to MedTech[98] include changes to technical documentation, classification, and the shift to a far more stringent approval process. To begin with, changes to technical documentation are quite extensive. These include changes to labels that give the manufacturer additional burdens such as the inclusion of a unique device identification and a notified body number added to the existing CE mark, but also force the manufacturer to include electronic instructions for use through a website, as well as the inclusion of new symbols created to assist patient tests and self-tests. IVDR lists them in Annexes II and III[99], requiring "clear, organized, readily searchable, and unambiguous manner" as regard to an IVD's technical documentation before manufacturers can even acquire their CE marking. The requirements are also quite extensive, requiring:

- Device description and specifications
- Reference to previous and similar generations of the device
- Package labelling and instructions for use (in appropriate languages)
- Product design and manufacturing information (including listing of all supplier and contract manufacturer sites)
- General safety and performance requirements (Annex I)
- Benefit-risk analysis and risk management plan
- Product verification and validation, including:
    - Specimen type/handling

94 Victoria Martindale, Andre Menache, 'The PIP scandal: an analysis of the process of quality control that failed to safeguard women from the health risks', May 2013, Journal of the Royal Society of Medicine

95 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance)Text with EEA relevance, ELI: http://data.europa.eu/eli/reg/2017/745/2017-05-05

96 Laura Maher, Niki Price, 'Ultimate Guide to IVDR for In Vitro Diagnostic Medical Device Companies', November 2022, Greenlight Guru

97 Zaide Frias, 'Update on EMA role in implementation of new legislation for medical devices (MDR) and in vitro diagnostics (IVDR)', 20 November 2019, Annual PCWP/HCPWP meeting with all eligible organisations

98 At 2, p6

99 At 15, p8

    - Analytical performance
    - Interfering endogenous/exogenous substances investigated
    - Clinical performance
    - Performance of self-testing devices/near-patient testing devices
    - Scientific validity
    - Pre-clinical and clinical data (performance evaluation report)
- Post-market surveillance plan and reports

Extensive documentation also extends to the new labelling requirements set out by the IVDR. he In Vitro Diagnostic Medical Devices Regulation (IVDR) includes new labelling requirements for in vitro diagnostic medical devices (IVDs) placed on the European Union (EU) market. These requirements aim to improve the accuracy, clarity, and comprehensibility of the information provided to users and patients about IVDs. The new labelling requirements under the IVDR include the following, among others[100]:

1. General labelling requirements: The label must include the name of the device, intended purpose, batch code, manufacturer's name and address, and other relevant information. The labelling must be clear, legible, and indelible.

2. Symbols and signs: Symbols and signs may be used on the label of IVDs provided that they are accompanied by a clear explanation of their meaning.

3. Instructions for use: The label must include clear and concise instructions for use, including any warnings or precautions for use.

4. Performance characteristics: The label must include the performance characteristics of the device, such as sensitivity and specificity, and any limitations on the use of the device.

5. UDI (Unique Device Identifier): All IVDs must have a UDI code, which allows the device to be identified and tracked throughout its life cycle.

6. Language requirements: The labelling must be in an official language of the EU country where the device is placed on the market, and in the case of devices with multiple languages, a language of the country where the device is placed on the market must be prominent.

Manufacturers are responsible for ensuring that their IVDs comply with these labelling requirements. The IVDR also requires that the labelling be periodically reviewed and updated to ensure that it remains accurate, up-to-date, and in compliance with the regulation.

Changes to the current classification system by adopting an entirely new one. For example, it divides IVD tests into 4 classes according to the personal and public risk they pose. Class A represents low individual and low public health risk, class B moderate individual and/or low public health risk, class C high individual and/or moderate public health risk, and class D high individual and high public health risk[101]. This new system determines how the EU will assess the IVD and adds new burdens to each device according to their assigned classification, such as the technical documentation required under Annex II, requiring new notified body certificates on the device under the new Regulation as well as various other information such as an information on product verification and validation[102].

The certification process will now become a lot more stringent, requiring issuance by a notified body. IVDs that require such a certification will require a new one, which affects the large majority of IVDs currently on the market, in compared to the miniscule amount required before. Depending on the classification and risk class of the device,

100 Ibid, p12

101 At 6, p2

102 At 2, pp98-99

a complex transitionary period has been set in place in order to facilitate the transition to the IVDR, with deadlines ranging from May 2025 to May 2027. As mentioned above, CE markings are required for an IVD before the product can be sold in any member state, and the only way to acquire one through the IVDR is with the involvement of a notified body, who will perform an audit of the manufacturer's quality management system (QMS), review the technical documentation mentioned above, before issuing a certificate. In regard to the QMS of an IVD, the manufacturer is required to address various aspects of the IVD's characteristics and strategy during its lifecycle as a product. These characteristics are listed in Article 10 of the Regulation[103], and include:

(a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for management of modifications to the devices covered by the system;
(b) identification of applicable general safety and performance requirements and exploration of options to address those requirements;
(c) responsibility of the management;
(d) resource management, including selection and control of suppliers and sub-contractors;
(e) risk management as set out in Section 3 of Annex I;
(f) performance evaluation, in accordance with Article 56 and Annex XIII, including PMPF;
(g) product realisation, including planning, design, development, production and service provision;
(h) verification of the UDI assignments made in accordance with Article 24(3) to all relevant devices and ensuring consistency and validity of information provided in accordance with Article 26;
(i) setting-up, implementation and maintenance of a post-market surveillance system, in accordance with Article 78;
(j) handling communication with competent authorities, notified bodies, other economic operators, customers and/or other stakeholders;
(k) processes for reporting of serious incidents and field safety corrective actions in the context of vigilance;
(l) management of corrective and preventive actions and verification of their effectiveness;
(m) processes for monitoring and measurement of output, data analysis and product improvement.

As noted from these requirements, post-market surveillance is a notable new addition of the IVDR as compared to the IVDD. The IVDR requires manufacturers to dedicate a high level of attention to monitoring a device's performance once it's on the EU market, imposing a requirement of a post-market surveillance (PMS) plan in order to facilitate that goal. Given the events that led to the creation of the IVDR, this is unsurprising. The minimum requirements of the PMS plan are set out under Annex III 1(b) of the Regulation[104]:

- Indicators and threshold values for continuous reassessment of the benefit-risk analysis and risk management (Section 3 of Annex I);
- Methods and tools to investigate complaints and analyze market-related experience collected in the field;
- Methods and protocols to manage the events subject to the trend report as provided for in Article 83, including the methods and protocols to be used to establish any statistically significant increase in the frequency or severity of incidents as well as the observation period;
- Methods and protocols to communicate effectively with competent authorities, notified bodies, economic operators and users; —
- PMS procedures to fulfil the manufacturers obligations laid down in Articles 78, 79 and 81; — systematic procedures to identify and initiate appropriate measures including corrective actions; —
- Trace and identify devices for which corrective actions might be necessary; and — a PMPF plan as referred to in Part B of Annex XIII, or a justification as to why a PMPF is not applicable.

It is also unsurprising that the IVDR also puts more stringent on Class C and D devices. While Class A and B devices will only require a post-market surveillance report, which would include a summary of results and conclusions

103 At 3

104 At 15, p10-11

regarding the factors laid out above, higher risk devices require some additional data. For the latter, a Periodic Safety Update report is required. It includes the data for lower risk devices, but builds upon them with key findings from the manufacturer, including a conclusion of the benefit and risk determination, data on sale figures, user demographics and populations, and the frequency of use of the IVD[105].

To facilitate a more coordinated information effort in that regard, as well as a more transparent environment, the EU has additionally set up EUDAMED, as part of both the IVDR, as well as Regulation (EU) 2017/745[106]. EUDAMED will act as a central repository for information on medical devices and in vitro diagnostic medical devices (IVDs) placed on the EU market, including their manufacturers, distributors, and authorized representatives and will facilitate the exchange of information between national competent authorities, the European Commission, and economic operators such as manufacturers, importers, and distributors[107]. EUDAMED will consist of six interconnected modules that cover different aspects of the medical device regulatory process, including registration of economic operators, registration of devices, certificates, clinical investigations, vigilance, and market surveillance. The database will allow authorized users to access information about medical devices and IVDs, including their technical specifications, conformity assessment, clinical evidence, post-market surveillance, and adverse events reporting. The implementation of EUDAMED was initially planned for May 2020, but due to technical difficulties, it has been delayed. The European Commission has proposed a phased implementation of EUDAMED, with some modules being available before others[108]. The new implementation date is expected to be announced soon, and once EUDAMED is fully operational, it will play a critical role in ensuring the safety and effectiveness of medical devices and IVDs in the EU market by providing a comprehensive and transparent database for regulators, manufacturers, and other stakeholders.

3.5.3 Impact and Challenges

By far the most impactful and controversial of these changes introduced by the IVDR, seems to be the changes introduced to the transitionary period to the IVDR from the IVDD. The new IVDR will require a tenfold increase in new certificates needed in comparison to the IVDD, as according to MedTech, 78% of devices will need a new certificate entirely, or to renew their current certificate, which represents a 736% increase in devices needing a certificate as compared to the old Regulation[109]. While 12% of IVDs have already been issued a new certificate needed under the new Regulation, with manufacturers predicting that at least 28% of IVDs will not be covered with a certificate by May 2022, and 60% of IVDs with ongoing certification or unknown status[110], this of course raises many concerns as regard to the capacity of the Notified Bodies responsible for granting these certificates during then regulatory process. While MedTech's survey data indicated that 21% of the manufacturers will not have any issues with completing the certification process, they expected that a portion of the manufacturers with unknown status are at risk of not being able to meet the certification deadline set under the IVDR, as the Notified Body's estimated approval date was 10-14 months, with the deadline for transition being only 9 months away at the time. As for the impact of these changes, according to MedTech, the greatest proportionate loss will come from SME manufacturers, who mostly make niche products and whose businesses are less likely to be able to endure loss of business that may occur due to the transition[111]. According to their survey, some 22% of IVDs will be unavoidably lost during the transition to the new IVDR, but SMEs will lose a portion equating to 29% of the market, almost double the 17% large manufacturers will endure[112].

105 Ibid

106 Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.), ELI: http://data.europa.eu/eli/reg/2017/745/oj

107 At 15, pp 12-13

108 MediCept, 'Eudamed Update: Implementation is Paused, MDR Compliance is Not', 29 April 2021

109 At 1, p6

110 Ibid, p7

111 Ibid, p6

112 Ibid, p6 figures 1 and 2

The EU did extend the transitional periods in January 2022 with the amending Regulation (EU) 2022/112[113] all the way to May 2025 to try and rectify this problem, however, allowing existing devices to stay on the market for longer and thus preventing a potential catastrophic deficit, such as the initial worries about Class I reusable surgical instruments like scalpels and scissors[114]. While in their latest survey[115], MedTech reports that 34% of devices expected under IVDR have CE-marking. 94% of large companies and 47% of SMEs have signed on with a Notified Body and started conformity assessment for their devices[116]. MedTech however is still not completely optimistic that the bottlenecks can be prevented by the new May 2025 deadline, as "51% of Class D legacy devices belong to manufacturers who do not have an agreement in place with a Notified Body"[117].

Moreover, potential risks in IVD supplies are not the only concern, as the IVDR also poses a challenge to IVD innovation in the EU. The MedTech survey also report an estimate of 17% of devices will be outright discontinued due to the cost of CE-marking under the new Regulation. However, despite 62% of respondents plan to prioritise the EU[118] for a first regulatory approval, which means that the EU remains a preferred market, they did report a 28% drop in manufacturers who would prioritize the EU for first product launches as well[119]. This means that the EU will see a delay to access of IVDs which were first launched in other jurisdictions around the world. Some other countries have also recently tried to rectify this, such as Switzerland, who changed its regulatory approval process to automatically approve devices that have already received approval in other jurisdictions[120]. The survey highlights the "Long, unpredictable, and inefficient conformity assessment timelines pose a significant financial and resource challenge for the industry. Many respondents provided comments explaining how long and uncertain timelines contribute to `blocking or delaying their innovation activities for Europe", with an average of 18 months needed to complete the technical documentation required to put a product in the market and financial difficulties in compliance for small startups and companies, as a huge allocation of resources is required to be diverted from research and development into conformity assessments for the IVDR[121]. Respondents of that survey also highlighted running performance studies in Europe as their third top concern, citing lack of predictable process, costs and time as the primary factors. While there are no details on performance studies published as of the time of writing, "the European medical devices database EUDAMED does not yet provide a centralised point for application of performance studies – instead, a patchwork of national rules applies[122]".

As it stands, while the EU has already followed some industry demands for deadline extensions, which seem to have been by far the biggest hurdle that it had to overcome. But as mentioned above, some work has to still be done in that regard. The most recent MedTech survey highlights just how much more work needs to be done by the Notified bodies[123], particularly in regard to the stress of their workload, which will see considerable overlap. In their October survey, they highlight their workload for May 2025:

- Notified Bodies have confirmed6 they have 544 applications open for various device classes, which should be considered as minimum ongoing work, given that many more applications should be expected by May 2025. Most of these current applications are for class B and C devices.

113 Published on 28 January 2022, ELI: http://data.europa.eu/eli/reg/2022/112/corrigendum/2022-02-03/oj

114 MedTech, 'Industry Perspective on the Implementation Status of the MDR/IVDR', 14.06.2019, p13

115 MedTech, 'Transition to the IVD Regulation – MedTech Europe Survey Results for October 2022', Public report February 2023

116 Ibid, p22

117 Ibid, p4

118 Ibid, p20

119 Ibid

120 Motion 20.3211, 'Für mehr Handlungsspielraum bei der Beschaffung von Medizinprodukten zur Versorgung der Schweizer Bevölkerung', accepted by the Swiss National Council on Monday 28 November

121 Ibid, p21

122 Ibid

123 At 12, p12

- . 1.101 class D devices require EU QMS and EU TDA certification. Class D will be a big portion of EU TDA certificates. Until relatively recently, many Notified Bodies either did not accept applications for class D or accepted the applications but did not proceed with their conformity assessment. 1.170 Class D devices require EU QMS and EU TDA certification. European Commission data from Notified Body survey provides the most complete picture of the number of IVDD certificates which will expire in 2023, 2024 and 2025 and how many devices they cover. According to this data, at least 1.551 IVD Directive certificates expire before 2025.
- 1.115i devices are expected to be first-launch or significantly changed and will need CE-marking in the next 12-18 months. It is unknown how many will require only EU QMS or also EU TDA certification.
- Conformity assessment for class C must start well in advance of May 2026, especially for self-tests, near-patient tests and companion diagnostics since this needs both EU QMS and EU TDA certification
- Oversight activities related to devices already certified under IVDR must be undertaken. This survey did not quantify that workload; however, it should represent considerable ongoing and annual work (including surveillance assessment, review of PSUR, review of summary of safety & performance, vigilance activities, management of change notifications, and more)

The second set of challenges cited by MedTech relates to that of SMEs and access to Notified Bodies. Currently, the majority of manufacturers who have yet to contract with a Notified body and started doing conformity assessments are SMEs. Without such a contract, it is unlikely that their devices will be IVDR compliant in time. Respondents indicate that 51% of Class D legacy devices are not covered by a Notified Body agreement[124]. More specifically, MedTech in their survey cite that:

- The Notified Body must audit one or more manufacturing sites, review at least one technical file for sampled devices and assess each technical file for devices requiring EU TDA certification. Each SME still requires almost three EU QMS certificates on average vs. just over five each for large companies. Given that there are many more SMEs than large companies, when all the companies are added together this means considerably more work for Notified Bodies to cover the remaining market.
- 53% of the SME respondents reported that they did not have access to a Notified Body. Most are waiting for their Notified Body to be designated. Other SMEs reported various difficulties in reaching an agreement with a currently designated Notified Body. A couple of SMEs comments noted that they did not (yet) need a Notified Body or that they expected they would still be in time to finalise certification later. Taken together, the data indicates that it may not be straightforward either for the manufacturer nor the Notified Body to find each other and sign an agreement, unless they already had existing agreements in place under the IVD Directive or for the purpose of ISO 13485.
- This survey did not evaluate the cost of transitioning to the IVDR. Nonetheless it should be noted that in their comments to various questions, SMEs often cited as barriers to transitioning to IVDR, the high investment needed for IVDR including resource and cost requirements together with a lack of predictability in scheduling conformity assessment.

Thirdly, another major challenge posed to the industry, as pointed out by the MedTech review, relates to the specific challenges for certifying all class D devices on time[125]. MedTech states that as of October 2022, three certifications for class D IVDs had been issued[126], and that many Notified Bodies have only just started conformity assessment. The biggest fear that this causes is that manufacturers might seek other ways to circumvent the lengthy and unpredictable, and complex regulatory process of the IVDR for the high-risk devices that fall into Class D, and look into alternative solutions and strategies, such as taking these devices out of the market altogether, or downgrading these devices, their scope and their features so they fall into a lower classification, and thus be subject to less scrutiny under the IVDR.

124 Ibid, p13

125 Ibid, p13-14

126 Ibid, 14

These challenges pose a great risk to the public health sector. It is imperative that critical IVDs and high-risk tests remain seamlessly available across the EU in order to safeguard public health. IVDs are needed to screen blood supply, check cells and organs for transplant operations and are vital in combatting disease outbreaks, as seen from the still recent COVID-19 (SARS-CoV-2) pandemic.

3.5.4 Alternatives and Recommendations

Considering the nature of IVDs, the most important comparisons to draw with the IVDR are the equivalent regulations in the USA. A brief look at the regulatory process in the USA, reveals that the changes introduced under the IVDR are more aligned to that process, and the general international standards. The FDA is responsible for the IVD regulation in the USA, and their regulatory process echoes a lot of the same characteristics we see adopted into the IVDR. The FDA classifies medical devices, including IVD products into three separate classifications according to the level of regulatory control that is necessary to impose on them in order to assure that they will be secure and effective[127]. The manufacturer has to submit a Premarket Notification (510(k)) to the FDA in order to demonstrate that the device to be marketed is at least as safe and effective, that is, substantially equivalent (SE), to a legally marketed device[128] that is not subject to premarket approval (PMA)[129]. The FDA will then proceed to make a decision and evaluation on the device according to the bias or inaccuracy of the new device, the imprecision of the new device and the analytical specificity and sensitivity. The manufacturer can demonstrate the security and effectiveness (substantial equivalence to another legally U.S marketed device) of the device through various studies, and seek to prove that "a device has the same intended use as the predicate; and has the same technological characteristics as the predicate; or has the same intended use as the predicate; and has different technological characteristics and does not raise different questions of safety and effectiveness; and the information submitted to FDA demonstrates that the device is as safe and effective as the legally marketed device"[130]. While the claim of substantial equivalence might sound like an uphill battle for new devices, does not imply that the new and predicate devices need to be identical. The FDA first establishes that the new and predicate devices have the same intended use and any differences in technological characteristics do not raise different questions of safety and effectiveness. FDA then determines whether the device is as safe and effective as the predicate device by reviewing the scientific methods used to evaluate differences in technological characteristics and performance data. This performance data can include clinical data and non-clinical bench performance data, including engineering performance testing, sterility, electromagnetic compatibility, software validation, biocompatibility evaluation, among other data[131]. Similar IVD regulation processes can also be found in other major economies and countries, such as Canada[132].

As regard to industry recommendations, MedTech recommend a reduction of time-to-time certification and increasing predictability of the conformity assessment system[133], as it is what they have found to be the weakest link in the transitionary process into IVDR, as mentioned above. Even with the EU extending the initial deadlines, many manufacturers that were surveyed responded that ""It takes an average of 18 months between declaration of completed technical documentation and final CE-mark. This has a negative impact on the availability of new technology to patients. A further slowdown in innovation is caused due to need to direct available resources to IVDR compliance program for existing products over innovation projects[134]." Specifically, they cite particularly lengthy pre-review phases, and highly irregular review phases. As regard to the pre-review phase of the regulatory process,

127 The Code of Federal Regulations lists the classification of existing IVDs in 21 CFR 862, 21 CFR 864, and 21 CFR 866

128 Under 21 CFR 807.92(a)(3)

129 U.S Food & Drug Administration, Overview of IVD Regulation, https://www.fda.gov/medical-devices/ivd-regulatory-assistance/overview-ivd-regulation

130 Ibid

131 Ibid

132 Government du Canada, 'Guidance Document: Guidance for the Risk-based Classification System for In Vitro Diagnostic Devices (IVDDs)', 2016-10-07

133 At 34, p15

134 Ibid, p21

MedTech specifically recommends that any "more than 3 months between receiving the application and starting the review should be considered excessive[135]" The reasons cited are as follows:

- The fact that respondents are reporting that 58% to 73% (EU QMS) and 59% (EU TDA) of them typically took more than 4 months to pass from application to review, should be tackled. This is also confirmation that it makes sense to invest in implementing 'structured dialogues' (MDCG 2022-14, action 15). By making this phase more efficient and supporting manufacturers to successfully pass their Notified Body's application completeness check, the system could save time and resources.
- Other factors may contribute to the length of the pre-review phase, such as long or unpredictable response times from the Notified Body or manufacturer. Some respondents noted that completion of complex application forms took time.
- In principle, the manufacturer is responsible for categorisation of their devices into device category or generic device group. Changes were needed 45% of the time to the device category or generic device group during the pre-review stage. This means that applications would need to be reworked, sampling plans re-done and Notified Body resources reassigned. It also indicates that the process of grouping of devices may be open to interpretation. It could be helpful to clarify or simplify how devices are grouped or allow structured dialogues (MDCG 2022-14, action 15) to build understanding between Notified Body and manufacturer of how their devices should be grouped.

They continue the recommendations in regard to the review phase too[136]:

- Survey data shows that the Notified Body is not making a difference between reviewing B and C applications. This means that the system is not investing in prioritising resources by the risk class. Evaluation of the device should be done against the general safety and performance requirements.
- In many cases, the timeline for the 2nd application increased when compared to the 1st application submitted by the same respondent. Some respondents noted that this increase was due to reviewers spending more time during the 2nd application checking requirements against a greater amount of available MDCG guidance. Given that most MDCG guidance is published in areas which are not directly related to the General Safety & Performance Requirements, this is indicative that the system resources might be re-focussed on device safety and performance rather than other areas.
- Some respondents noted that inconsistency between reviewers including on what had been agreed as an interpretation or on number of questions per product. Such inconsistencies could perhaps be addressed by Notified Body internal practices or best practice.
- Other factors may contribute to the length of the review phase, such as long or unpredictable response times from the Notified Body or manufacturer. Some respondents commented that the review time was slow and sat with the Notified Body most of the time. Also, checklists used by Notified Bodies were seen as contributing to the length and complexity of the process.
- While respondents did not comment, it is possible that some applications were more complex or needed more attention, which contributed to longer review timelines.
- Although COVID travel restrictions are no longer in place, the ability to conduct hybrid audits may cut down on the travel time needed and improve review times.

Overall, it seems that despite some efforts, access to notified bodies and the time required for said notified bodies to actually certify an IVD, combined with the immense workload of having to re-approve all previous devices already on the market are the biggest growing pains of the IVDR regulation. Even once there is a positive recommendation to issue a certificate, the actual issuing of the certificate by the Notified Body to the manufacturer can take months[137]. While the IVDR seems to address many of the issues that led to its creation, with a wide variety

135 Ibid, p19

136 Ibid, pp19-20

137 Ibid

of mechanisms to survey the market and prevent future regulatory failures, it is clear that the transition to the new model has had a rocky start, with issues that pose a threat to innovation and seamless supply of IVDs in Europe.

3.6 Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance

3.7 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union

3.7.1 Executive Summary

The Regulation rests on four cornerstones: *i)* the outright prohibition of data localization measures except for those grounded on public security yet respectful of the proportionality principle (Article 4(1)), in line with the procedural requirements established in the same provision; *ii)* a cooperation mechanism incentivizing the cross-border exchange of non-personal data among competent authorities based in Member States (Articles 5 and 7); *iii)* development of self-regulatory codes of conduct facilitating interoperability and open standards in relation to the switching of service providers through the porting of data in machine-readable format from one provider to another; iv) information requirements to professional users and certification schemes (Article 6).

This executive summary leaves apart crucial aspects which underpin the potential of this Regulation. Firstly, the extension of the public security exception under the EU framework, whose applicability is subject to a "necessity test" and follows the interpretation of the CJEU (Recital 19); secondly, full understanding of the concept of non-personal data and the interdependence from the GDPR, restricting the applicative sphere beyond Recital 16; thirdly, the role of public authorities and undertakings, that are still in full control of their outsourcing practices, as no obligation exists with regard to mandatory flows of non-personal data under the present Regulation (Recitals 13 and 14); lastly, the boundaries of the concept of "abuse", referred as to a source of interim penalties when users refuse to provide data to competent authorities (Recital 28, Article 5(4)). In particular, the most relevant points touched yet still clouded in indeterminacy by looking at the text are the following ones: *a)* the prevalence rule to be applied once that a dataset is mixed, containing both personal and non-personal data, as the Regulation should only apply to the part of the dataset made of non-personal data, yet most of the times the two parts are inextricably linked; *b)* the threshold to apply the exception based on public security for the introduction of Member State law-based data localization requirements, that is eager to create a discrimination between cross-border exchanges of non-personal data in B2B and B2G/GtG case-scenarios; *c)* the concept of abuse undertaken by the user upon request of providing non-personal data to competent authorities seeking to exchange such data on a cross-border level. Apart from these unclear aspects, there is growing concern about the structure and non-mandatory character of Article 6, that mildly suggests the adoption of codes of conduct about open standards and interoperability.

This rule concerns the most crucial policy drivers behind the 108 Regulation. In fact, the same was enacted for the very purpose of enhancing competitiveness within the market of IoT services, with a view to fueling the emergence of EU SMEs and startups in the ICT field, by avoiding vendor lock-in practices and other barriers to switching and portability of non-personal data contained in digital services, ultimately impairing the Union-wide dissemination of cloud computing systems.

As this vacuum is likely to be fulfilled by data- and sector-specific regulations (e.g., EU Health Data Space) and all-encompassing interoperability standards for public sector entities ("Proposal for an Interoperable Europe Act"), it

can be said that the present Regulation largely failed at addressing the quandaries mentioned above or, at least, needed complementary legislative measures on a data- and sector-specific level.

3.7.2 Background

As summarized by the Impact Assessment, the policy drivers of the Regulation are multiple and mainly revolve around the necessity of *i)* improving data mobility within EU, removing perceived and existing legal barriers based on Member State law data localization restrictions, that lead to a climate of legal uncertainty and increase fragmentation, ultimately hampering the objectives of the internal market; *ii)* ensuring free flows of non-personal and above all industrial data across Member States, thus increasing trust in the development of an Union-wide data economy, whilst, at the same time, allowing the persistence of supervisory control by competent Data Protection Authorities (DPAs) at the national level; *iii)* fueling switching and portability practices, that are key in order to boost the emergence of a cloud market in the EU, benefitting SMEs and startups operating within the field; *iv)* enhance trust in a harmonized legal framework, avoiding fragmentation in terms of Member State lawmaking, as extensively spelled out in policy reports portraying the sector-specific data localization requirements enacted by law in the various Member States. The Regulation was mainly enacted to address the conundrums summarized above, with a view to facilitating the cross-border movement of non-personal data, simultaneously improving access and data storage both between CSPs and in-house IT systems and between CSPs across EU.

In particular, the Regulation was set within the context of the DSM Strategy, announcing that a "European Free flow of data initiative" would address the existing regulatory and contract-based restrictions to free movements of non-personal data, with a view to repealing the unjustified ones based on location. The core principle is to foster EU policymaking under the label of a unitary principle of free movement of data within the EU, as a corollary of Article 36 TFEU (Communication "Building a European Data Economy"). It follows that a "principle of availability of certain data for regulatory control purposes" should be inferred and held applicable "also when that data is stored in another Member States", by taking into account "Member States' legitimate interests on secure storage of data." As a paradigmatic example, the present Regulation was enacted in order to foster the porting of data from an nation-based IT environment to another, overcoming the existing barriers to cloud services developed on a cross-border level. In fact, cloud computing systems are cross-border by nature and keeping them at a national level brings additional costs to firms, which can be prohibitive for smaller enterprises and startups, leading to lock-ins and hampering the competitiveness of EU SMEs.

As mentioned in the Impact Assessment, Article 22 GDPR, allowing data subjects to retrieve their personal data back in the case of transfers from one data controller to another, does not apply in B2B relationships. For this reason, the position of professional users and developers of further digital devices, keen on developing cloud computing systems, is underpinned by way of comparison with customers/data subjects of the same services, potentially creating a discrimination between B2B and B2C porting scenarios. This, in turn, risks fueling monopolization practices in digital markets, market failures and distortions in key sectors of EU data economy, such as cloud services and ICT in general. Moreover, it must be mentioned that, once accurately anonymized, personal data are turned into non-personal ones (Recital 9), whose lack of transferability for business purposes risk causing a loss of net incomes for a huge number of businesses. Despite grounded in security reasons, it was recognized by both literature and policy reporting that stakeholders rely on the inaccurate assumption under which a national data storage guarantees a higher degree of security from cyberattacks, which, in fact, is not the case. Rather, EU countries where businesses and public bodies can afford a high level of data security may benefit from fragmentation, rather underpinning Member States where procedural compliance costs are too high to be borne and where, as a consequence, a market of certain services is unlikely to flourish.

The relevance of the problem at the core of the Regulation stems from the inherently **ubiquitous** nature of data and, in turn, from the inherently **cross-border character** of data processing activities. In particular, this Regulation is a response to the obstacles created by legislation, and/or perceived due to the patchwork of data-related legal solutions, to **"data mobility"**, referred as to "the degree in which data can be (re-)located to different IT-systems, regardless of the physical location of such systems in the Union or the owner of such IT-systems, which

might be the data holder himself or a data storage and processing service provider/CPS". Obstacles are listed in the following way:

(1) Legislative and administrative restrictions (administrative and legislative constraints, based on data localization requirements developed on a Member State level)
(2) Legal uncertainty (perceived data localization requirements, complex legal frameworks with consistent degree of ambiguity with regard to the definitional interplay between personal and non-personal data)
(3) Lack of trust (insufficient data availability for EU regulators, compliance concerns and data sovereignty)
(4) Vendor lock-in (among IT services-producers)

Leading to:

1) Lack of innovative potential
2) Lack of operational efficiency
3) Inefficiency in the data sector
4) Market distortions

In general, when a firm working with data has to decide whether to store or further process them outside from the origin country, it has to make a decision based on the following questions: "*are there regulatory requirements which would be breached if data was transferred to another country*?". If no, "*do our customers have binding contracts to store their data in particular locations/countries*"? If no, "*are there public concerns around data travelling outside a country which could lead to loss of market share*?". If to one of these questions, the answer was no, the decision would have inevitably been in the negative, thus hampering the creation of a Union-wide digital market. In fact, when a for-profit company decides on whether to adopt a specific business decision, it firstly looks at "market size and potential profitability on a macro level", therefore turning to analyze "legal, regulatory and binding rules" affecting their position in first instance.

Before the enactment of the present Regulation, it is noteworthy that many national statutory laws mandated the country-based processing of different types of datasets, in accordance with a mostly sector-specific and strictly Member State law-based concept of "public interest". This is likely to vary from one country to another without respect of the proportionality principle. In fact, most of these regulations end up covering non-critical data as well, thus resulting in a legislative intervention that is excessive in relation to the policy aim pursued. In this respect, the Impact Assessment recalls that no EU law puts a ban on these types of localization measures, except for an intrinsic contrast that can be found with regard to cross-border portability rights and rules. Yet, these rules are content- or data-specific, therefore unlikely to have an all-encompassing impact such as the one pursued by the present Regulation.

Specifically, these legal constraints based on location, from which other "perceived" and "indirect" barriers might follow, are generally referred to as **data localization requirements**, and are mostly based on confidentiality, data security and integrity or, alternatively, the necessity of submitting access requests to supervisory authorities due to the public relevance and/or sensitive character of the dataset at issue. The high level of fragmentation and widespread character of these regulatory or merely perceived requirements was extensively discussed in a high number of policy reports. For example, Law n° 80-538 dated 16 July 1980 (French Blocking Statute) under French law put a ban on communication of all data affecting "sovereignty, security or any other public order or essential economic interest of France", except for cross-border exchanges of data based on rules contained in international treaties, agreements and specific regulations). Along the same lines, a Ministerial Decree issued in November 2011 prohibited disclosure of state secrecy information outside France and to others than French citizens except for secured transmission networks, military or diplomatic special ways of communication. Additional bans in this regard concern public archives covering digital public bodies or undertakings' data (Article L111-1 of the French Cultural Heritage Code), with the effect that these datasets cannot leave the country except for specific approval of the Ministry of Culture and through a cloud service which ensures that data processing takes place within the French territory, in a way that is necessarily compliant with French rules in relation to public record making. A specific accreditation procedure concerns French patients' data under Act 2002-303 released on 4th March of 2002 on top of the French Code of Public Health. Accordingly, healthcare entities and organizations must use an Hosting Service Provider accredited by the State and cannot use their own electronic storage service. The level of fragmentation can be captured by the fact that these regulations are strictly data-specific and therefore reveal a different kind of sensitiveness towards public interest in storing specific types of data in different Member States. In contrast with

France, where particular attention is drawn to health, cultural heritage and security data, in Germany, the policymaker has addressed rather cautiously the issue of cross-border transfers of tax and business data, by establishing an outright prohibition in this regard. Section 146 of the Tax Code has established that all companies are forced to pay taxes and keep their book records in Germany, except for holdings and transnational firms, which, by the way, have to face many requirements and procedural constraints as well. Section 14 on Value Added Tax also settles that companies legally located in Germany should store their invoices therein, while Section 41 of the Income Tax Act provides that all employers must keep their payroll accounts within the business place. In addition to that, sensitive information held by German federal institutions (e.g., sensitive data related to IT infrastructures, confidential or other business data somehow related to public bodies and undertakings within the country) can be processed through cloud services only within the German territory, in full respect of confidentiality agreements signed thereof. Financial and company data are also a hot issue in Luxembourg and Spain. In Luxembourg, this is only an indirect barrier, because cross-border transfers of banking data are abstractly possible yet discouraged in the light of the burdensome procedural compliance rules established through private ordering. Rather, local requirements are imposed by Luxembourgish company law with regard to specific company documents, such as lists of shareholders, accounts, merger transactions etc. In Spain, confidentiality concerns hindering cross-border transfers of non-personal data come from contract normally concluded between the Ministry of Defense and companies operating under their control. As a result, data cannot leave Spain. Although specific limitations do not directly concern financial data, banks are obliged by law to detail a plan of outsourcing when they are willing to transfer customary banking data outside from the national territory.
Beyond the proliferation of data-specific regulatory schemes in the EU, discouraging cross-border transfers, other quandaries for open data flows come from the fact that data ownership is often unclear and no regulatory instrument at the EU level clarifies the threshold after which it is possible to deem a dataset protectable through copyright, trade secrets or other proprietary rights such as *sui generis* database rights. Despite this issue was not even touched by the text of the Regulation, the same was stressed by the Bird & Bird policy report for the EU Parliament as a key aspect to be addressed in order to boost data-sharing effectively at the EU level.

The few remarks made by the CJEU in this regard need to be carefully analysed. In fact, in *UsedSoft*, the CJEU implied that “there is a specific ownership on tangible goods like software downloaded via internet” and, for this reason, a digital exhaustion rule for IPRs over such software cannot apply after the first sale as if it was for tangible goods. This stretches the level of protection beyond expected, pushing towards the “propertization of data” as such. The same principles, issued in the context of the limits to IPRs yet extendable to the issue of data ownership in general, were reaffirmed in *Tom Kabinet*, a later decision cutting off the possibility of developing a second-hand market of digital copies of copyrighted books. Apart from that, lax requirements on IP protectability, such as those resulted in the seminal cases *Magill* and *IMS Health*, are proven to create a regime of de-facto data ownership in favor of some dominant firms. As a result, problematic competition law issues arise, therefore triggering the application of the “essential facilities doctrine” with regard to IPRs over datasets and software programs. This amounts to a distortion of competition law rules from their purpose, while, at the same time, outlining the necessity of a more proactive legislative measure with regard to the interplay between open data and IP constraints.

In order to avoid costly proceedings before EU courts and authorities, the Regulation fosters free flows of non-personal data, implicitly yet too mildly suggesting the accommodation of IP rules to such purpose. In the light of the existing data ownership-alike regime sparse in the EU, it is unlikely that a broad application of the Regulation will enhance the development of a prosperous EU data market.
In a regulatory landscape where the Data Act and the Data Governance Act, as well as the Proposal for an Interoperable Europe were yet to be conceptualized, the present Regulation was seen as the first step towards the development of best contractual practices to encourage B2B data sharing, leading to functional de-facto access regimes in favor of national DPAs (i.e. public authorities only) on a cross-border level, also encouraging best contractual practices and self-regulatory codes of conduct with regard to mutual recognition of interoperability standards, data-sharing standard contract terms and cross-border FRAND licensing of protected datasets. In this sense, the present Regulation was to be intended as a still too weak policy lever towards the development of data-specific pools, such as health data pools, addressing the needs of specific market sectors, e.g., eHealth, IoT and ICT technologies and FRAND licensing in the same regard.
to sum up with the main obstacles to free flows of data are due to:

- Member State law data localization restrictions – which are partially addressed by the regulation
- Intellectual property rights/data ownership regimes – which are not addressed by the regulation

This results in:

- High switching costs, leading to lock-in effects and increasing costs on consumers and SMEs
- Competition law issues
- High procedural and administrative costs
- High IPR licensing costs
- Concentration of operational efficiency on few companies based on one Member State

As an example, which is also listed in the Impact Assessment of this Regulation, we can take the proposal brought to the Roundtable "banking in the digital age", organized by the Commission in November 2016, where the EU Banking Federation proposed the adoption of a principle of free flow of data with a proper legal basis, forwarding the case scenario of a bank willing to increase efficiency and reduce costs through outsourcing of customary banking data. As it can be inferred from the examples of Spain and Luxembourg cited above, there are many statutory laws that prohibit so tout court on a national level. Apart from that, banks are usually reluctant to the establishment of an IT data infrastructure operating on a cross-border level, although this may avoid duplication of IT data and thus improve efficiency to a significant extent. Despite providing documents that ensure that there are low risks for loss of security, the proposal was quashed because of lack of full approval by national central banks. As a result, an opportunity to reduce cost expenditure and discrimination among the levels of operational efficiency across EU was lost.

The policy drivers of the Regulation mentioned above are also sparsely yet not fully recalled within its very same text. In this sense, the wording of some Recitals is telling.

- **Recitals 2, 18, 21, 23**: full potential inherent to data aggregation, reuse, organization and cross-border processing should be exploited by removing the main two obstacles to data mobility: data localization requirements and vendor lock-in practices put in place by the private sector, with the effect that switching becomes economically and technically unfeasible;
- **Recital 11**: need to repeal fragmentation, lack of predictability and legal uncertainty with regard to free flows of non-personal data through a principle-based approach, yet respectful of national security as interpreted under Recital 19 in a restrictive manner;
- **Recital 24**: lack of trust towards supervisory power of DPAs on a cross-border level, that should be overcome by fostering cooperation rather than through invalidity clauses;
- **Recitals 29, 30**: pro-competitive trait of open data, interoperability and data-sharing policies, leading to a situation where users are encouraged to switch from one service provider to another without hindrance, thereby fostering the creation of a market of digital and data processing services;
- **Recital 31:** ban on vendor lock in business practices, preventing porting on a national or cross-border level.

3.7.3 Analysis of specific issues

These are the problems that emerged from an analysis of the regulation by focusing on a data/product/service access point of view

- **Vendor lock-in practices (partially addressed)**: switching from a provider to a new one is economically, contractually or technically unfeasible through contractual terms and/or monopolization practices;
- **IPR protection (unaddressed)**: datasets are partially or entirely covered by IPRs, such as trade secrets, copyright or *sui generis* database rights, which exist on a separate basis or in combination, thereby putting an additional and unaddressed obstacle to free flows of non-personal data

- **Combination of personal and non-personal data within the same dataset (unaddressed)**, which is further complicated by the CJEU-led broad reading of the concept of personal data and from the blurred boundaries with the one of non-personal data (no clear prevalence rule and high risk of refraining from exchanging data due to the high compliance costs posed by the GDPR);
- **Remaining regulatory data localization requirements (partially addressed)**, based on a satisfactory reading of the public security exception under the present Regulation, which is specifically the case of state-owned and other types of "Public Sector Information" (PSI), such as national archives and other confidential information;

a) The following are the problems emerging as regards **data\product\service usage**
   - **Vendor-lock in practices** (as above)
   - **Competition issues and concentration of market power within one service (provider (unaddressed)**, exacerbated by lax IPR protection requirements, so as EU courts are forced to apply the essential facilities doctrine and issue judge-made compulsory licensing rules compensating for the lack of access regimes and the restricted scope of portability rights across EU, also due to the "inextricable link" between personal and non-personal data within the same dataset;
   - **Cybersecurity/data security policies (left to relevant legislation)**

- The following are the problems emerging as regards **data\product\service sharing**
  - **B2B v B2G disparities (unaddressed)**, based on a different reading of the national security exception, leading to a possibility of further constraining B2G data-sharing
  - **Licensing malpractice both outside and within the IP field (unaddressed)**, as the elaboration of open data standards and standard contract terms is left to private ordering without any further guidance;
  - **National law-based stringent reading of national public security concerns preventing data exchange on a cross-border level (partially addressed)**

- The following are problems emerging as regards **data\product\service 'ownership'**
  - **Lawful basis/more caution may be required for third party transfers of "PSI" (unaddressed)**, although the Open Data Directive (ODD) sets a Union-based procedure for access, which, however, does not amount to a "positive" access right/regime operating on a national level, thus leading to uncertainty/fragmentation when data are owned by public bodies and undertakings and shall be used for cross-border processing in order to develop data storage services;
  - **National security concerns (as above)** when data are owned by public authorities and subject to confidentiality complying with the security exception and the proportionality principle under the present Regulation;
  - **IPR protection (as above)**;

- The problems emerging in case of different **purposes (e.g. research, medical treatment, etc.)** are the following. Firstly, there is a fragmentation and different regimes in relation to data localization requirements when in place in compliance with the exception based on public security can have an impact on the extent of cross-border exchange of non-personal data according to the **purpose** for which such processing has been undertaken. Moreover, many data-specific regulatory interventions have been undertaken at the EU level, complementing and specifying the present Regulation. Yet, this leads to a different treatment for the various types of non-personal data, with the effect that **cross-border exchange can become more or less feasible** according to the **structure of the dataset** at stake. In fact, some categories of data are particularly difficult to be anonymized with an appropriate level of security, thus hardly ever classifiable as non-personal under the present Regulation, because re-identification is always possible. This is, e.g., the case of **health data** that, however, are eager to be subject to the EU Health Data Space if the Proposal is approved, which furthers and partially tailors the objectives of the present Regulation to the specificities of the health sector. In this sense, the all-encompassing ambition underlying

this legislative measures can be deemed obsolete and mostly replaced with sector-specific regulatory and legislative measures, which address ownership, access and transfer-related issues on a separate and data-specific basis. In relation to **data inferred from IoT services**, the Proposal for the Data Act has been released, establishing an exception under Article 35 to *sui generis* database protection and thus addressing one of the main obstacles to free flows of non-personal data, that persisted despite the interested Regulation. With regard to this particular category of data, there might be more room for freedom while exchanging data on a cross-border level. Yet, the optional nature of this rule is likely to hamper its potential to a significant extent and lead to further fragmentation according to the different readings of national courts. Regarding **PSI access and reuse**, the Data Governance Act establishes a complementary policy framework. By introducing the concept of "data altruism" among data cooperatives and businesses, data-sharing is encouraged, in full compliance with a rationale based on "data philanthropy", that dates back to the policy spirit behind the present Regulation and enshrined in Article 6. Advancing its core principles within the framework of public sector data, the Data Governance Act aims at promoting B2B and B2G sharing licensing practices, especially for scientific research and other valuable policy grounds in the light of the compatibility by default rule enshrined in the GDPR itself. Along the same lines, the issued Proposal for an Interoperable Europe is also introducing interoperability standards for public sector information that is eager to advance cross-border processing consistently.

As a consequence, the following are the main aspects affected by the **structure of the dataset**:

- Risk of re-identification
- Compliance duties on data controllers requiring a certain degree of interoperability/data-sharing (**positive**) and/or security (**negative**)
- IPR carve-outs
- Cybersecurity policies under the national implementation of NIS I and II Directives

See below (Impact and interplay with other legislative measures enacted at the EU level).

3.7.4 Impact of legislation and interplay with other legislative measures enacted at the EU level

3.7.4.1 Impact of the legislation

The present Regulation aimed at and was likely to produce:

- More cooperation between national DPAs in terms of cross-border exchange of non-personal data
- More competitiveness in the ICT and cloud services market
- More consumer choices in the above mentioned market fields across EU
- Incentive to remove unjustified data localization practices and establish access regimes increasing the amount of data in the hands of DPAs
- Incentive to introduce penalties for abuses arising from refusing to provide relevant data without relevant justifications, thereby eliminating de-facto ownership data regimes
- Incentive to adopt open data policies, standard data-sharing contract terms and codes of conduct regulating B2B and B2C relationships on a national and cross-border level
- Incentive to clarify the definitional boundaries between personal and non-personal data at a national and CJEU level
- Incentive to repeal too lax IPR protection requirements establishing de-facto ownership regimes and therefore hampering cross-border flows of non-personal data

- Incentive to adopt FRAND, statutory and compulsory licensing terms for datasets including protected data that are eager to constitute industry standards and thus are key for the EU digital market

3.7.4.2 Interplay with other legislative measures

EU Health Data Space: the Proposal aims at facilitating e-health services and cross-border exchange of health-related exchange materials s, also through the establishment of a cross-border data infrastructure for primary and secondary use of electronic health data, with the effect of complementing the objectives of the present Regulation. In this sense, a cross-border exchange of highly sensitive and personal data will be provided, thus bypassing one of the main drawbacks unaddressed by the Regulation, which is the narrow objective scope thereof.

As Article 34 establishes a lawful basis for specific purposes underlying a legitimate secondary use of health and genomic data, there is no need to refer to the Regulation at issue as the sole basis to enhance cross border (further) data processing of anonymized health data, with high risks of re-identification, high compliance costs and reduced competitiveness in the e-Health sector. Yet, for purposes other than those enlisted in Article 34, anonymization remains the safer measure to be adopted to allow further data processing and secondary use of health data, in full compliance with data minimization. The scope of further data processing is narrowly defined by Article 46 of the same Proposal, establishing the requirements and procedural constraints to which the applicant is subject while submitting a request for secondary use of health data to the appointed authorities ("health data access bodies"). The specificity of the "data permit", once issued, is particularly constraining, as, on many occasions, purposes related to scientific research, are unlikely to be predictable in first instance. In these "grey areas", where secondary purpose is strategically undefined, a subsidiary application of the Regulation on free flows of non-personal data can lead to circumvent the burdensome proceedings imposed under the EU Health Data Space.

***Sui Generis*, Trade Secrets and Software Directives**: IPRs still constitute an insurmountable obstacle to data exchanges on a cross-border level, therefore discouraging full implementation of the present Regulation. The so-called Database Directive is the main source of limits based on exclusive rights, as most of datasets are at least protected through sui generis rights, whose boundaries have been stretched so far by the CJEU so as nearly to cover data themselves. In particular, Article 7(1) of the Database Directive (DbD) provides a property right to the maker of a database who has made a qualitatively and/or quantitatively substantial investment in the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of whole or substantial part of such contents (sui generis database right). The CJEU read both the concept of "re-utilization" and "extraction" in a broad manner, with the collateral effect of creating a de facto ownership regime in favor of *sui generis* database holders, who are not compensated for the creative effort but rather building on their capability of arranging and storing a huge amount of data. Exceptions are provided on the grounds of public security and/or for research/teaching purposes under Article 9 DbD, thus in a case-scenario where the very same present Regulation is unlikely to apply, whilst the national public security exception thereof would.

With regard to the scope of database *sui generis* rights, the CJEU specified its contours throughout the years and held that (**i**) the act of arranging an independently collected amount of data is encompassed by the broad concept of database under Article 7 DbD (*Fixtures Marketing*); (**ii**) the human, economic and technical efforts made by the database maker are the main relevant criterion to establish whether substantial investment has been made in the arrangement of a dataset eligible for protection under Article 7 (*British Horseracing Board*) (**iii**) the act of making a copy through transferal of the contents from a database to another may very well infringe *sui generis* rights (*Directmedia Publishing*), with the effect of impairing cross-border data porting and switching from one digital provider to another through a digital copy of the dataset detained by the first data controller; (**iv**) "re-utilization" of a *sui generis* protected database to determine whether an infringement has occurred depends on whether the original dataset can be otherwise/alternatively accessed through the new service including the re-utilized original database, thereby potentially depriving *sui generis* database rightsholders of a fair return for the investment made in the arrangement and systematic collection of the overall dataset (*Innoweb BV*); (**v**) taking from *Innoweb*, the evaluation on whether the database *sui generis* rightsholder lost the investment made to build the dataset at stake depends on whether such investment was redeemable under a proportionality assessment, thereby reducing the scope of Article 7 DbD, after years of broad reading embraced by the CJEU (*CV-Online Latvia*). To conclude on

database rights, most datasets interested by the present Regulation are unlikely to be "original", so as to deserve copyright protection. Rather, most of them can qualify for sui generis protection under Article 7. Thus, acts of "re-utilization" and "re-use" of database contents are likely to be read expansively, in line with the predominant interpretation of the CJEU. Although in *CV-Online Latvia*, the CJEU seems to have slightly changed the attitude, sui generis obstacles to data transfers on a cross-border level remain consistent and need to address through favorable licensing conditions. Moreover, exceptions to these rights are strictly sector-specific and left to Member State law, suffering from the high level of fragmentation structurally affecting the panorama of EU copyright flexibilities insofar. Therefore, it follows that, in correspondence with national public security concerns, a strictly tailored exception may also be enacted on a national level, yet not certainly for the purpose of facilitating cross border exchanges of non-personal data, which is excluded on the same grounds.

Other IP restrictions come from the Software and the Trade Secrets Directive. With regard to the Software Directive, it is quite relevant that Recital 11 recalls that protection does not extend as to cover ideas and facts underlying the program and related interfaces. Specifically, the Software Directive covers computer programs, as long as the same is original (Article 1(4)) and therefore forbidding acts of temporary or permanent reproduction, loading, display, running, storage, adaptation, translation, arrangement, alteration and any other form of distribution. As the number of restricted acts is quite broad, cross-border exchanges of datasets contained in protected computer programs on a free-of-charge basis are unlikely to occur due to the full applicability of Article 4. Moreover, by way of contrast with the case of copyrighted or sui generis protected databases, where few exceptions were granted for scientific research and/or national public security, the Software Directive only provides some room for flexibility in the case of lawful use and further study/observation of the functioning behind the program. This little room for flexibility risk underpinning the objectives of the Regulation consistently, as the same was enacted for the specific purpose of enhancing the flourishment of an ICT/Cloud Computing services market. In addition to that, trade secrets under Article 3 of the related Directive risk covering substantial parts of potentially exchangeable datasets, thus leading to the adoption of specific measures against IP theft, disclosure and espionage which ultimately hamper free flows of non-personal data. However, the array of exceptions under Article 5 may leave room to extensive interpretations. In fact, Article 5(d) allows the provision of exceptions for protecting a mostly undetermined "legitimate interest" under both EU and national law. Hinging on this rule can foster national and Union lawmaking functional to encourage IP carve outs with regard to trade secrets covering large parts of exchangeable datasets.

Proposal Data Governance Act (DGA): in order to overcome the roadblocks created by the need to require consent when cross-border exchanges of mixed datasets owned by public bodies or undertakings are at stake, Recital 35 of the Proposal for the Data Governance Act (DGA) attempts to establish an alternative form of consent based on "data altruism", defined under Article 2(10) DGA. By making available PSI through compliance with specific procedural requirements (such as, e.g., registration as a "Data Altruism Organization recognized in the Union"), cross-border further processing of public sector data can be fueled, so as data subjects can also consent on an *ex-ante* basis to purposes unlikely to be envisaged at the time of first data collection (Recital 36), provided that such processing takes place on public interest grounds and within a secured electronic environment. From these Recitals becomes clear that the DGA will push the core principles of the Regulation at stake forward with regard to G2B data sharing agreements when datasets contain PSI. Yet, like in the present Regulation and as provided under the Open Data Directive (ODD), there is no obligation with regard to PSI re-use, so as public sector bodies are free of restricting flows of non-personal data, when confidentiality agreements supported by the national public security exception are in force. In this regard, the national public security exception still constitutes a withdrawal, carrying the risk of hampering both the objectives of the present Regulation and the DGA. As in the case of health data, also the DGA establishes a rigid procedural scheme for data sharing providers, also if they decide to operate on the grounds of data altruism. For example, Article 19, with regard to the conditions in order to share data on the grounds of data altruism, sets that recognized organizations shall notify data holders about the purposes of general interest for which processing is undertaken through this streamlined form of consent, ensuring, under Paragraph two, that no further processing activity is undertaken beyond such purposes. However, it is still noteworthy that licensing of PSI on FRAND terms, on a non-exclusive basis and under transparency requirements is mandated under the DGA (Articles 4 and 5 DGA). This is a pull towards higher competitiveness within the field of EU data and digital services created through PSI reuse, facilitating startups and SMEs scale-ups and removing barriers to free flows of these datasets. At

the same time, this might create disparities with data-sharing licensing practices when other dataset-structures are involved.

Proposal Data Act: this Regulation is eager to remove substantial obstacles to data access and de facto ownership regimes for a specific category of data, i.e. those generated by IoT services, which also affected the very same feasibility of cross-border exchange initiatives. The Proposal establishes a B2C access regime which can also be extended to third parties (Article 5), thus setting the milestone for free flows of non-personal data, as long as trade secret law and data protection rights of others are respected (Article 5(8)-(9)). Apart from removing hindrance to data access in favor of consumers, thus enabling free flows of data in general, the Data Act also provides a blacklist of unfair clauses that can be imposed to SMEs in B2B sharing agreements, in line with the pro-competitive objectives looming in the background of the Regulation on free flows of non-personal data. In fact, also the present Regulation encouraged, yet in a milder way, the adoption of standard contract terms in data licensing agreements (Article 6).
A specific Union-based access regime is also provided with regard to public sector bodies, whose position is highly evaluated due to the public interest behind such request (for this reason, e.g., data should normally be provided on a free-of-charge basis under Article 20(1)). In relation to public bodies, a specific rule addresses the quandary of cross-border exchange of information. In this respect, Article 22(1) allows cross-border cooperation among national competent authorities, providing that, when a public sector body needs to obtain data from a data holder in another Member State, prior request should be submitted before the authority thereof. In this sense, a favorable access regime is established with regard to both cross-border and national exchanges of data on a B2G basis, thus fostering the objectives of the present Regulation in the particular case when public sector bodies apply for the obtaining of data generated by IoT services on the grounds of the public interest. Following one of the main rationales behind this Regulation, the Data Act also dedicates an entire Chapter (IV) to rules favoring switching from one service provider to another. Article 23 mandates the removal of any organizational, technical, contractual and economical stalemate to portability practices, preventing users from concluding a contract with a new provider of the same service offered by the former, thereby porting data and maintaining the same level of functional equivalence between the two IT-environments. Mandatory clauses against vendor lock-ins are established under Article 24, taking the policy basis of the Regulation analyzed here to a much more advanced level. In line with that, interoperability standards are also mandated under Articles 28 and 29 of the Proposal. Strikingly, Article 35 contains an optional exception to *sui generis* database rights, in order not to impair the access regimes established under Articles 4 and 5. Although limited to non-personal data generated by IoT services, this provision is highly impactful on cross-border exchange and flows of non-personal data, removing one of the remaining obstacles which were not touched by the 108 Regulation. However, the real impact of such provision remains to be seen. Notwithstanding, it is undeniable that the Data Act, if approved, is likely to increase the levels of access, sharing and interoperability of IoT-generated data to a significant extent, because essential requirements and contract terms are strictly mandated by directly applicable Union rules. This will reduce fragmentation and legal uncertainty with regard to data-sharing contractual practices, also facilitating the development of the digital market across EU and in parallel with the objectives of the DGA and of the Proposal for an Interoperable Europe Act.

Proposal Interoperable Europe Act: this recently issued Proposal can have a huge impact on the advancement of the objectives first pursued by 108 Regulation. The same aims at boosting the creation of a Union-wide harmonized data interoperability infrastructure, aiming at ensuring the digital transition with regard to public sector bodies. For the purpose of enhancing free flows of non-personal data, several provisions are relevant. Firstly, Article 3 is paramount for mandating a cross border interoperability assessment, that should be undertaken by public bodies in order to enable electronic management of public services on a cross-border basis. This will be useful to create an European Interoperability Infrastructure and, simultaneously, help with increasing effective cross-border exchange data flows through a secured, harmonized and homogenous framework which goes beyond sector- and data-specific regulatory approaches. Secondly, Article 4 establishes that a public sector bodies within EU, upon request, must provide mandatory interoperability solution that support public services in electronic format. This may bolster the flourishment of G2B transfers of public data, highly favored by the all-encompassing adoption of interoperable solutions on a compulsorily basis. Yet, this last rule does not affect datasets on which IPRs hinge (Article 4(1)(b)), which is often the case of datasets addressed by the present Regulation. In this respect, it is also relevant that Article 11(3), while introducing "regulatory sandboxes" for the purpose of boosting innovation within the field of digital interoperability services, mentions the following objectives: "*(c) facilitate the development of an open European*

GovTech ecosystem, including cooperation with small and medium enterprises and start-ups; enhance authorities' understanding of the opportunities or barriers to cross-border interoperability of innovative interoperability solutions, including legal barriers; contribute to the development or update of Interoperable Europe solutions." All these policy purposes are in full alignment with the ones pursued by the present Regulation, which was enacted to put the basis for a prosperous market of digital interoperability and cloud storage services in first instance.

NIS I and II Directives: all data exchanges flows on a cross-border level should be undertaken in full compliance with the requirements established by the NIS I and NIS II Directives and, in particular, the activities of the cross-border Cooperation Group provided under Article 4 of the proposed NIS II Directive can be enhanced when cross-border exchanges of non-personal data are at stake, as cross-border national interests easily come into play. In this respect, Cooperation group members are incentivized to exchange best practices and information about increasing exchange of data flows on a cross-border level (Recital 114), with the consequence of increasing standardization of cybersecurity practices. Yet, at the same time, the heightened cybersecurity standards mandated under Article 7 may create further fragmentation in relation to the various degrees of compliance of different Member States. This, in combination with full application of the present Regulation and rapid technological advancement, might implicitly increase risks for unforeseen cyberattacks, especially when in the case of G2B cross-border exchanges.

GDPR: as recalled in white papering materials about non-personal data flows, Recital 53 has already suggested, despite in a non-binding form, that free flows of personal data on a cross-border level should not be hampered by 108 Regulation. In the same fashion, Article 89(1) GDPR establishes a derogation affecting particular categories of highly sensitive data, i.e., those enlisted in Article 9(1) GDPR, for further processing undertaken for research and other purposes relevant for the public interest. *A fortiori*, the same reasoning cannot be denied with regard to non-personal data, which are subject to less stringent requirements and guarantees for being outside from the objective scope of the GDPR. Nevertheless, provided that the GDPR and the present Regulation are complementary in scope and application, the boundaries between the concept of personal and non-personal data is eager to impact on the number of compliance duties and restrictions which may be imposed on cross-border data exchanges in the case of mixed datasets. In fact, an incompatibility rule seems to be suggested in the case of mixed datasets, which, however, seems to be replaceable with a regime of problematic coexistence between the two Regulations when personal and non-personal data are inextricably linked. In these situations, all guarantees and procedural requirements established under the GDPR shall apply to the full dataset (full-encompassing prevalence rule), with the consequence that cross-border transfers are inevitably prejudiced. In fact, a lawful basis granted by Article 6 under Member State or Union law (such as in the case of health data under the Proposal for the EU Health Data Space) is mandatory in order to support data exchange of mixed datasets on a cross-border level. In this sense, apart from purposes related to scientific research, where it is quite unclear whether the GDPR itself can constitute a separate and self-sufficient legal basis to legitimize further processing, data exchanges on a cross-border level are unlikely to be feasible except for consent being explicitly required. In any case, the specificity and necessarily narrow scope is eager to impair the extent of cross-border exchanges of datasets, with the result of hampering the objectives behind the present Regulation.

3.7.4.3 Relevant CJEU case law

The CJEU influences the scope and application of this Regulation with specific regard to **two key aspects**:

- **The broad concept of personal data**: by drawing the line between the concept of personal and non-personal data, the CJEU implicitly distinguishes between the objective scope of the GDPR by way of contrast with the one of the present Regulation. In general, it can be said that the prevailing trend is to read the notion of "personal data" expansively, thereby encroaching 108 Regulation in its applicability.
  Traditionally, non-personal data encompass environmental readings, spatial, industrial or agricultural data. When merged into complex and mixed datasets and due to technological advancement, re-identification starting from non-personal data became increasingly easier and nearly always possible. In 2019, the EU Commission set the principle under which non-personal data can be established in two ways, as they

coincide with "*data that from the outset do not concern an identified or identifiable natural person (such as weather data); data that were initially personal and only later became anonymous through a process of anonymization (e.g., data concerning the travel abroad of a person after the use of special techniques to ensure anonymity)*".
In the light of CJEU consolidated case law, personal data became intrinsically associated with the concept of "*any information; concerning; a natural person; identified or identifiable*", which, in parallel, delineates the contours of the definition of non-personal data from a "negative" perspective.
In *Nowak*, the CJEU held that, while referring to "personal data", Article 2(a) of the e-Privacy Directive aimed at establishing a **broad notion**, encompassing "*all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject*". Yet, the concept of re-identification was further specified and narrowed down by both the WP29 and the CJEU before, showing a tendency of broadening the concept of personal data, simultaneously curtailing the one of non-personal. The WP29 had previously clarified that, although identification might be possible, data can be held as non-personal if, in order to relate to a specific individual, contextual linkages are still needed and missing in the case at issue. Likewise, in *YS and M,S*, the CJEU held that if re-identification is possible with regard to a dataset of non-personal data, the individual at stake was not identifiable on the basis of the content thereof. Thus, it set the so-called "concerning parameter", under which, data can be held as personal "*where the information, by reason of its content, purpose or effect, is linked to a particular person*".
In line with that, in Breyer, the CJEU broadened the concept of "re-identification" as well, allowing the same to be performed by more than one person in order to deem information about a data subject as personal data ("cross-referencing information from different data controllers), due to the intrinsically dynamic nature of re-identification processes. Therefore, under the complicated legal framework delineated by the CJEU, non-personal data are for sure only those which are originally non-personal, thus have never been linkable with a natural person.

- **The restrictive concept of public security**: the CJEU has interpreted the concept of national public security in a **restrictive manner**. In particular, "*it has reserved the right to decide on the legitimacy and adequacy of national security measures*", so as "*a Member State cannot by simple reference to internal security", be relieved from its obligations under EU law*". In particular, restrictions on free movement of goods and services on the grounds of national public security concerns are particularly difficult not to be quashed down by the CJEU. For example, the same endorsed a rigid posture in 1997 against a French measure adopted on the grounds of public security concerns. The Court held that, although Member States enjoy a margin of discretion, as the Union does not have the ability to verify the existence of a national public security concern in one Member States, the measure adopted by the French Government was not sufficient and thus could not been advocated in order to justify failure to comply with EU rules. As underlined by Advocate General in the case at issue, the burden of proof about the proportionate character of the legislative measure rests on the Member State. The same restrictive reading was embraced in *Tele 2 Sverige*, where a Swedish law imposing an IT provider retention of traffic data for six months was held in contrast with EU law, in full compliance with the Digital Rights Ireland. That was the decision of the CJEU despite the same was enacted, according to the argument endorsed by the Swedish government, for the purpose of fighting organized crime and therefore on national public security grounds. As modern investigation methods do not require data retention in order to achieve the same purposes, the second prong of the proportionality test under Article 52(1) CFREU was not satisfied.
  Thus, also the concept of public security under the present Regulation is to be held restrictively, except for falling under the hammer of the CJEU for noncompliance with EU law and lack of proportionality. This element, in contrast with the blurry interplay between the concepts of personal and non-personal data, fuels a broader application of 108 Regulation, as a reduced scope for the so-called "national security exception" should be inferred from CJEU wording.

3.7.5 Alternative Solutions/Policies

The alternatives to the enactment of the present Regulation are efficiently wrapped up in the Impact Assessment and briefly listed here below:

- **Revision of sector-specific Directives**, i.e., at the time the E-Commerce Directive, Services Directive, Transparency Directive and the INSPIRE Directive, option to be discarded due to the lack of effectiveness of sector-specific regulation in the area and due to the policy priority of repealing data localization requirements, which would be unfeasible in this way
  Not fully/exhaustively discussed

- **No change of EU law at all:** private ordering is unpredictable and likely to increase fragmentation and uncertainty, high compliance costs due to the necessity of submitting formal requests to judicial cooperation authorities and DPAs in order to obtain authorization for cross-border data transfers, blind reliance on NIS Directive for security standards for data storage and processing;

  Resulting in
  - **Unequal and fragmented regulatory scenario** across EU;
  - Cloud service providers have to take into account **data localization restrictions** as opposed to a market-driven approach, building local data centers even if they serve cross-border users, choosing ideal locations for data infrastructures and losing economic and operational efficiency due to the increase of costs;
  - **Lack of competitiveness** in specific sectors, damaging smaller providers and SMEs in first instance, thus increasing the costs of setting up a new business, carrying with it the risk of infringing Article 16 CFREU (freedom to conduct a business) for delimiting business choices and the opportunities of cloud service providers for better serving customers' needs;
  - Sharp **rise in administrative burdens and compliance costs**, also affecting the position of consumers in the downstream market (costs on businesses are reflected by higher prices)
  - **Excessive switching and portability costs** leading to a high degree of vendor lock-ins;
  - **Environmental and social impacts** as data localization requirements require service providers to locate data infrastructures where there are substantive energy gains, thereby increasing employment only in such areas and leading to a "*concentration of data skills demand*";
  - **Data security and storage risks**, leading to potential cyber-attacks;
  - **Competition case-law over-burden** due to the high number of abuses of dominance that are likely to materialize within the tech-sector;

- **Non-legislative initiative (option 1)** based on guidelines, the strengthening of enforcement rules and transparency mechanisms based on the existing legal instruments, whose effectiveness should be effectively bolstered through the mere promotion of stakeholder dialogues, the adoption of self-regulatory codes of conduct and co-regulation proceedings;

  Resulting in
  - **Persisting climate of legal uncertainty** about data localization requirements and difficulty in pursuing infringement proceedings targeting data localization requirements, that rather stems from private ordering, administrative or other kinds of national policies rather than Member State regulatory law and therefore are uneasily identifiable by EU institutions;
  - **Lack of impact on competitiveness**;
  - **Marginally positive impact on reduction of costs** created by the regulatory environment and on sharing of cloud and digital services in general among providers;
  - **Reduction of administrative burdens** thanks to guidelines on data availability towards DPAs;
  - **Limited impact on the downstream sector**, leading to lack of operational efficiency, market fragmentation and high switching costs;
  - **Transparency measures** may foster the establishment of an EU cloud market;
  - **Limited positive impact** on the environment;

- **Better cooperation on standardization of interoperable formats**, such as APIs;
- Better enforcement increases costs in terms of human resources yet having a moderately positive regulatory impact on the elimination of data localization restrictions on a case-by-case basis, as informal and/or perceived barriers are much more compelling in this regard than existing ones;
- **Cybersecurity high compliance costs** in the lack of an EU principle of free movement of non-personal data and therefore of legal certainty in the area;

- **Principle-based initiative (option 2)** setting the principles of free flows of non-personal data across EU, data storage and processing should facilitate porting and switching, a user of data storage and processing shall not be denied request to exchange data on a cross-border level by DPAs, single contact points and common standards for security and storage of data must be established;

  Resulting in…
  - **Higher legal certainty and trust about removing data localization** requirements across EU on a compulsorily basis, except for those based on public security grounds that are unlikely to affect businesses;
  - **Higher legal certainty and trust about data security and cross-border processing** of non-personal data;
  - **Pro-competitive effect**, impairing the business strategies of those firms which misuse data localization to gain competitive advantages and avoiding discrimination between Member States where it is more convenient to settle data infrastructures and those where it is not, thus increasing SMEs competitiveness in the EU, as well as the costs to set up a new business;
  - Higher certainty in granting authorization to DPAs for data access in order to facilitate cross border exchanges, having a **short-term positive impact on the operational efficiency in the downstream sector**;
  - Principle under which businesses should provide data portability **contrasts vendor lock-in practices** and lead to **a faster take-up of public cloud services**;
  - **Positive impact on freedom to conduct a business under Article 16 CFREU**, carrying with it potential increases the number of data infrastructure-related **job places** and reduced **environmental impact** arising from the concentration of data infrastructure in few Member States, also due to the minimum interoperability standards imposed;
  - **Reduces risks of cyberattacks**
  - **Moderate administrative costs due to the soft institutional framework whilst relatively coordination costs**

- **Detailed legislative initiative (option 3)** providing pre-defined assessments of what should constitute a disproportionate and unjustified data localization measure, a horizontal, cross-border mandatory cooperation framework to enhance access regimes of DPAs, fully binding obligations on switching, portability and harmonization of legal conditions thereof, including the development of common standards and an EU-based certification scheme for security and storage of data processing.

  Resulting in…
  - **Negative impact on innovation**, as stakeholders have pointed out how data portability requirements for each kind of data held by companies can be overly burdensome, increasing compliance regulatory costs;
  - **No further discussion**

3.7.6 Comparison of Alternatives

- **Non-legislative initiative**
  - Strengthened enforcement approach as an effective incentive for removal of data localization requirements (+1)
  - No clear legal framework/time-consuming (-1)

- **Principle-based initiative (+ self-regulatory codes of conduct/sub.2a):**
    - All four policy objectives are reached (higher regulatory certainty, data availability for Data Protection Authorities on a cross-border level, reduced costs/higher incentives for data portability and switching practices, reduction of administrative burdens/costs) (+4)
      → ***preferred option***
        - Ensuring a balancing approach among legal certainty and policy flexibility
        - High reliance on pre-existing legal instruments
        - No influence on IPR regimes

- **Detailed legislative initiative**
    - Three policy objectives are reached except for facilitating the uptake of cloud services at the EU level (+3)
    - Specification of portability requirements on a cross-border level can lead to further restrictions and the impact on innovation can be negative (-1)

3.7.7 Recommendations

Description of Policy Recommendation(s) and recommendations for other stakeholders

108 Regulation keeps several issues unaddressed, that need to be clarified/implemented by stakeholders**:**

- **Interplay between interoperability standards, data-sharing practices and IPR protection requirements**, which vary consistently in accordance with the structure of datasets and therefore impair the all-encompassing nature of this Regulation;
- **Sector-specific applications of national public security policies**, carrying with them the risk of breaching EU law for lack of compliance due to the restrictive interpretation of the notion;
- **High level of granularity** in the patchwork of legal solutions impacting on data-sharing, access and ownership, carrying with it the risk of hindering the effectiveness and the practical significance of the present Regulation;
- **The non-mandatory character of B2B and B2G data-sharing best practices and mere self-regulatory nature of interoperability standards provided under Article 6** of the present Regulation, that needs to be coordinated with the related EU legislatures proposed in this regard;
- **Differentiation/further articulation of data access regimes** in view of administrative rules adopted at national level and affecting DPAs, also arising from the undetermined concept of “abuse”;
- **Growing concerns about the obsolete divarication in regime between personal and non-personal data**, also considering the need to coordinate it with the sector-specific lawmaking approach more recently endorsed by the EU Commission (holistic view of data regulation).

The principle-based initiative was preferred thanks to its assumed capability of finding a middle ground between the need to ensure a consistent level of regulatory certainty, which can be granted through a principle-based lawmaking technique affecting areas of key concern for the EU digital and data markets. Yet, **the interplay between the preferred option and a detailed legislative initiative in terms of policy convenience was not adequately investigated**.
Apart from a cursorily reference to the fact that strict portability requirements and a mandatory B2B-specific legal portability right are eager to produce a negative impact on innovation, reliable economic data have not been added as supporting evidence in this regard. Glossing over a detailed analysis of the impact of a detailed regulation on which data localization measures can be allowed is a weak point of this Impact Assessment policy evaluation. This raises several doubts about whether and to which extent the EU Commission has been overly

hesitant with the 108 Regulation, especially if such a reluctant approach is compared with much more advanced and detailed EU legislatures, that have substantially followed the path abandoned in favor of a principle-based spirit of the present Regulation. In fact, 108 Regulation appears vague and largely underpinned in both application and scope in comparison with the overarching significance of later sector-specific legislative measures adopted at the EU level, such as the Data Act and the Data Governance Act. In this respect, a change in law and policy-making can be observed in the EU in the last four years, leaving principle-based legislation aside in favor of *command-and-control* and more pervasive industrial policies.

The final selection mostly rests on consideration of legal nature. Noticeably, the scenario described if the self-regulatory landscape of option 1 were to be adopted does not change significantly by way of comparison with the preferred option. In general, it can be said that the EU Commission rather preferred the "safer option" of setting bright-line rules rather than relying on private ordering, best practices and codes of conduct solely. In fact, in situations where monopolization threats are likely to materialize, a strong regulatory intervention is needed in order to repeal uncertainty and help SMEs with flourishing through the removal of entry barriers. While comparing option 1 and 2, no technical nor significant political aspects are taken into consideration except for the policy pressure in fostering the creation of an EU cloud service market, avoiding loss of operational and economic efficiency at the expense of EU based SMEs and smaller providers. In this sense, competitiveness is the absolute policy priority to be addressed. Moreover, environmental aspects are marginally tackled as reinforcing arguments in order to support the decision to de-localize data infrastructures and therefore avoid concentrations in single Member States. However, both the arguments related to social and environmental aspects recalls the concept of "sustainable development", intended as a way in order to integrate economic growth with social inclusion and environmental protection within EU law, thus promoting a balancing approach that is also reflected by the rationale of 108 Regulation. In addition to that, there is a strong emphasis on the need to preserve incentives to innovation, through avoiding lessened protection to IPRs and through the choice not to adopt a clear-cut legal portability right under option 3. Yet IPR based restrictions and the little scope of portability rights are nowadays the main sources of obstacles to free flows of non-personal data in the EU, both insufficiently addressed by the Regulation at stake.

3.8 REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 19 OCTOBER 2022 ON A SINGLE MARKET FOR DIGITAL SERVICES AND AMENDING DIRECTIVE 2000/31/EC (DIGITAL SERVICES ACT) (TEXT WITH EEA RELEVANCE)

3.9 PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS COM/2021/206 FINAL

3.9.1 Executive summary

The Proposed 'Artificial Intelligence Act' (hereinafter referred to as 'Proposed Regulation') answers the call for legislative action to ensure a well-functioning internal market for artificial intelligence systems ('AI systems') where both benefits and risks of AI are adequately addressed at Union level.

The text referred to for the purpose of the present analysis dates to 21 April 2021, when it was first published, while further references will be made *infra* with regard to the current amendments proposals.
It amounts to an Explanatory Memorandum, a total of 89 Recitals, 85 Articles, and 9 Annexes.

The **Explanatory Memorandum** accompanies the Proposed Regulation and accounts for the reasons and objectives of the Proposed Regulation, namely the need to establish the EU's technological leadership in AI to ensure that Europeans benefit from a technological development that is compliant with EU values and fundamental rights and principles. It briefly explains the context of the Proposed Regulation with regard to the issues and regulatory needs raised by AI, its specific objective to provide a robust and flexible legal framework adopting a risk-based approach for the placing on the market of AI systems. As such, the regulatory framework on AI deals with the following specific objectives: a) ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values; b) ensure legal certainty to facilitate investment and innovation in AI; c) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; d) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation. For these purposes, the Proposal follows a risk-based approach to set harmonized rules for the development, placement on the market and use of AI systems in the EU market. The legal basis in accordance with the principles of subsidiarity and proportionality is to be identified under Article 114 TFUE: the primary objective of the Proposed Regulation is to ensure the proper functioning of the internal market to prevent its fragmentation and the substantial diminishment of legal certainty. Moreover, it contains references to consistency requirements with existing policy provisions in the EU, such as the EU Charter of Fundamental Rights and secondary legislation on data protection, consumer protection, non-discrimination and gender equality, competition law, sectoral safety legislation covered by the New Legislative Framework (NLF), as well as forthcoming policies and the other initiatives related to the EU strategy for data (Data Governance Act, Open Data Directive, etc.). For this purpose, the Proposed Regulation defines ex-ante common mandatory requirements applicable to the design and development of certain AI systems, further operationalized through harmonized technical standards - yet to be established - and ex-post market controls.

The proposed legislative text contains **89 Recitals**, providing additional guidance on the interpretation of the Proposed Regulation's provisions.

Specific provisions of the Proposed Regulation are summarized as follows:

Title I – Scope and definitions (Articles 1-4): it defines the subject matter and the scope of application of the new rules covering the placing on the market, putting into service, and use of AI systems, and contains also with the relevant definitions. To provide the needed legal certainty, it is complemented by Annex I, which contains a detailed list of approaches and techniques for the development of AI.

Title II - Prohibited Artificial Intelligence Practices (Article 5): following a risk-based approach, the Proposed Regulation differentiates between uses of AI that bear (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk. It prohibits altogether the use of AI systems whose risks are considered unacceptable as contravening to EU values or violating fundamental rights, such as manipulative or exploitative practices against vulnerable groups in order to distort their behaviour in a manner that is likely to cause psychological or physical harm. It also explicitly prohibits social scoring for general purposes carried out by public authorities, while 'real-time' remote biometric identification in publicly accessible spaces for law enforcement is generally prohibited, unless certain limited exceptions apply.

Title III - High-risk AI systems (Articles 6-51): An extensive number of provisions in this Title deals specifically with high-risk AI systems: the classification as high-risk is based on the intended purpose of the AI system and its modality of use. The deployment of AI systems that create high risk to the health and safety or fundamental rights of natural

persons is subject to certain rules to ensure compliance with mandatory requirements and to a conformity assessment before putting it on the market.
For this purpose, Chapter 1 sets the classification rules and identifies two main categories of high- risk AI systems: i) AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment; ii) other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III, which contains a predefined number of AI systems whose risks have already materialised or are likely to materialise in the near future.
Chapter 2 sets out the legal requirements for high-risk AI systems, under the framework of a risk management system (Article 9) regarding data governance (Article 10), documentation and record-keeping (Articles 11, 12), transparency and provision of information to users (Article 13), human oversight (Article 14), and finally robustness, accuracy and cybersecurity (Article 15). The content of such requirements may be substantially determined either by harmonized standards, if available, or technical specifications, or otherwise be developed in accordance with the state-of-the-art of scientific knowledge at the discretion of the provider of the AI system.
Chapter 3 places clear obligations for providers and users of high-risk AI systems, along with obligations on other parties involved, such as importers, distributors, authorised representatives. Such obligations are articulated mainly in the adoption of a quality management system (Article 17) and the performance of a conformity assessment (Article 19), with specific heed to the obligation to draw up technical documentation as referred to in Annex IV.
Chapters 4 and 5 are specifically dedicated to the conformity assessment procedure: while the former sets the framework to involve the notified bodies in the conformity assessment procedure, the latter explains in detail the procedure to carry out the conformity assessment for each type of high-risk AI system. It is important to notice that AI systems that comply with the relevant harmonised standards (Article 40) or other common specifications (Article 41) where such standards do not exist, are insufficient or specific safety or fundamental rights concerns need to be addressed, are presumed to be in conformity (Article 42) with the requirements set out in Chapter 2. An initial distinction is to be made with regard to AI systems intended to be used as safety component of products or as stand-alone products. In the first case, the conformity assessment procedure will be subject to compliance with both the requirements set out in the Proposed Regulation and those under the New Legislative Framework sectorial legislation for the products of which they are a component. In the second case, the conformity assessment procedure (Article 43) may be carried out either based on internal controls (Annex VI) or based on assessment of the quality management system and the technical documentation with the involvement of a notified body (Annex VII). AI systems undergoing substantial modifications shall be subject to new ex-ante conformity assessment.

Title IV – Transparency obligations for certain AI systems (Article 52): for other AI systems that are not classified as 'high-risk' but are characterised by the fact that they (i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content ('deep fakes'), the Proposed Regulation imposes transparency obligations to allow users to make informed choices.

Title V – Measures in support of innovation (Articles 53-55): national competent authorities are encouraged to set up regulatory sandboxes in order to establish a controlled environment to test innovative technologies.

Titles VI – VII – VIII – Governance and implementation (Articles 56 – 68): the provisions in the mentioned titles establish a European Artificial Board (Article 56), composed of representatives from Member States and the Commission, tasked with facilitating a smooth, effective and harmonized implementation of the Proposed Regulation. At a national level, Member States are tasked with designating one or more national competent authorities as well as the national supervisory authority. An EU-wide database for standalone high-risk AI systems with fundamental rights implications, operated by the Commission, will be established for the registration of AI systems before their placing on the market. Finally, ex-post obligations concerning monitoring and reporting of AI-related incidents and malfunctioning are established. In fact, market surveillance authorities are entrusted with ex-post enforcement and compliance monitoring after the AI system is placed on the market or otherwise put into service.

Title IX – Codes of conducts (Article 69): it provides a framework for the creation of codes of conduct to encourage providers of non-high-risk AI system to voluntarily comply with the mandatory requirements for high-risk AI systems

and other voluntary commitments, such as environmental sustainability, accessibility for persons with disability, stakeholders' participation, etc.

Title X – Confidentiality and penalties (Articles 70 – 72): it imposes rules for the respect of confidentiality of information and imposes penalties for the infringements thereof.

Titles XI – XII – Other and final provisions (Articles 73 – 85): it imposes rules for the exercise of delegation and implementing powers by the Commission to ensure uniform application of the Proposed Regulation, and to adopt delegated acts to update or complement the lists in Annexes I to VII. Finally, it also lays down provisions for the differentiated transitional period for the initial date of applicability of the Proposed Regulation.

The text of the Proposed Regulation is accompanied by a total of **9 Annexes**, listed as follows:
Annex I - Artificial Intelligence Techniques and Approaches Referred to in Article 3, Point 1
Annex II - List of Union Harmonisation Legislation
Section A. List of Union Harmonisation Legislation Based on the New Legislative Framework
Section B. List of Other Union Harmonisation Legislation
Annex III - High-Risk AI Systems Referred to in Article 6(2)
Annex IV - Technical Documentation Referred to in Article 11(1)
Annex V - Eu Declaration of Conformity
Annex VI - Conformity Assessment Procedure Based on Internal Control
Annex VII - Conformity Based on Assessment of Quality Management System and Assessment of Technical Documentation
Annex VIII - Information to be Submitted upon the Registration of High-Risk AI Systems in accordance with Article 51
Annex IX - Union Legislation on Large-Scale IT Systems in the Area of Freedom, Security and Justice

3.9.2 Analysis of the Legislative Proposal

3.9.2.1 Background of the Legislative act

The Proposed Regulation is part of the Commission's agenda of making Europe fit for the digital age. Since 2018 the Commission has put forward a European strategic plan for AI,[138] which resulted in some relevant initiatives, such as the High-level Expert Group on Artificial Intelligence publishing the Ethics Guidelines for Trustworthy AI[139] and Policy Recommendations[140], followed by the White Paper on AI[141] setting the policy options for a regulatory approach towards AI based on an ecosystem of excellence and trust for AI[142], which was subject to a wide public consultation launched on 19 February 2020 until 14 June 2020, targeting all relevant stakeholders ranging from public to private sectors, academia, and civil society. The results of the stakeholder consultation are available in the accompanying impact assessments.[143]

138 European Commission, Artificial Intelligence for Europe, COM(2018) 327 final, 2018.

139 High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.

140 High-Level Expert Group on Artificial Intelligence, Policy and investment recommendations for trustworthy AI, 2019.

141 European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust,

COM(2020) 65 final, 2020.

142 European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.

143 Commission Staff Working Document, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 final, PART 1/2 and 2/2.

The Commission Staff Working Document Impact Assessment accompanying the Proposed Regulation provides a clear background of the legislation under analysis: not only does it provide with the necessary introduction to the technological, the socio-economic, and the legal context, but it also points out the problem at stake and accounts to some extent for the prior efforts to solve it by assessing the (in)adequacy of the pre-existing legal framework. After introducing the technological context of AI, viewing it as a machine-based system that can for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments with different degrees of autonomy[144], it defines the socio-economic impact on healthcare, farming, education, infrastructure management, energy, transport and logistics, public services, security, and climate change mitigation, in terms of both benefits and risks.

However, a thorough analysis whether the pre-existing legal framework is fit for purpose in the context of risks arising from AI has been carried out, with reference to the following legislative sectors:[145]

i) Relevant fundamental rights legislation, namely the EU Charter of Fundamental Rights, including specific provisions on data protection and consumer protection.

ii) Relevant product safety legislation, which constitutes a solid body of EU secondary law, aimed at ensuring that only safe enough products are placed on the Union market. The so-called 'New Approach' was developed in 1985 with the main objective to restrict the content of legislation to 'essential high-level requirements' leaving the technical details to European harmonised standards. Against this background, the New Legislative Framework (NLF) was then developed in 2008, introducing harmonised elements for conformity assessment, accreditation of conformity assessment bodies and market surveillance.

iii) Relevant liability legislation, which traditionally identifies the liable party for harm and the conditions for compensation. The Product Liability Directive (PLD)[146], which imposes 'strict' liability on the producers for physical or material damage caused by a defective product, while still providing a certain degree of legal certainty and protection for consumers, it is challenged by AI due to its complexity, opacity and potentially autonomous behaviour. For these reasons, the Commission acted for a revision of liability rules, resulting in proposals for an amendment of the PLD[147] and a more specific AI Liability Directive.[148]

iv) Relevant legislation on services, whenever an AI-driven software is deployed as stand-alone or integrated service. In this context, rules regarding the responsibility of intermediaries, including transparency and accountability obligations, as laid down by the Digital Services Act for instance,[149] shall be considered.

Against this background, the European legal framework is not equipped with the appropriate regulatory tools for AI, as it does not provide for a definition of an AI system, nor for horizontal rules for classifying its risks.

The same Commission Staff Working Document – drafted at the time the Regulation was proposed - provides with a thorough problem definition, which can be summarized in the following table:

144 OECD, Recommendation of the Council on Artificial Intelligence, 2019

145 Please note that interdependencies with other policy areas are specifically addressed infra.

146 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

147 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.

148 Proposal for a directive of the European Parliament and of the Council on adapting noncontractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.

149 Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.

DRIVERS	PROBLEMS
The complexity and lack of transparency (opacity) of AI makes it difficult to monitor, identify and prove possible breaches of laws, including legal provisions that protect fundamental rights. Some AI systems change and evolve over time and may even change their own behavior in unforeseen ways. It can give rise to new risks. The existing legislation is not adequately addressing these risks. Autonomy can affect the safety of the product, because it may alter a product's characteristics substantially, including its safety features. The dependence of AI systems on data and their quality, the AI's 'ability' to infer correlations from data input and learn from context data, including proxies, can reinforce systemic biases and errors, and exacerbate discriminatory and adverse results.	**(1)** Use of AI poses **increased risks to safety and security** of citizens **(2)** Use of AI systems poses **increased risk of violations of citizens' fundamental rights and Union values** **(3) Authorities do not have powers, procedural frameworks and resources to ensure and monitor compliance** of AI development and use with applicable rules **(4) Legal uncertainty and complexity on how existing rules apply to AI systems** dissuade businesses from developing and using AI systems **(5) Mistrust in AI would slow down AI development in Europe** and reduce the global competitiveness of the EU economy **(6)** Fragmented measures create **obstacles for cross-border AI single market and threaten Union's digital sovereignty**

Source: European Commission Staff Working Document Impact Assessment accompanying the Proposed Regulation part ½

Figure 3

Problem 1: The use of AI poses increased risks to safety and security of citizens.
Two main reasons explain the limitations of the existing EU safety and security framework in relation to the application to AI technologies. The first related to the nature of safety risks caused by AI (biases in data or model, edge cases or other negative side effects), which may also be related to cybersecurity issues (malicious attempts to exploit AI vulnerabilities through evasion, data poisoning, model extraction, backdoor, etc.); as such, AI specific risks were not or were only partially covered by the EU legislation, while no specific safety or performance requirements were set for AI systems, as opposed to other software or ICT products, which can be highly problematic from a consumer protection perspective. The second concerns the lifecycle of an AI product, since under the existing legal framework ex-ante conformity assessments were conceptualized for products that are not subject to considerable change after entering the market, hence the inadequacy when applied to AI systems that – by design – are subject to modifications given their machine-learning capabilities.

Problem 2: Use of AI poses increased risk of violations of citizens' fundamental rights and Union values.
The use of AI can have a significant impact – both positive and negative - on the fundamental rights enshrined in the EU Charter of Fundamental Rights. Extensive literature proves that the use of AI systems present risks of violation of virtually all fundamental rights[150]: human dignity and personal autonomy, privacy and data protection, non-discrimination, right to an effective remedy, fair trial and good administration, all risks for which the pre-existing legal framework may not be adequate.

Problem 3: Authorities do not have powers, procedural frameworks and resources to ensure and monitor compliance of AI development and use with applicable rules.
Due to their specific technical characteristics, it may be difficult to assess the decision-making process involving an algorithmic output, thus not even public authorities may possess the appropriate technical capabilities and expertise to inspect the AI systems. Moreover, existing secondary legislation on data protection, consumer protection and non-discrimination legislation that relies on ex-post mechanisms of enforcement to find remedies for the single affected subject, but it does not allow for an ex-ante evaluation of compliance. The same holds true for the product

150 For an extensive overview of documented cases in which AI has been (partly) responsible for fundamental rights violations, see European Commission, Study to Support an Impact Assessment of Regulatory Requirements For Artificial Intelligence In Europe, Table 43 in Annex 1: Summary of AI risks to fundamental rights, Final report, April 2021.

safety legislation, which does not provide for specific safety requirements, neither for binding obligations to prior testing and validation before placing the AI system on the market, nor for post-market monitoring duties, regardless of it being an embedded or a stand-alone product. Furthermore, given the complexity of such technology, competent authorities may lack the necessary resources, expertise and technological tools to effectively supervise and carry out joint investigation with national authorities for possible violations of fundamental rights.

Problem 4: Legal uncertainty and complexity on how existing rules apply to AI systems dissuade businesses from developing and using AI systems.
Uncertainty around how to comply with existent legislation, given the complexity of the value chain for the development of an AI system, and the multiple levels of risk it presents, create challenges to the correct allocation of responsibility, which ultimately results in inadequate risk management. This is corroborated by the lack of harmonized standards over principles or requirements such as security, transparency, non-discrimination or fairness, accuracy, human oversight etc. to be adopted at the design and development stage, which affects the business's compliance mechanism and capacity to attract investments. Hence, the need for new laws or regulation to avoid a chilling effect on innovation.

Problem 5: Mistrust in AI would slow down AI development in Europe and reduce the global competitiveness of the EU economy.
Reluctance from consumers to accept the use of AI may cause businesses to face challenges in establishing a sufficient degree of credibility for certain AI-based products that suffer from a general lack of trust from the public.

Problem 6: Fragmented measures create obstacles for cross-border AI single market and threaten Union's digital sovereignty.
General legal uncertainty coupled with divergent legislative or regulatory initiatives from the Member States may cause market fragmentation, with adverse competitive effects on small businesses entering the market. The same conclusion applies to the possible proliferation of voluntary international technical standards for 'Trustworthy AI' adopted by international standardization organisations.

The **problem drivers** are to be identified in the specific characteristics of an AI system:[151]

1. Opacity, or the lack of transparency, makes it difficult to monitor, identify and prove possible breaches of laws, including legal provisions that protect fundamental rights.
2. Complexity makes it difficult to monitor, identify and prove possible breaches of laws, including legal provisions that protect fundamental rights.
3. Continuous adaptation and unpredictability may give rise to new risks that were not adequately addressed by the existing legislation.
4. Autonomous behaviour can affect safety because of the functional ability of an AI system to perform a task with no to little human intervention.
5. Functional dependence on the quality of data can reinforce systemic biases and errors and exacerbate discriminatory results.

3.9.2.2 Analysis of specific issues

- **The problems emerging as regards the definition of Artificial Intelligence**

There is a general agreement amongst stakeholders on a need for regulatory action, a narrow, clear and precise definition for AI, together with the criteria for AI risk-classification, to be determined on a sector and case-based approach. See stakeholders' consultation.

151 A deeper explanation of the five characteristics of AI that have an impact on the legal framework can be found in the Commission Staff Working Document, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 final, PART 2/2, p. 35.

- **The problems emerging as regards the risk classification of AI systems**

The criteria for classifying an AI system as high-risk are still uncertain. One such criterion may be related to the rights at stake. Extensive literature proves potential harmful impact of AI on fundamental rights, beyond the often-mentioned bias and discrimination caused by the deployment of machine learning algorithms. In fact, the emergence of a particular risk is determined not by the technology itself, but by the specific way it is used and the environment in which it is implemented. Similarly, if AI solutions are designed and implemented correctly, they could potentially enhance fundamental rights. This could be achieved through various means, such as allowing courts to offer fair and efficient proceedings to people, promoting freedom of expression by providing a more equitable and comprehensive news service, detecting external attempts to breach user privacy to protect the right to private life, and so on. The influence of AI systems and applications on fundamental rights, and other aspects, is largely influenced by the context and specific usage. Therefore, an assessment of the impact of a specific AI solution on fundamental rights should be conducted by the deploying entity. This highlights two important factors that relate to the accountability of deployers to implement measures to reduce the risk of significant violations of fundamental rights, such as the adoption of oversight arrangements that should not the dictated by a mere cost-efficiency balancing.
Example: the use of LLMs, such as ChatGPT, already available for wide use, brings new challenges as its risk classification would not be clear: it may fall within the low-risk category (codes of conduct) or transparency requirements?

- **The problems emerging as regards the conformity assessment procedure and the presumption of conformity under the liability regime**

There is a certain degree of disparity between conformity assessment of AI systems meant as safety components of a product, for which harmonised standards and compliance procedures may already be available, and those meant as stand-alone products that bear important fundamental rights implications, for which such standards may not exist, and common specifications are yet to be developed.
This creates also legal uncertainty from the product liability perspective. The framework advanced in the Proposed Regulation and the proposed liability framework are viewed as complementary: the former mainly aims to protect against risks to fundamental rights and safety from an ex-ante perspective, the latter concerns damages caused by AI from an ex-post angle, ensuring compensation should the risks materialize. Moreover, compliance with the requirements of the AI horizontal framework will be taken into account for assessing liability of actors under future liability rules. Article 4 of the Proposed AI Liability Directive lays down a rebuttable presumption of causality establishing a causal link between non-compliance with a duty of care or requirements under the Union law and the harmful output produced by the AI system, if the following cumulative conditions are met: first, the claimant has proved non-compliance with a certain EU or national obligation, relevant to the harm of an AI system caused the damage (Article 4 (1)(a)); second, it must be reasonably likely that, based on the circumstances of each case, the defendant's negligent conduct has influenced the output produced by the AI system or the AI system's inability to produce an output that caused the relevant damage(Article1(b)); third, the claimant has demonstrated that the output produced by the AI system or the AI system's inability to produce an output gave rise to the damage (Article 1(c)). These rules are accompanied by provisions granting national courts the power to order the disclosure of evidence about high-risk AI systems, according to the principles of necessity and proportionality to protect trade secrets and confidential information (Article 3). However, lacking harmonized standards, legal uncertainty arises with regards to both the presumption of conformity under the Proposed Regulation and the presumption, albeit rebuttable, of causality.

- **The problems emerging as regards the technical specifications or the harmonized standards**

The conformity assessment procedure which ensures presumption of conformity with the set requirements in the case of high-risk AI systems fundamentally relies on either technical specifications or harmonized standards. While

the latter must be issued by certain recognized standardisation organizations (ISO, IEEE, CEN, CENELEC)[152], the former may either the adopted by the European Commission, although no such obligation upon the Commission exists, or the AI system provider himself, according to the generally acknowledges state-of-the-art. However, this might impose, on the one hand, an unreasonably high duty of care onto the AI system's provider to ensure that the system is reasonably safe which may not be fully compatible with the fast pace at which AI technological solutions develops and advance, and on the other hand an unreasonably low duty of care that might result in harm and damage.
With regard to harmonized standards, scholars have raised concerns over the democratic legitimacy of the standardisation organizations, which are often private, to determine the standards for compliance. [153]
Finally, there may also possible divergent standardisation procedures among Member States, if harmonisation at EU level is not guaranteed.

- **The problems emerging as regards to the adoption of voluntary codes of conduct**

The adoption of non-binding ethical principles by companies in an effort to reassure customers about the safety and fundamental rights implications of AI is likely to continue, but this approach cannot build the necessary trust as it lacks enforcement mechanisms and leads to confusion for consumers who must navigate multiple commitments.

3.9.2.3 Impact of the legislative proposal

Interdependencies with other policy areas are found on a two-tier perspective.
The first one is the protection of fundamental rights, considered together with the relevant EU secondary legislation on data protection, non-discrimination, consumer protection, migration and asylum, judicial cooperation in criminal matters, financial services, and online platforms, depending on the practical use of the AI system. A tentative list of the concerned legislations is:

- The EU Charter of Fundamental Rights
- General Data Protection Regulation (Regulation (EU) 2016/679)
- Law Enforcement Directive (Directive (EU) 2016/680)
- Unfair Commercial Practices Directive (Directive 2005/29/EC)
- Proposed Revision of the Products Liability Directive (Directive 85/374/EEC)[154]
- Proposed AI Liability Directive[155]
- Directive 2013/36/EU on access to credit
- European strategy for data (Proposed European Data Governance Act, Proposed Data Act etc.)
- Regulation (EU) 2018/1807 on the free flow of non-personal data
- Digital Services Act (Regulation (EU) 2022/2065)
- Etc.

The second perspective concerns the relevant (horizontal and sectoral) product safety legislation. In fact, an AI system will be high-risk if it is a safety component of a product or a device which undergoes a third-party conformity assessment under the relevant sectoral NLF legislation, whose concerned legislations are listed as follows:

- Regulation (EU) 2019/1020 on market surveillance and compliance of products

152 See European Commission, DRAFT Request on a standardisation request to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) in support of safe and trustworthy artificial intelligence, 5 December 2022.

153 Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (SocArXiv, 5 July 2021) <https://osf.io/preprints/socarxiv/38p5f/> accessed 27 July 2022.

154 Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.

155 Proposal for a directive of the European Parliament and of the Council on adapting noncontractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.

- Regulation (EU) 1025/2012 on European standardization
- Directive 2001/95/EC on general product safety
- Directive 2006/42/EC on machinery (which is currently subject to review);
- Directive 2009/48/EU on toys;
- Directive 2013/53/EU on recreational craft;
- Directive 2014/33/EU on lifts and safety components for lifts;
- Directive 2014/34/EU on equipment and protective systems intended for use in potentially explosive atmospheres;
- Directive 2014/53/EU on radio-equipment;
- Directive 2014/68/EU on pressure equipment;
- Regulation (EU) 2016/424 on cableway installations;
- Regulation (EU) 2016/425 on personal protective equipment
- Regulation (EU) 2016/426 on gas appliances;
- Regulations (EU) 745/2017 on medical devices;
- Regulation (EU) 746/2017 on in-vitro diagnostic medical devices.
- Regulation (EU) 765/2008 on accreditation and market surveillance

Since conformity assessments already existing under the NLF will be kept in force and integrated with the AI horizontal framework, the competence of the Notified Bodies will be extended to include assessing compliance with AI requirements. The same principles apply to the operators along the AI value chain. With regard to market surveillance, Regulation (EU) 2019/1020 on market surveillance will apply to the AI horizontal framework, extending thus the competences of the market surveillance authority under the NLF. The horizontal framework on AI will establish new requirements for high-risk AI systems (e.g. transparency, documentation, data quality) that will be integrated into the existing old approach safety legislation, whose concerned legislations are listed as follows:

- Regulation (EU) 2018/1139 on Civil Aviation;
- Regulation (EU) 858/2018 on the approval and market surveillance of motor vehicles;
- Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles;
- Regulation (EU) 167/2013 on the approval and market surveillance of agricultural and forestry vehicles;
- Regulation (EU) 168/2013 on the approval and market surveillance of two- or three-wheel vehicles and quadricycles;
- Directive (EU) 2016/797 on interoperability of railway systems.
- Directive 2014/90/EU on marine equipment (which is a peculiar NLF-type legislation, but given the mandatory character of international standardization in that field, will be treated in the same way as old-approach legislation).

3.9.3 Alternative Solutions/Policies

The general objective of the policy intervention is to ensure the proper functioning of the single market by creating the conditions for the development and use of trustworthy AI. It entails the achievement of the following specific objectives:

1. set requirements specific to AI systems and obligations on all value chain participants in order to ensure that AI systems placed on the market and used are safe and respect the existing law on fundamental rights and Union values;
2. ensure legal certainty to facilitate investment and innovation in AI by making it clear what essential requirements, obligations, as well as conformity and compliance procedures must be followed to place, or use an AI system in the Union market;
3. enhance governance and effective enforcement of the existing law on fundamental rights and safety requirements applicable to AI systems by providing new powers, resources and clear rules for relevant authorities on conformity assessment and ex post monitoring procedures and the division of governance and supervision tasks between national and EU levels;

4. facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation by taking EU action to set minimum requirement for AI systems to be placed and used in the Union market in compliance with the existing law on fundamental rights and safety.

3.9.3.1 Listing of the Alternatives Considered

The Staff Working Document Impact Assessment (part 1/2) accompanying the Proposed Regulation[156] presents the different policy options and carries out a thorough comparison, accounting for their policy rationales and possible impact.

The analysed policy options are based on the following main dimensions:
a) The nature of the EU legal act (no EU intervention/ EU act with voluntary obligations/ EU sectoral legislation/ horizontal EU act);
b) Definition of AI system (voluntary/ ad hoc for specific sectors/ one horizontal definition);
c) Scope and content of requirements and obligations (voluntary/ ad hoc depending on the specific sector/ risk-based/ all risks covered);
d) Enforcement and compliance mechanism (voluntary/ ex ante or ex post only/ ex ante and ex post);
e) Governance mechanism (national, national and EU, EU only).

The policy options taken into consideration are briefly presented as follows:

Option 1: EU legislative instrument setting up a voluntary labelling scheme

Nature of act	An EU act establishes a voluntary labelling scheme, which becomes binding once adhered to
Scope	OECD definition of AI; adherence possible irrespective of the level of risk, but certain risk differentiation amongst the certified AI systems also possible
Content	Requirements for labelled AI systems: data, transparency and provision of information, traceability and documentation, accuracy, robustness and human oversight (to be ensured by providers who choose to label their AI system)
Obligations	Obligations for providers (who voluntarily agree to comply) for quality management, risk management and ex post monitoring. No obligations for users of certified AI systems (impractical given the voluntary character of the label aimed at certification of specific AI systems)
Ex-ante enforcement	Self-assessment and ex ante check by national competent authorities responsible for monitoring compliance with the EU voluntary label
Ex-post enforcement	Ex post monitoring by national competent authorities responsible for monitoring compliance with the EU voluntary label
Governance	National competent authorities designated by Member States as responsible for the EU label + a light EU cooperation mechanism

Table 1

Option 2: A sectoral 'ad-hoc' approach

Nature of act	Case-by-case binding sectoral acts (review of existing legislation or ad hoc new acts)
Scope	Different sectoral acts could adopt different definitions of AI that might be inconsistent. Each sectoral act will determine the risky AI applications that should be regulated.

156 Commission Staff Working Document, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 final, PART 1/2, p. 36 ff.

Content	Sector specific requirements for AI systems (could be similar to Option 1, but adapted to sectoral acts). Additional safeguards for specific AI use cases: - Prohibition of certain harmful AI practices - Additional safeguards for permitted use of remote biometric identification (RBI) systems, deep fakes, chatbots.
Obligations	Sector specific obligations for providers (could be similar to Option 1, but adapted to ad hoc sectoral acts). Sector specific obligations for users depending on the use case (e.g. human oversight, transparency in specific cases etc.)
Ex-ante enforcement	Would depend on the enforcement system under the relevant sectoral acts For use of remote biometric identification (RBI) systems at publicly accessible spaces (when permitted): prior authorisation required by public authorities
Ex-post enforcement	Ex post monitoring by competent authorities under the relevant sectoral acts
Governance	Would depend on the existing structures in the sectoral acts at national and EU level; no platform for cooperation between various competent authorities.

Table 2

Option 3: Horizontal EU legislative instrument establishing mandatory requirements for high-risk AI applications

Nature of act	A single binding horizontal act following a risk-based approach
Scope	OECD definition of AI (reference point also for other sectoral acts); clear methodology and criteria how to determine what constitutes a high-risk AI system
Content	Risk-based approach: a. Prohibited AI practices and additional safeguards for the permitted use of remote biometric identification systems in publicly accessible spaces (as per Option 2) b. Horizontal requirements as per Option1, but binding for high-risk AI and operationalized through harmonised standards c. Minimal transparency for non-high-risk AI (inform when using chatbots and deep fakes as per Option 2) +Measures to support innovation (sandboxes etc.)
Obligations	Binding horizontal obligations for all actors across the value chain: a. Providers of high-risk AI systems as per Option 1 + conformity (re-) assessment, reporting of risks/breaches etc. b. Users of high-risk AI systems (human oversight, monitoring, minimal documentation)
Ex-ante enforcement	Providers: a. Third party conformity assessment for high-risk AI in products (under sectoral safety legislation) b. Mainly ex ante assessment through internal checks for other high-risk AI systems + registration in a EU database Users: Prior authorisation for use of Remote biometric identification in publicly accessible spaces (as per Option 2)
Ex-post enforcement	Ex post monitoring by market surveillance authorities designated by Member States
Governance	Governance at national level with a possibility for joint investigations between different competent authorities + cooperation at EU level within an AI Board

Table 3

Option 3+: Horizontal EU legislative instrument establishing mandatory requirements for high-risk AI applications + voluntary codes of conduct for non-high risk applications

Nature of act	Option 3 + code of conducts non high-risk AI
Scope	Option 3 + voluntary codes of conduct non-high-risk AI
Content	Option 3 + industry-led codes of conduct for non-high-risk AI

Obligations	Option 3 + commitment to comply with codes of conduct for non-high-risk AI
Ex-ante enforcement	Option 3 + self- assessment for compliance with codes of conduct for non-high-risk AI
Ex-post enforcement	Option 3 + unfair commercial practice in case of non-compliance with codes
Governance	Option 3 + without EU approval of the codes of conduct

Table 4

Option 4: Horizontal EU legislative instrument establishing mandatory requirements for all AI applications, irrespective of the risk they pose

Nature of act	A single binding **horizontal act**, **applicable to all AI**
Scope	OECD definition of AI; applicable to all AI systems without **differentiation between the level of risk**
Content	Same as Option 3, but applicable to all AI systems (irrespective of risk)
Obligations	Same as Option 3, but applicable to all AI systems (irrespective of risk)
Ex-ante enforcement	Same as Option 3, but applicable to all AI systems (irrespective of risk)
Ex-post enforcement	Same as Option 3, but applicable to all AI systems (irrespective of risk)
Governance	Same as Option 3, but applicable to all AI systems (irrespective of risk)

3.9.3.2 Comparison of Alternatives

Table 11: Summary of the comparison of options against the four criteria

	EFFECTIVENESS				EFFICIENCY (cost-effectiveness)	COHERENCE	PROPOR-TIONALITY
	Objective 1	Objective 2	Objective 3	Objective 4			
Baseline scenario	0	0	0	0	0	0	0
Option 1: Voluntary labelling	0	0	0	+	++	+	+
Option 2: Ad-hoc legislation	+	+	+	+	++	+	+
Option 3: High risk only	++	++	++	++	++	+++	+
Option 3+: High risk + Codes of conduct	++	++	++	+++	++	+++	+
Option 4: All AI	+++	++	+++	++	0	+++	0

Notabene: table annotations should only be read in vertical; in the table, for options 3, 3+ and 4 it is assumed that ex-ante third party conformity assessments are mandatory for AI systems that are safety components of products and for remote biometric identification in publicly accessible spaces; "0" means same as baseline, "+" means partially better than baseline, "++" means better than baseline, "+++" means much better than baseline

Source: European Commission Staff Working Document Impact Assessment accompanying the Proposed Regulation part 1/2

Figure 4

The following criteria are used in assessing how the options would potentially perform, compared to the baseline:

1. **Effectiveness** in achieving the specific objectives (see above the four specific objectives)

Specific objective 1: Ensure that AI systems placed on the market and used are safe and respect the existing law on fundamental rights and Union values

- Option 1's effectiveness in limiting risks for individuals regarding labeled applications is uncertain, as it relies on consumer demand and may not encourage all high-risk applications to apply for the label.

- Option 2 would limit risks for individuals in cases where action has been taken with tailored obligations for AI applications, but it would not protect against potential risks by other AI applications and would be limited to specific sectors.
- Option 3 effectively limits risks to individuals by setting requirements and ex ante conformity assessments for high-risk AI applications, establishing post-market monitoring, and enabling additional AI applications to be added as needed, making it more effective than the baseline.
- Option 3+ would have the same legal effectiveness as Option 3 but would also allow companies to voluntarily fulfill obligations for AI applications that are not classified as high risk, reducing overall risk of violation and making it more effective than the baseline.
- Option 4 would comprehensively limit risks for individuals by setting requirements for all AI applications, making it much more effective than the baseline in achieving this objective.

Specific objective 2: Ensure legal certainty to facilitate investment and innovation in AI.

- Option 1 lacks legal certainty and could discourage investment in AI due to uncertainty around the application of EU regulations to AI.
- Option 2 would improve investment and innovation conditions by providing legal certainty only for applications that have been regulated.
- Option 3 would provide legal certainty to AI developers and users by defining high-risk AI applications and requirements for compliance, improving conditions for investment and innovation and making it more effective than the baseline in achieving objective 2. However, regulatory changes may still occur over time and would be supported by a group of experts and national administrations.
- Option 3+: the additional code of conduct scheme for medium to low-risk applications would improve conditions for investment and innovation, making it more effective.
- Option 4 would provide legal certainty to all AI applications, but may increase legal complexity unnecessarily for applications with low risk, making it more effective than the baseline in achieving objective 2, but potentially at the cost of increased complexity.

Specific objective 3: Enhance governance and effective enforcement of the existing law on fundamental rights and safety requirements applicable to AI systems

- Option 1 would only moderately improve enforcement for labeled applications and would be more complicated than the baseline due to coexisting national legislative frameworks, making it ineffective.
- Option 2 would improve enforcement and governance for regulated applications, but the complications arising from different sectorial legislation would make overall enforcement and governance more complicated.
- Options 3, 3+, and 4 would all lead to improved enforcement of AI regulations through ex-ante verification and ex-post compliance assessment. National authorities would have enhanced competences, funding, and expertise, and would be able to cooperate in joint investigations at national and cross-border levels.

Specific objective 4: Facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation

- Option 1 would improve the baseline by establishing common requirements and a voluntary label, allowing consumers to choose trustworthy products. However, it only applies to labeled applications, which could lead to market fragmentation if Member States take additional legislative action, thus it would only be partially effective.
- Option 2 would improve the baseline for products covered by ad-hoc legislation, but not for other products. There is a risk of fragmentation of the single market for products not covered by ad-hoc legislation.
- Option 3 would be more effective by providing a clear improvement that allows consumers and businesses to rely on a European framework for lawful, trustworthy, and safe AI applications. The legislation covers high-risk applications, while low-risk products are likely to avoid fragmentation of the single market.
- Option 3+ would have all the same effects of option 3, with the added benefit of increasing trust by businesses and consumers.
- Option 4 would create a comprehensive increase in trust, but the increase in costs for all AI applications may lead to fewer AI applications being offered, thus potentially leading to a smaller market than otherwise.

2. **Efficiency**: cost-benefit ratio of each policy options in achieving the specific objectives;

- Option 1's costs would be similar to option 3 on a per-application basis, but with a less precise targeting of costs and potential for higher or lower aggregate costs, although participation is voluntary and thus cost-effective, and public administrations would still need to bear the costs of supervising the system.
- Option 2 has low overall costs for AI providers and users, but the costs for each application can be significant and compliance may be complicated due to specific regulations; public administrations would only incur costs in specific areas and the costs of determining high-risk applications would correspond to the choice of applications to be regulated, making it a cost-effective option.
- Option 3's costs mainly consist of compliance and verification costs for a small number of high-risk AI applications, but its precise targeting and unified requirements allow for inexpensive and reusable compliance procedures, with limited costs for public administrations and policy-makers, making it a cost-effective option with a strong positive impact on high-risk applications where it is most needed.
- Option 3+: the voluntary character of the codes of conduct ensures cost effectiveness.
- Option 4 would not be cost effective as it has the highest aggregate costs for AI providers and users, and requires significantly more resources for monitoring and enforcement by public administrations, despite covering all AI applications.

3. **Coherence** with other policy objectives and initiatives;

All options align with existing legislation on safety and fundamental rights, promote or impose obligations to implement existing legislation, and aim to prevent barriers to cross-border commerce; however, options 1 and 2 are only partially coherent with European policy, while options 3, 3+, and 4 are fully coherent and contribute to the digital transformation of the European economy.

4. **Proportionality**: whether the options go beyond what is a necessary intervention at EU level in achieving the objectives.

Options 1, 2, 3, and 3+ all implement procedures that are proportionate to their objectives, with option 1 imposing burdens only on voluntary companies, option 2 imposing burdens only for addressing specific problems, and options 3 and 3+ imposing targeted requirements for high-risk applications, while option 4 imposes disproportionate burdens across all AI applications.

As a result from the comparison of the options, **the preferred option is option 3+,** a regulatory framework for high-risk AI applications with the possibility for all non-high-risk AI applications to follow a code of conduct. Overall, this option strikes a balance between ensuring safety and fundamental rights protection while also allowing for innovation and development in the field of AI.

3.9.3.3 Constraints, Including Political ones

The policy options were evaluated against the following economic and societal impacts, with a particular focus on impacts on fundamental rights. For the scope and purpose of the present legislative analysis, specific focus will be put on the preferred option 3+ and the actual provisions as laid down in the Proposed Regulation, although a thorough study is available also for the alternative options.[157]

- **Economic impacts**

With regard to the functioning of the internal market, Options 3 and 3+ provide a comprehensive regulatory framework for sensitive or high-risk application areas and a European approach for low-risk applications, eliminating the need for additional legislation by Member States, with a mechanism in place for future amendments.

157 For a thorough analysis of the policy options and their possible economic and societal impact see Commission Staff Working Document, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 final, PART 1/2, p. 64 ff.

Concerning the impact on the uptake of AI, the EU currently lags behind the US in AI adoption, but faster uptake by companies could lead to significant economic benefits, and the regulatory framework can increase trust and legal certainty for AI users and suppliers, with Option 3 and 3+ targeting high-risk cases, while Option 4 is best suited for increasing trust for many applications.

Further considerations are relevant in terms of compliance costs and administrative burdens. In fact, the costs are calculated relative to the baseline scenario not taking into account potential national legislation. However, if the Commission does not take action, Member States would be likely to legislate against the risks of artificial intelligence. This could lead to similar or even higher costs if undertakings were to comply with distinct and potential mutually incompatible national requirements. A comprehensive study on the compliance costs generated by the Proposed Regulation is carried out in the Final Report carried out by the European Commission.[158] The costs estimates for regulatory intervention in AI are based on a Standard Cost Model that assesses the required time and evaluates costs based on the reference hourly wage rate for the IC sector, which represents the theoretical maximum of costs and assumes that all businesses need to adopt measures to comply with every requirement set out, but for companies that already fulfil certain specific requirements, the corresponding cost for these specific requirements would be zero (e.g. if they already ensure accuracy and robustness of their system).
In option 3 there would be five sets of requirements, concerning i) data; ii) documentation and traceability; iii) provision of information and transparency; iv) human oversight; and v) robustness and accuracy. However, economic operators would already take a certain number of measures even without explicit public intervention (e.g. with regard to robustness and accuracy), whereas for the other requirements, operators would also take some measures by themselves, which would however not be sufficient to comply with the legal obligations, which may require additional expenditure to ensure compliance. Assuming the set of all the requirements, under option 3 the theoretical maximum compliance costs of algorithmic transparency and accountability per AI application would amount to around €10.000 per companies following standard business procedure.
In addition to minimum compliance costs, one may need to account for verification costs. Under option 3+, for AI systems that are safety components of products under the new legislative approach, the requirements of the new framework would be assessed as part of the already existing conformity assessments which these products undergo. Provided that harmonised standards exist and the providers have applied those standards, they could replace the third-party conformity assessment with an ex-ante conformity assessment through internal checks applying the same criteria. All other high-risk applications would equally be assessed via ex-ante conformity assessments through internal checks applying the same criteria.
Option 3+ incurs additional costs for verifying data accuracy through random checks on companies with a code of conduct. The fees will be paid by participating companies and will only be a fraction of the total verification expenses.

Regarding SMEs, Options 3 and 3+ focus on a few high-risk AI applications and impose only necessary transparency and accountability requirements, minimizing costs and administrative overhead. This approach benefits SMEs and includes automatic record-keeping of user data through system logs. These options also propose the use of regulatory sandboxes to provide guidance and minimize legal risks for SMEs testing innovative AI solutions, allowing for a proportionate application of rules and facilitating compliance in the pre-market phase.

From a competitiveness and innovation perspective, given the size of the EU market, which one fifth of the world market, it is very unlikely that the limited additional costs of algorithmic transparency and accountability would really prevent the introduction of this technology to the European market. Moreover, option 3+ provides legal certainty for AI providers and users, ensuring that their application is lawful and enabling them to invest and innovate with AI, thereby increasing competitiveness.

- **Costs for public authorities**

While it is true that in-house conformity assessment as well as third-party conformity assessment would be funded by the companies, Member States would have to designate a supervisory authority in charge of implementing the legislative requirements and/or the voluntary labelling scheme, including market monitoring.

158 European Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, April 2021, p. 113 ff.

- **Social impact**

Options 3 and 3+, setting requirements for training data in high-risk applications can contribute to reducing involuntary discrimination by AI systems, especially in areas like recruiting and career management. This would improve the situation of disadvantaged groups and lead to greater social cohesion. Option 3 would address the most pertinent applications in the health sector, while option 3+ would give other AI applications the opportunity to prove their trustworthiness, even if they are not strictly high-risk. Increasing the uptake of AI applications will lead to additional labor market impacts of AI, where the net balance of job loss, creation, and transformation is uncertain: it has important implications for skills, both in terms of requiring high-level AI skills and expertise and in ensuring that people can effectively use and interact with AI systems across a wide range of applications. Nonetheless, the uptake of AI will accelerate the development of socially beneficial applications, such as in education, culture, or youth, by enabling new forms of personalized education and collaboration. Furthermore, AI applications have the potential to improve health outcomes through better prevention, diagnosis, and treatment.

- **Impacts on safety**

Options 3 and 3+ would subject a larger scope of AI systems to AI-specific requirements, reducing risks to safety from the introduction of AI applications. Harmonized implementation of requirements would ensure legal certainty, consistency, and safety for products and services, avoiding a sectoral approach to tackling AI risks. Additionally, a horizontal instrument would provide harmonized requirements for managing evolving risks, which would be valuable to AI providers and users operating in several sectors. Streamlining the process of development and adoption of harmonized standards on AI systems would support compliance with relevant rules, and integration of AI requirements into conformity assessment procedures would minimize the burden on sector-specific providers and operators. Option 3+ introduces a system of codes of conduct for companies supplying or using low-risk AI, which could encourage them to ensure a higher safety baseline for their products voluntarily.

- **Impacts on fundamental rights**

Options 3 and 3+ propose a horizontal framework for regulating AI systems to ensure consistency and address cross-cutting issues related to fundamental rights protection. This framework will establish common requirements for trustworthy AI applicable across all sectors and prohibit certain AI practices that contravene EU values. It will also impose specific requirements relating to the quality of data, documentation, transparency, human oversight, robustness, and accuracy of AI systems, which are expected to mitigate risks to fundamental rights and improve the effective enforcement of existing legislation. The codes of conduct in option 3+ will encourage companies supplying or using low-risk AI to ensure a higher safety baseline for their products, even if they are low-risk. This is expected to enhance trust in AI technology, stimulate its uptake, and promote a range of political, social, and economic rights while minimizing risks and addressing the problems identified.

- **Environmental impacts**

Although the requirements do add some tasks related to testing and keeping records, it is important to note that most of the energy consumed during machine learning occurs during the training phase. Therefore, the additional energy consumption would only occur if a large-scale retraining is required, which may happen initially but developers are expected to find ways to avoid it due to the high costs involved. The indirect environmental impacts of the proposed measures are significant. The increase in trust resulting from the measures will lead to more AI development and usage, including in lower-risk applications. AI can also benefit the environment through its superior efficiency compared to traditional technology, such as reducing the amount of resources needed in process optimization and improving vehicle automation and traffic management. AI can also be directed towards improving the environment, such as helping with pollution control and modeling the impact of climate change mitigation or adaptation measures. Policies can encourage the minimization of resource usage and energy consumption through technical solutions such as efficient cooling systems, heat reuse, and renewable energy. The Commission will

consider options to promote AI solutions that have a neutral or positive impact on climate change and the environment.

3.9.4 Recommendations

A. Description of Policy Recommendation(s) and recommendations for other stakeholders
B. Rationale for Recommendation(s)
While convincing arguments for adopting Option 3+ were made, it is worth to point out that the final text of the Proposed Regulation is still under discussion for amendments at the European Parliament.[159] Proposals for modifications have been put forth from the following Committees:

- Committee on Transport and Tourism (12 July 2022)
- Committee on the Environment, Public Health and Food Safety (22 April 2022)
- Committee on Culture and Education (16 June 2022)
- Committee on Industry, Research and Energy (14 June 2022)
- Committee on Legal Affairs (12 September 2022)
- Committee on the Internal Market and Consumer Protection Committee on Civil Liberties, Justice and Home Affairs (14 June 2022)

3.10 PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HORIZONTAL CYBERSECURITY REQUIREMENTS FOR PRODUCTS WITH DIGITAL ELEMENTS AND AMENDING REGULATION (EU) 2019/1020 COM(2022) 454 FINAL (CYBER RESILIENCE ACT)

3.10.1 Executive Summary

On September 15th, 2022, the European Commission approved a proposal for a new regulation aimed at defining horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 of the European Parliament and of the Council, on market surveillance and compliance of products. This regulation will apply to all products with digital elements, except those specifically indicated in Article 1, which are already regulated by other European regulations. In particular, excluded from the regulation are: medical devices for human use (EU Regulation 2017/745) and *in vitro* medical diagnostic devices with the same intended use, together with their related accessories (EU Regulation 2017/746); products with digital elements certified under Regulation (EU) 2018/1139, concerning high and uniform levels of civil aviation safety, as well as those already regulated by Regulation (EU) 2019/2144, concerning the approval requirements for motor vehicles and their trailers, as well as systems, components and technical entities intended for such vehicles, with regard to their general safety and the protection of vehicle occupants and vulnerable road users. For the purposes of this regulation, "*products with digital elements*" are defined as "*any software and hardware product and its related remote data processing solutions, including software or hardware components to be placed on the market separately*" (Article 3).

One of the key issues addressed by the regulation in Articles 10 and following, is the provision of specific obligations on economic operators, namely manufacturers, importers and distributors of hardware and software products, to ensure that the product is monitored and controlled, in terms of cybersecurity, at every stage of its lifecycle. Manufacturers, first and foremost, are obliged to verify that the product has been designed in compliance with the requirements indicated by the regulation, through the cybersecurity risk assessment: this is an evaluation of cybersecurity risks, the evidence of which must be taken into account from the design phase of the product to its use, in order to achieve one of the objectives of the regulation, namely to minimize any accidents related to the

159 References to the amendments can be found here: https://artificialintelligenceact.eu/documents/, accessed 4 April 2023.

cybersecurity of devices with digital elements. Complementary to this duty is the obligation to document the product's risks and vulnerabilities, managing them for a period of five years from the product's entry into the market and promoting informative policies for final consumers. Manufacturers are also required to notify ENISA (EU Agency for Cybersecurity) of any vulnerabilities or accidents related to the product, with the consequent duty of communication to users of such accidents. Following these precautions adopted by the manufacturer, the control process continues with some obligations on the importer, who, in addition to verifying that the manufacturer has carried out conformity assessments and prepared the required documentation, is required to make sure that the product bears the CE marking and is accompanied by the information specified in Annex II of the regulation. Finally, before placing the product on the market, the importer must verify the product's compliance to the essential requirements specified in Annex I. As for the duties of distributors, the regulation provides that, in addition to carrying out further checks on the CE marking, they must oversee the activities of manufacturers and producers, verifying that both have properly fulfilled their obligations.
Therefore, the regulation aims to ensure, through the cooperation of individual economic operators, a constant high level of safety for products with digital elements, achievable only through the fulfillment of all the obligations specified therein. Compliance with all these requirements therefore allows the benefit, on the market, of only products that meet the essential requirements of cybersecurity laid down in the regulation, in particular in Annex I. In order to ensure that economic operators comply with these obligations, the proposal for a regulation also provides for appropriate financial administrative penalties (art. 53) to be imposed by each Member State, when the latter becomes aware that a product does not comply with the cybersecurity requirements laid down in the Annexes to the regulation.

3.10.2 Analysis of the Legislation

3.10.2.1 Background of the legislative act

The European legislator was induced to enact the regulation under review due to the increasing number of cyber-attacks against hardware and software products whose cybersecurity is not regulated by any European legislation in the majority of cases - particularly with regard to non-incorporated software -. For example, the cyber-attack known as "*WannaCry*", which affected many organizations worldwide, as well as several national healthcare systems in 2017. In order to avoid such risks and to adopt sufficient minimum requirements for cybersecurity of products, it was therefore felt necessary to intervene at a supranational level, given that the adoption of different regulations by individual Member States could have hindered the creation of an open and competitive single market for products with digital elements. In particular, as specified in the introductory report to the text of the regulation, these products suffer from two problems that bring costs for both users and society, namely: 1) a low level of cybersecurity, which leads to greater vulnerability of the products themselves, as well as significant difficulty in developing security updates that can remedy these risks; 2) the inability to provide with understandable and accessible information to the user that can guide him in choosing products with adequate cybersecurity properties, as well as in their use. To counter further incidents, the aforementioned legislation aims to act on the characteristics of the products and the information provided to the consumer, in order to, first of all, fill existing gaps on the subject at a supranational level, and secondly, to achieve the following four objectives: 1) improve the cybersecurity of products from the production phase to their entire life cycle; 2) ensure a consistent framework for cybersecurity to facilitate compliance for hardware and software manufacturers; 3) implement transparency; 4) enable safe use of these products by businesses and consumers. This proposal is therefore part of the European strategy on digital matters, which already includes numerous legislative acts regulating some cybersecurity issues, namely: 1) Directive (EU) 2013/40 of the European Parliament and of the Council, concerning attacks against information systems; 2) Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of networks and information systems, also known as the "NIS directive," which has subsequently been revised and became the "NIS2 directive"; 3) Regulation (EU) 2019/881 of the European Parliament and of the Council, on cybersecurity and, in particular, on the certification of cybersecurity in order to improve TIC products, services, and processes.

The proposal under review is adequately thorough in relation to the needs that led to the intervention of the European legislator. The need to strengthen cybersecurity at the European level arises, in particular, from several large-scale cyber-attacks that have highlighted the importance of addressing these issues from a perspective of: implementation of the internal market; legal certainty; increase trust in products by users and the resulting greater attractiveness of the products; creation of a more level playing field among product sellers.

The introductory report to the regulation lists several legislative acts adopted before the current regulation that addressed some aspects of cybersecurity, albeit together with other issues, namely: 1) Directive (EU) 2013/40 of the European Parliament and of the Council, concerning attacks against information systems; 2) Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of networks and information systems, also known as the "NIS directive," which has subsequently been revised and became the "NIS2 directive"; 3) Regulation (EU) 2019/881 of the European Parliament and of the Council, on cybersecurity and, in particular, on the certification of cybersecurity in order to improve TIC products, services, and processes. Additionally, the need to introduce legislation containing specific cybersecurity requirements was explicitly expressed in some European Union programmatic and policy documents, such as: a) the EU's cybersecurity strategy for the digital decade; b) the Council's conclusions of 2 December 2020 and 23 May 2022; c) the European Parliament's resolution of 10 June 2021.
The report accompanying the text of the regulation explicitly highlights the importance that the cybersecurity of products covers, in terms of risks, from individual consumer to the global society. The numerous (and sophisticated) cyber-attacks that have occurred in recent years due to a low level of cybersecurity of products with digital elements have affected not only the individual user (in terms of privacy compromise) but also, given their evident transboundary dimension, entire organizations, and supply chains, thereby having significant economic consequences, so much as to estimate the cost of cybercrime for 2021 amounting to €5.5 trillion.

3.10.3 Analysis of specific issues

From the proposal under examination, several problematic aspects emerge regarding data/products/services, which can be distinguished as follows:
1. As regards the data, the issue of ensuring a higher level of security/protection emerges, given the need to protect them from the risk of theft and manipulation caused by the numerous cyber-attacks that have occurred in recent years;
2. With regard to the products, the diversity of products on the market could determine a different level of vulnerability and risk, resulting in difficulties in identifying and applying a common security standard for all and the problem that arises in having a product able to apply digital services is related to an easier risk of cyber-attacks against users.

3.10.3.1 Impact of legislation

The consequences of the application of this proposed regulation would undoubtedly be extremely advantageous for different categories of subjects, as well as, in the first place, for the European Union, in order to reduce the costs that it currently incurs due to the incidents suffered by companies, which amount to around 180-290 billion per year. In addition to the EU, also the companies themselves could not only be subject to a single regulation on cybersecurity of products with digital elements, but also see their reputation increase worldwide, thanks to the possibility of selling such products in non-EU countries. Finally, the benefits of this proposal would also involve end-users of the product, who, in addition to obtaining greater transparency of security properties with consequent ease of use of products with digital elements, would also enjoy a stronger guarantee of fundamental

rights, with particular reference to the protection of life and personal data. On the other hand, the benefits resulting from such regulation could lead to an increase in the market costs of products with digital elements, to the detriment of users, intended as commercial users, consumers, and citizens. Similarly, in order to comply with the new security standards, software developers and hardware manufacturers should incur new direct costs, together with those deriving from conformity assessments and documentation and reporting obligations. However, the main consequence explicitly desired by the proposal would be to implement the security of products with digital elements to increase consumers' confidence in them and to reduce, once and for all, the risks arising from cyber-attacks.
On the issues addressed in the proposed regulation, in the opinion of the writer, there is no jurisprudence that addresses the subject in question, except for the abundant decisions of the Court of Justice of the European Union in relation to the protection and processing of personal data, a topic that is only marginally addressed in this proposal.

3.10.3.2 Interdependencies with other policy areas

The main interdependence of the regulation is between the latter and Regulation (EU) 2016/679 of the European Parliament and of the Council, concerning the protection of personal data. The essential cybersecurity requirements identified by the regulation under examination should contribute to improving the protection of personal data and, in general, people's lives. However, further relationships can be obtained from the reference made in the proposal to the following legislative acts: Regulation (EU) 2017/745 of the European Parliament and of the Council, concerning medical devices; Regulation (EU) 2017/746 of the European Parliament and of the Council, concerning *in vitro* diagnostic medical devices; Regulation (EU) 2019/2144 of the European Parliament and of the Council, concerning the approval requirements for motor vehicles and their trailers, as well as systems, components and technical entities intended for such vehicles, with regard to their general safety and the protection of vehicle occupants and vulnerable road users; Regulation (EU) 2018/1139 of the European Parliament and of the Council, laying down common rules in the field of civil aviation; Directive 85/374 of the Council, concerning the approximation of the laws, regulations and administrative provisions of the Member States on liability for defective products.

3.10.4 Alternative Solutions/Policies

3.10.4.1 Listing of the Alternatives Considered

In order to achieve the set goal, namely to identify the minimum requirements for horizontal cybersecurity, four strategic options/alternatives have been considered and examined: 1) adopting a non-binding soft law approach, addressing these issues through communications, guidelines, recommendations, and possible codes of conduct, without issuing any mandatory regulatory acts; 2) intervening on horizontal cybersecurity with specific acts concerning individual products; 3) adopting a mixed approach, including mandatory rules for cybersecurity of tangible products with digital elements and their incorporated software, and a staggered approach for non-incorporated software; 4) intervening with a regulatory act containing cybersecurity requirements for tangible and intangible products, including non-incorporated software. The list of the alternatives given is complete but there is no explanation as to why some alternatives were chosen for further analysis.
As a matter of facts, the proposal lists the advantages and sometimes the disadvantages of each alternative outlined, without delving into one or more in particular, except to explain the reasons why option number 4 was ultimately preferred and chosen.

3.10.4.2 Comparison of Alternatives

In order to compare the alternatives listed in the regulation proposal, especially in terms of cost-benefit analysis, it is necessary to individually analyze the various options:
1) The option n. 1, which involves the voluntary promotion of cybersecurity standards, is undoubtedly the least expensive alternative among those identified, but also the riskiest for consumers and product users, as it would imply the adoption of different standards in each Member State and therefore not uniform at the European level;
2) Even the option n. 2, which is certainly more expensive than the first, would involve the application of a fragmented discipline, providing such alternative specific *ad hoc* interventions for each product with digital elements, which would modify the already established cybersecurity requirements. From a benefits perspective, a targeted intervention such as that of option n. 2 would allow for greater attention to the peculiarities, risks, and cybersecurity needs of each individual product with digital elements;
3) The option n. 3, called "mixed," would exclude non-incorporated software from regulation, as it provides for the adoption of mandatory horizontal rules for the cybersecurity of tangible products with digital elements and only incorporated software;
4) Finally, the adopted option is the number 4, which is defined by the proposal as the most cost-effective alternative in terms of cost-benefit ratio. There are indeed multiple benefits derived from the adoption of mandatory regulation on cybersecurity requirements. This alternative allows for: defining specific cybersecurity requirements for all products with digital elements introduced or made available in the internal market; considering the entire digital supply chain; including non-incorporated software in the discipline, which is often exposed to significant vulnerability risks; imposing duties of diligence for the entire product life cycle, and even for the moment after it is placed on the market. The advantages that this option would bring to various stakeholders are also significant, in particular: for businesses, as it would reduce compliance costs, reduce the risks of cyber-attacks, resulting in a reduction in management costs and damage to reputation, and finally prevent the adoption of divergent security regulations; for the entire EU, it would reduce the costs of accidents, resulting in increased revenue from increased demand for products with digital elements; finally, users could enjoy greater transparency in terms of product security, along with an increase in the protection of their fundamental rights, such as privacy and personal data. Being the most rigorous approach among those listed, it is certainly also the most expensive, but at the same time, the safest for consumers and users of products with digital elements.

3.10.4.3 Constraints, Including Political

One of the most evident constraints is the technical one, resulting from the diversity of products with digital elements present and circulating on the European, as well as the global market. This variety implies greater difficulty in establishing standardized cybersecurity requirements for all existing products. This diversity is also reflected in the complexity of some products, which makes it more challenging to ensure a high level of security for these devices. Another emerging constraint from the proposal is economic, concerning costs. This proposal would indeed produce an increase in compliance and application costs not only for companies but also for notifying bodies and public authorities, as well as hardware manufacturers and software developers. The latter would also have to bear the additional cost increase for the new security requirements imposed by the regulation, for reporting and documentation obligations. Such burdens could constitute a constraint on technological innovation, as companies may feel discouraged from producing new technological devices due to compliance costs. From a feasibility standpoint, compliance with the chain of control, and thus with all the cybersecurity obligations imposed on suppliers, distributors, and manufacturers of products with digital elements, implies that they have been correctly trained to carry out these activities, so as to have sufficient technical knowledge in the sector. Therefore, the level of specialization required of economic operators can indeed be a constraint on implementing the regulation.

3.10.5 Recommendations

In the opinion of the writer, the proposal does not provide a detailed description of the political recommendations and those directed to other stakeholders. However, the text suggests various recommendations, the main ones of

which are addressed: to the Member States and the European Union, to achieve a single policy on cybersecurity, thanks to adherence and collaboration in implementing the regulation, and in order to quickly suppress possible cyber-attacks, also through strengthening market surveillance; to suppliers, importers, and distributors, to disseminate and make known to consumers and users the main information about the risks and safe use of products with digital elements, to promote more conscious use. The recommendations outlined in this proposal aim to promote and encourage greater awareness of the importance of cybersecurity throughout the product lifecycle, from production to use. To achieve a high level of security, it is necessary that all stakeholders involved collaborate to ensure a proper balance between security needs and innovation needs that lead to the creation of devices with increasingly complex and potentially risky digital elements.

ANNEX: Summary of Policy considerations for stakeholders in the form of a short brief (to publish online)

Focus: **The global problem of the cybersecurity of products with digital elements: what can be done?**

The proposal for the European regulation on horizontal cybersecurity requirements for products with digital elements aims to finally solve the problems caused worldwide by the frequent cyber-attacks. Such attacks, facilitated by the current low level of cybersecurity in digital products, pose significant risks and damages, especially regarding the protection of personal data of individual citizens/users. To remedy this situation, the regulation aims to establish minimum cybersecurity requirements, whose implementation involves the help and participation of various stakeholders, such as: manufacturers, importers and distributors of hardware and software products, and finally end-users. For these economic operators, the regulation under exam provides many obligations so that the products are monitored and controlled since the production stage. To fulfill these obligations, economic operators have to bear costs that they had never supported until then as well as having a solid specialization to properly carry out the activities required by the regulation. On the other hand, respect for all these activities would mean a safer use of the product as well as the possibility of selling it at a higher price and also in non-European markets. So, the imposition of obligations on manufacturers, importers and distributors of hardware and software is balanced by

3.11 PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON HARMONISED RULES ON FAIR ACCESS TO AND USE OF DATA (DATA ACT) COM/2022/68 FINAL

3.12 PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE EUROPEAN HEALTH DATA SPACE COM(2022) 197 FINAL

3.13 DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 6 JULY 2016 CONCERNING MEASURES FOR A HIGH COMMON LEVEL OF SECURITY OF NETWORK AND INFORMATION SYSTEMS ACROSS THE UNION (NIS I DIRECTIVE)

3.13.1 Executive summary

The document provides a legislative analysis of directive (EU) 2016/1148 of the European Parliament and of the Council, an in-depth analysis of the impact of the legislation and, finally, an analysis of the problematic aspects that led to the need for its modification.
Indeed, the directive has been repealed by the new Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/ 2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), which entered into force on 17 January 2023, whose implementation must take place by 17 October 2024. The provisions of the NIS Directive 1 will therefore be relevant until the transposition of the new directive.

The NIS 1 directive, adopted on 6 July 2016 and entered into force on 8 August 2016, introduced on the basis of the principle of minimum harmonization (Article 3), the first regulation aimed at ensuring a common level of security of networks and systems information, i.e. aimed at preventing and managing the risks associated with the availability, authenticity, integrity and confidentiality of data, the compromise of which is capable of undermining the functioning of society and the economy of the Member States.

The legislation affects specific sectors and subjects, as specified below.
Regarding sectors (and sub-sectors), the directive concerns the "essential services" identified in Annex II of the directive (energy, transport, banking sector, financial market infrastructures, healthcare sector, supply and distribution drinking water and digital infrastructure).
The purpose is to ensure and guarantee their continuity.
With regard to subjects, the directive applies to "operators of essential services", (OES) public or private subjects who, pursuant to art. 5, provide an essential service for the maintenance of fundamental social and/or economic activities, the supply of which depends on the network and information systems and which, therefore, would suffer detrimental effects in the event of attacks on cybersecurity.
The identification of such subjects had to take place by the Member States by 9 November 2018. In this regard, Article 5 (7), of the directive required the Member States to report the results of this identification by 9 November 2018, so that the Commission could, pursuant to art. 23 of the directive, submit to the European Parliament and the Council a report assessing the consistency of the approach adopted by the Member States in identifying the operators of essential services. Given the delays in communications, the evaluation was carried out after the deadline of 9 May 2019 set by the legislation, and more precisely on 28 October 2019. Secondly, the directive applies to digital service providers (DSP), i.e. entities (legal persons) who, for the purposes of the directive, provide three specific types of service (identified in Annex III): online marketplace, online search engine and service in the cloud (cloud computing).The directive considers the latter as these services represent the basic infrastructure for companies to operate online and across borders.Unlike the first subjective category, their identification did not fall within the obligations imposed on the Member States

As will be detailed, a common element to both categories is the subjection to safety and notification obligations to the competent authorities.
With regard to the obligations to which digital service providers are subject, indicated by Article 16, the legislation is not self-sufficient and must be coordinated with the provisions contained in the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by

digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

The Member States had to transpose the directive within 9 May 2018 also in the light of the indications contained in the Communication from the Commission to the European Parliament and the Council of 4 October 2017, making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.
In September 2019, all 28 Member States notified full transposition. In the Italian legal system, the transposition took place through Legislative Decree 18 May 2018, n. 65.

According to the provisions of art. 21 of the directive, the Member States had the task of imposing effective, proportional and dissuasive sanctions to be imposed in case of violation of the national implementing provisions.
This was one of the elements which led the European legislator to amend the directive.

3.13.2 Analysis of the Legislation

3.13.2.1 Background of the legislative act

Directive 2016/1148 on security of network and information systems (the NIS Directive) is the first horizontal legislation undertaken at EU level for the protection of network and information systems across the Union. Given the increasing importance of ICT-based services and products in our daily life, any disruption or incident that affect such services and their underlying infrastructures may constitute a serious threat to the functioning of the whole Internal Market. The cyberattack that started in Estonia in 2007 and affected almost all Member States was an example of the technological interdependencies among cross-border services as well as the proof that the level of security achieved in the member States was extremely uneven. Accordingly, the European Commission started the drafting of a legislative measure aimed at achieving a "high common level of security of network and information systems within the Union so as to improve the functioning of the internal market". The NIS directive is the result of such process.

The NIS Directive has three main pillars:
(1) enhance the strategic cooperation and information exchange at European level, through the creation of a Cooperation Group and a computer security incident response teams network (CSIRTs network);
(2) require the adoption of national cybersecurity strategy plan at national level, including the creation of national competent authorities and CSIRT for the essential services; and
(3) identify the prevention and resilience mechanisms for operators of essential services (OESs) and digital service providers (DSPs).
The (2) and (3) pillars are the most interesting and innovative ones and will be analysed in detail.

(2) Each Member State must adopt a national framework that includes the national strategy on the security of network and information systems and the designation of the authorities that shall be responsible for the monitoring the implementation of the NIS Directive.
According to Article 7 NIS, the national cybersecurity strategy has a set of predefined issues, namely, a risk assessment plan, a governance framework to achieve the objectives of the national strategy, the identification of measures relating to preparedness, response and recovery etc. A part from the issue listed above, however, the directive leave the Member States free to design their national strategy.
This approach may run against the objective of harmonization set by the directive, yet it proved initially effective, as the Member States were able to adapt the Directive's provisions to the needs and special characteristics of the undertakings operating within their territory. Moreover, the directive defines a set of safeguards in order to promote

convergent interpretation: the role of ENISA in advice and assistance to Members (art. 7(2)), the use of European or internationally accepted standards (art. 19)
Then, Articles 8, 9, 11 and 12 of the NIS Directive identify the authorities and other bodies that shall be tasked with the role of monitoring its application at national and EU level. Each Member State shall also designate a national Single Point of Contact to liaise and ensure cross-border cooperation with other Member States. Although the Directive does not require a specific structure or hierarchy for the national authority, the latter should receive adequate technical, financial and human resources to carry out, in an effective and efficient manner, the tasks assigned to them.
One relevant innovation is the creation of a computer security incident response teams CSIRTs at national level (at least one) which has the task of monitoring incidents at national level, provide early warning, alerts and information to relevant stakeholders about risks and incidents, respond to incidents, provide dynamic risk and incident analysis and increase situational awareness, as well as, to participate in a network of the CSIRTs across Europe.

(3) NIS Directive affects two categories of undertakings, under an admittedly differentiated approach in terms of obligations placed upon each one of them: operators of essential services and digital service providers.
Operators of essential services (OES) are defined by Article 4 NIS, and they are defined as public or private entity that activates in specific sectors (listed in Annex 2: Energy, Transport, Banking, Financial market infrastructure, Health sector, Supply and distribution of drinking water, Digital infrastructure) which at the same time meets the essential criteria defined in art. 5 NIS directive. The criteria include the following:
(a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
(b) the provision of that service depends on network and information systems; and
(c) an incident would have significant disruptive effects on the provision of that service (for a definition of a significant disruptive effect, art. 6 NIS provides for specific criteria).

Consequently, not all operators of essential services fall within the scope of the NIS Directive. It is up to the Member States to identify the list of OES at national level and inform the Commission about the selection. This list is then updated at least every two years in order to take into account potential changes in the market. A consistent approach toward the identification of OES is crucial as it will avoid risks related to cross-border dependencies, ensure a level playing field for operators in the internal market, and also reduce the risk of divergent interpretation (inconsistencies may affect those operators active in more than one Member State). It should be noted that, the directive is based on minimum harmonization, thus Member States can adopt legislation ensuring a higher level of security, for instance extending the security and notification obligations also to operators in other sectors (e.g. public administrations, the postal sector, the food sector, the chemical and nuclear industry, the environmental sector and civil protection).

Article 14 NIS identifies two linked obligations for OES: security requirements and incident notification. First, OSEs must adopt adequate and proportionate technical and organisational measures to manage risks and to prevent and minimise the impact of network and information system security incidents to ensure service continuity.
The security requirements engage the participation of individual OES and Member States to ensure that OES have implemented appropriate and proportionate security measures. Accordingly, the OES should evaluate the effectiveness of existing technical and organisational controls in order to assess the level of their preparedness. However, the Directive does not indicate the type of methodology to carry out the relevant risk assessments nor the form of technology to be used. This is justifiable as the identification of specific approach would risk being outdated, given the swift developments occurring in the sector, but also due to the fact that the risk assessment should be adapted to different sectors. Given the intertwining between security requirements and notification of incidents, the directive seems to imply that the risk management approach should include a two-step 'monitoring process': one after the selection of specific control mechanisms that are assessed as appropriate for risk management; and one after the implementation of the finally selected control mechanisms to incidents.

Given the wide leeway given to the Members States and consequently to OES as regards the security requirements, some guidance in order to avoid fragmentation and inconsistency was needed. In this sense, the intervention of the NIS Cooperation group was crucial, as it provided several guidance documents. For instance, the Reference document on security measures for Operators of Essential Services (available at https://digital-

strategy.ec.europa.eu/en/policies/nis-cooperation-group) lays down some general principles that should be taken into consideration by all Member States during adopting security measures. These measures should be effective, tailored, compatible, proportionate, concrete, verifiable and inclusive.

The OES has also a mandatory obligation to notify incidents. Article 14 provides that OES are obliged to notify, without undue delay, incidents that have a significant impact, respectively on service continuity and service provision to the national Computer Security Incident Response Team (CSIRT). OES are obliged to report incidents that fall within the scope of the NIS Directive, namely *significant* incident, which has a serious impact on the service provided. In order to identify which are the significant incidents, the directive provides for a set of criteria:

a. the number of users affected by the interruption of an essential service
b. the time interval during which the essential service was not operational
c. the geographical spread of the area affected by the incident.

It should be noted that the provision, as of timeframe for the notification, refers to the ambiguous terminology of "without undue delay". This ambiguity is only solved at national level, however differences exist among the member states (in some cases strict, such as UK – 72 hours – or Estonia – 24 hours, in some cases wide, replicating the terminology of the directive). These discrepancies may become an issue as the OES active in more Member States may be subject to different notification requirements and timeframes.[160]Once the notification of the significant incident has been made, the national competent authority or CSIRT will support the notifying entity with assistance in handling the incident. Sometimes there is a need to notify the incident to the public; in this situation the NCA or CSIRT, after consulting the notifying operator of essential services, may communicate the individual incident to the public to raise awareness of the prevention or management of an ongoing incident.
It must be underlined that incidents that are not qualified as significant are not subject to the obligation to notify. The same is valid for legal entities that are not identified as OSEs. However, in both cases, the companies may submit voluntary notifications to the CSIRT of incidents that have a material impact on the continuity of the services they provide. In fact, the intention of the NIS Directive and its transposition decree is to encourage the widest dissemination of a conscious culture in the field of cybersecurity and a consequent increase in the relative levels of security, also through a greater exchange of information.

The second category of entities that fall under the scope of the NIS Directive are digital service providers. Being digital service at the basis of the activity of many business, the disruption of the provision of such services may have an impact on key economic and societal activities in the Union.
Pursuant art. 4 (5) NIS 'digital service' means a service within the meaning of Article 1(1)(b) of Directive (EU) 2015/1535, namely a service provided under the following conditions:
a. at a distance and by electronic means
b. at the request of the person concerned to receive the service
c. for remuneration.

Among these types of services, the directive lists three specific types that falls within the scope of application: *online market place providers, online search engine providers and cloud computing service providers*. Differently from OES, the Directive does not require Member States to identify which DSPs should fall within its scope.
Art. 16 NIS mirrors the security requirements and notification obligations applicable to OES also to DSP. However, differences emerge, showing a lighter approach towards DSP.
Member States will have to ensure that DSPs 'identify and take appropriate and proportionate technical and organisational measures to manage the risks to the security of the networks and information systems they use in the context of service provision'. Some criteria are listed in the same provision, including the security of the systems and facilities, incident handling, business continuity management, monitoring, auditing and testing and compliance

160 Note that in case of significant incidents that also involve a data breach, according to art. 33 GDPR, would require an additional notification to the Data protection authority at national level, within 72 hours from the moment that the data processor acquires knowledge of the breach.

with international standards. The Commission, by virtue of article 16(8) of the NIS Directive, issued an Implementing Regulation that specified further these elements.

The notification obligation is instead framed in a slightly different manner than the one for OES. The notification procedure should be followed only in case of incidents with a substantial impact on the provision of the DSP service. Article 16 (4) mentions the parameters to be taken into account in order to determine whether the impact of an incident is substantial, namely: (a) the number of users affected by the incident, in particular users relying on the service for the provision of their own services; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent of the disruption of the functioning of the service; (e) the extent of the impact on economic and societal activities. These parameters are further specified in the Implementing Regulation.[161]

This softer approach towards DSP is also evident in their obligation to notify an incident only in those cases where they have access to the information needed to assess the impact of such incident. Furthermore, in the case of DSP, contrary to OES, the competent authorities take action, if necessary, through ex post supervisory measures when provided with evidence by the DSP itself or a user or another competent authority.

The softer approach towards DSP is mainly based on the different nature of the infrastructures they use as well as of the services they provide. The DSP have more freedom to conduct business, which is considered a key factor to their successful operation.[162]

However, there are cases where this approach may result counterproductive, for instance when OES rely on DSP to provide their services, for instance a hospital (OES in the health sector) hosting its patient records in the cloud (DSP that provides cloud computing services). In this case, the notification is allocated on the OES only, on the basis of the information provided by the DSP, pursuant art. 16 (5) NIS.

3.13.2.2 Impact of legislation

According to the Commission evaluation and impact assessment of the NIS directive (ex art. 23 NIS), although the NIS Directive has served as a catalyst in many Member States, paving the way for a real change in the institutional and regulatory cybersecurity landscape, several issues and problems emerging from the analysis of the implementation of the Directive are identified.

In particular, the Commission highlighted that **the scope of the directive has become too limited** in terms of the sectors covered, mainly due to increased digitalisation in recent years and a higher degree of interconnectedness; and to the changes in the types of key services in digitalized sectors serving the economy and society as a whole.

The requirement to identify the OES at national level has triggered a comprehensive assessment of the risks associated with operators active in critical activities and modern network and information systems in almost all Member States. However, the **lack of clear guidelines in the selection of OES** led to the inconsistencies among Member States, hampering the smooth functioning of the internal market, and most importantly the effective management of IT dependencies. As matter of fact, Member States have developed a variety of methodologies and

161 Article 4 Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

(a) the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;

(b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;

(c) the incident has created a risk to public safety, public security or of loss of life;

(d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

162 See also ENISA, incident notifications for DSPs, 2017

different level of granularity for the sectors covered, reducing the possibility to compare the lists of OES across the EU. The extension to additional sectors of subsectors in order to identify other OES at national level showed that there are other sectors potentially vulnerable to cyber incidents than those covered by the NIS Directive.

The **wide discretion** left to Member states **as regard security and incident reporting requirements** for OES has also been an issue, having Member States implemented these requirements in significantly different ways, creating an additional burden for companies operating in more than one Member State.
Additionally, the supervision and enforcement regime of the NIS Directive was deemed as ineffective, as, for example, Member States have shown great reluctance to apply sanctions.
The financial and human resources set aside by Member States for fulfilling their tasks, and consequently the different levels of proficiency in dealing with cybersecurity risks, vary greatly.
The Commission draws the preliminary conclusion that, while the NIS Directive has set in motion a crucial process to increase and improve operators' risk management practices in critical sectors, there is a considerable degree of fragmentation in the Union when it comes to identifying OES. This is partly due to the structure of the Directive and partly due to the different implementation methodologies used by Member States.

3.13.3 Alternative Solutions/Policies

3.13.3.1 Listing of the Alternatives Considered

During the review of the legislation by the Commission, following the studies conducted on its behalf[163], a series of policy options were considered, with the purpose of solving the problems that emerged after the transposition of the directive by the Member States.
The measures adopted following the directive have proved to be insufficient for several factors.

More specifically, these factors include the ambiguity of the legislation and the low level of harmonization achieved, which has led to differences, for example, regarding the identification of the subjects and sectors to which the directive applies, the requirements companies must comply with, the notification procedure to be followed; the scarcity of investments in cybersecurity (also due to the absence of incentives); the lack of an aware culture on the matter; the absence of an adequate supervisory and sanctioning system for cases of non-compliance with the law; the lack of effective cooperation at the European level, which is characterized by its voluntary nature. It emerged that within the European Union Member States developed different capabilities to react to threats against cybersecurity and, consequently, an unsatisfactory level of overall resilience, also due to the increase in the interconnection and interdependence between the different sectors on which the functioning of society and the economy is based.

On the basis of these considerations and this baseline scenario, ignoring the option of leaving the *status quo* unchanged, three strategic options were evaluated, based on increasing intervention and harmonization strategies. The first option consists in the adoption of non-legislative measures, such as guidelines and recommendations on a voluntary basis aimed at clarifying different aspects, such as the identification of operators of essential services and digital service providers, safety requirements and incidents reporting, supervision and enforcement. Based on this policy option, the purpose, requirements, and obligations imposed would remain unchanged. Among the measures to be adopted, it was also considered the need to incentivize the financing of the competent authorities, such as for example the CSIRTs and, finally, that of increasing cooperation between the Member States and the exchange of information through the cooperation group and the CSIRT network.

163 Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)- No. 2020-665, Final Study Report.

Alternatively, the second option would introduce targeted legislative changes, with the aim of achieving a broader level of harmonization. The purpose is to clarify the controversial aspects of the legislation (for example in relation to the identification of digital service providers and the incident reporting requirements, as well as the jurisdiction rules) and to ensure greater effectiveness, for example thanks to the extension of the scope of the directive to new sectors, sub-sectors and services of interest. The new elements would include some harmonization measures relating to specific aspects, such as the identification of essential services, the identification thresholds, security and incident reporting requirements, the introduction of general conditions for the application of administrative sanctions and their minimum level. Another new aspect would be the introduction of equal treatment between operators of essential services and digital service providers (with regard to the latter, the light-touch approach would be removed and full supervision would be introduced). Further, for this policy option it was assessed the need to ensure that Member States take measures to ensure the availability of all the resources necessary for the competent authorities to carry out their supervisory and guiding roles, as well as the need for closer collaboration, in this case also through a public-private partnership.

The third policy option proposed consists of a substantial modification of the existing legislation through the adoption of a new directive, involving structural changes to the previousdirective.
In this option, some aspects belonging to the previous strategic option would be maintained (first, the need to broaden the scope of application of the directive).
Among the new elements appear important modifications relating to the subjective categories.
In fact, with a view to simplification, this strategic option considers subjects according to their importance and criticality and based on a series of requirements, elements to which different obligations and supervision regimes follow.

Given the problems associated with identification, the new directive should introduce uniform criteria for the identification of all subjects interested, excluding from the subjective scope of application smaller companies (small and medium-sized enterprises) not having a key role in the provision of essential services.
This strategic option evaluated the opportunity to establish a register, kept by ENISA, to which digital service providers should communicate the data necessary for their identification, with an evidently simplification intent.
This strategic option also considers establishing an equal footing between the categories of OPS and DPS, subjecting the latter, if considered critical, to the same rules.
A similar regime would instead cover non-critical DSPs and operators of services deemed important but non-essential, which would be subject to a light regulatory regime, including only ex post supervision and lighter requirements on sanctions.
According to this option, the harmonization should introduce uniform and explicit requirements on safety, incident reporting, supervisory and sanctioning measures, differentiated and customized for each category of subjects according to the level of importance of the services provided.
Other key elements taken into consideration are the communication and exchange of information relating to incidents and vulnerabilities related to cybersecurity measures, at national and supranational level, with the purpose to facilitate wider cooperation between Member States.
Finally, the adoption of a specific system for monitoring the state of cybersecurity in the European Union was evaluated.

3.13.3.2 Comparison of Alternatives and preferable choice

In this paragraph, only the assessments carried out by the Study to support the review of the NIS Directive mentioned in the previous paragraph will be examined in depth, postponing the in-depth analysis of the Commission's assessments as envisaged in the impact assessment report relating to the NIS Directive 2.

When assessing the various strategic options, it was decided to carry out a comparative assessment of the various alternatives according to their qualitative and quantitative impact based on a series of criteria, including effectiveness and related social effects, efficiency and related economic impacts, coherence with other EU legislations, impact on fundamental rights, EU added value.

Limiting the study to the first two, due to their particular interest, in relation to the first element of evaluation, effectiveness and social impacts, the evaluation was carried out in relation to six specific pre-established objectives[164]. The comparison revealed differences related to the degree of incisiveness of the legislation. In fact, it has been noted that strategic option 1, through the provision of non-binding rules, would not have led to significant changes, primarily due to the absence of changes relating to the scope of the directive. Regarding strategic option 2, a particular criticality was assessed, absent in the third, due to the equal treatment between companies.
This element would entail compliance costs for small and medium-sized enterprises as well as administrative costs, without this could have positive implications in terms of legislation effectiveness.
The third option was considered the most advantageous and therefore preferable, due to the higher level of harmonization, precision, and binding nature of the legislation in relation to some aspects, such as for example supervision and enforcement, also thanks to the peer review mechanism having the function of evaluation the capabilities of the Member States.

A further element positively evaluated in relation to the third strategic option is represented by the information system based on the sharing system.
The economic impacts (administrative costs to monitor and audit and costs borne by companies due to the need to comply with the legislation) vary according to a series of elements, among which appears the extension of the scope of the directive, the degree of it, the population affected by the services offered. Also, in the light of these assessments, the third strategic option was considered preferable, as it represents the compromise solution aimed at avoiding the impact of much higher costs, such as those caused by cyber-incidents, destined to increase in the absence of the adoption of adequate regulatory measures.

3.14 DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 14 DECEMBER 2022 ON MEASURES FOR A HIGH COMMON LEVEL OF CYBERSECURITY ACROSS THE UNION, AMENDING REGULATION (EU) NO 910/2014 AND DIRECTIVE (EU) 2018/1972, AND REPEALING DIRECTIVE (EU) 2016/1148 (NIS 2 DIRECTIVE)

3.14.1 Analysis of the Legislation

3.14.1.1 Background of the legislative act

In December 2020, the Commission presented the new legislative instrument that should substitute the Networks and Information Systems directive (NIS 1), namely the proposal for a directive on measures for a high common level of cybersecurity across the Union (NIS 2), which would repeal the NIS 1 and overcome some of the flaws of the latter.
The approach of the European legislator has not changed, and both NIS 1 and NIS 2 share the same legal basis: article 114 TFEU, addressing the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. Accordingly NIS 2 is still aimed at enhancing the level of security in order to safeguard the digital internal market, establishing harmonized rules in the area of cybersecurity risk management

164 Study to support the review of Directive (EU) 2016/1148, pp. 119-121.

and incident reporting.[165] This approach is also supported by the extension of number of areas that fall into the scope of NIS 2, which as a result would increase the number of entities that would be bound by the NIS 2 obligations and requirements.

NIS 2 has three general objectives:

1. Enhance cyber-resilience level of European business through a uniform and harmonized set of cybersecurity requirements (applicable to all public and private entities that fulfil important functions for the economy and society).
2. Increase the coherence of the cyber-resilience obligations through the alignment of (i) the de facto scope; (ii) the security and incident reporting requirements; (iii) the provisions governing national supervision and enforcement; and (iv) the capabilities of the Member States' relevant competent authorities.
3. Improve the coordination and information sharing among business and authorities, enhancing the level of trust in the latter, and setting clear and efficient rules and procedures in the event of a large-scale incident or crisis.

It is important to highlight that the current structure of the NIS 2 is based on the evaluation and reporting addressing the impact of NIS 1 directive. As a matter of fact, one of the first challenges emerging from the NIS 1 structure was the identification of the actors subject to the legislation.[166] The NIS 2 identifies as a first criterion the size of the company, excluding from its scope small and micro sized enterprises[167] (art. 2 (1) NIS 2). Accordingly, no additional criteria will have to be indicated by the member states to identify the, at the time, OES.
While the Commission admits that this criterion is "not necessarily an ideal stand-alone criterion to determine the importance and/or criticality" of an entity, it to be a "meaningful proxy" in order to determine whether certain entities have key roles for society and economies.
However, the text provides for a wide list of exceptions, which apply regardless the size of the company. For instance, the size is irrelevant in case of services provided by providers of public electronic communications networks or of publicly available electronic communications services, or trust service providers, or also top-level domain name registries and domain name system service providers; in case of entities that is the sole provider in a Member State of a service which is essential for the maintenance of critical societal or economic activities; in case the disruption of the service provided by the entity could have a significant impact on public safety, public security or public health; or for public administration entity. Additionally, the NIS 2 applies to entities providing domain name registration services.
The second criterion is the activity carried out in one of the sectors identified in Annex I and II of the NIS 2 Directive. It is interesting to note that the NIS 2 extends significantly the scope of NIS 1 by adding new sectors such as telecoms, social media platforms and the public administration.

165 Note that in the NIS 2 proposal the Commission does not focus on the risks of cybersecurity, but rather of the impact that differences emerging at legislative level may have on the internal market "because entities that engage in cross-border activities face different, and possibly overlapping, regulatory requirements and/or their application, to the detriment of the exercise of their freedoms of establishment and of provision of services" (see Explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final – hereinafter Explanatory Memorandum of NIS 2).

166 See the Explanatory Memorandum of NIS 2 which affirms that the NIS 1 approach was too "complex".

167 This would exclude all entities that employs fewer than 50 employees and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.

Table 1 Comparison of sectors under NIS1 (not in bold) and NIS2 (in bold); sub-sectors in parenthesis. The order of the listed (sub-)sectors corresponds to the one in the NIS2 Annexes

Essential entities	Important entities
– Energy (electricity—now including **production**; **aggregation**; **demand response** and **energy storage**; **electricity markets**—; **district heating**; oil; gas and **hydrogen**) – Transport (air; rail; water; road) – Banking – Financial market infrastructures – Health (healthcare; **EU reference labs**; **research and manufacturing of pharmaceuticals and medical devices**) – Drinking water – **Waste water** – Digital infrastructure (IXP; DNS; TLD; cloud; **data centre service providers**; **CDN**; **trust service providers**; **electronic communications**) – **Public administrations** – **Space**	– **Postal and courier services** – **Waste management** – **Chemicals** (**manufacture**; **production**; **distribution**) – **Food** (**production**; **processing**; **distribution**) – **Manufacturing** (**medical devices**; **computer, electronic and optical products**; **electrical equipment**; **machinery**; **motor vehicles and (semi-)trailers**; **transport equipment**) – Digital providers (online marketplaces; search engines; **social networks**)

Source: Thomas Sievers, Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations, Int. Cybersecur. Law Rev. (2021) 2:223–231

The Annex I and II provides for another of the innovations of NIS 2: the shift from the distinction between Operators of essential services (OES) and Digital service provides (DSP) to the distinction between so called essential entities (EE) and important entities (IE). As it will be clarified below, the distinction is no more justified upon a different set of requirements and notification obligations, rather it only affects the type of market surveillance mechanisms applicable to EE and IE, being the security requirements and the notification mechanisms completely overlapping. Article 21 and 23 NIS 2 clarify that both EE and IE are subject to the same cybersecurity requirements and reporting obligations. NIS 2 is also more detailed in terms of guidelines regarding the security requirements, although it repeats the wording already used in Article 14 NIS 1 on "appropriate and proportionate" measures as well as the standard of "state of the art", it adds a list of seven key elements that all companies must address or implement, including incident response, supply chain security, encryption and vulnerability disclosure. [168]

168 Article 21 (2) provides that security measures shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

As regards the reporting obligations, NIS 2 envisages a two-stage approach to incident reporting which overcomes the problems emerged in the implementation of NIS 1.[169] During the first stage, the affected entity should inform, with an initial report, the national authority or CSIRT within 24 hours from when they first become aware of an incident. Then, the entity will provide a full report within 72 hours from when they first become aware of an incident. The second stage address the complete restoration of the problem, with the submission of a final report one month later from the initial report.
Note that reporting for significant incidents is mandatory, any other lower level of incidents does not require notification. However, in order to acquire a full picture of the threat landscape, Article 29 NIS 2 Proposal provides a legal basis for voluntary notifications of significant incidents, cyber threats and near misses by entities falling outside the scope of the NIS2 Directive, leaving the choice to member states how to prioritise the processing of mandatory notifications over voluntary notifications.[170]

The differentiation between EE and IE provided by NIS 2 is in the type of supervision applied to each of them. Article 32 NIS 2 provides for the supervisory and monitoring powers applicable to EE and it differentiates between ex ante supervision, i.e. the taking of supervisory measures in advance and ex post supervision, i.e. taking supervisory action when provided with evidence or an indication that an entity does not meet the cybersecurity and incident notification requirements. EE are subject to a "fully-fledged" supervisory regime that includes both ex ante and ex post supervision. Whereas, art. 33 NIS 2 provides that IE are subject to a "light" supervisory regime, which includes only ex post supervision.
Necessarily, supervision of essential entities includes for example "regular audits" in Article 32(2)(b) NIS 2, while Article 33 (b) NIS2 with regard to important entities includes "targeted security audits based on risk assessments or risk-related available information" only.
Regarding enforcement, it establishes a minimum list of administrative sanctions whenever entities breach the rules regarding cybersecurity risk management or their reporting obligations laid down in the NIS 2 Directive. These sanctions include binding instructions, an order to implement the recommendations of a security audit, an order to bring security measures into line with NIS requirements, and administrative fines (up to €10 million or 2 % of the entities' total turnover worldwide, whichever is higher).

3.14.1.1.1.1 Impact of legislation

The Directive entered into force on 14 December 2022, however, it will be applicable from 18 October 2024, in order to guarantee to the member states the possibility to adapt their national legislation to the new legal framework.
Although the changes in the NIS 2 directive are relevant, its impact at national level depends on the level of maturity that the cybersecurity framework has achieved. According to the Commission, the NIS 1 directive was crucial in order to improve the national cybersecurity capabilities requiring Member States to adopt national cybersecurity strategies and to appoint cybersecurity authorities. However, the increased digitisation of the internal market and the evolving cybersecurity threat landscape required an additional effort that was not met by all national legislators. Accordingly, the NIS 2 may qualify as a "blessing in disguise" in that Member States may

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

169 Article 14 NIS 1 referred generically to 'without undue delay' which was interpreted differently by EU member states in their implementation, leading to different response to critical incidents.

170 See article 29 (1) which provides that

"Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks".

rework their national cybersecurity legislation that may be fragmented.[171] In this case, it will be up to the national legislators to exploit this opportunity and harmonise their national cybersecurity legislation within a single, organic, comprehensive and coherent legislative text reaching the objectives provided for by the NIS2 Directive.

3.14.2 Alternative Solutions/Policies

According to the Impact assessment presented by the Commission, the policy options evaluated for improving the legal framework in the area of cyber resilience and incident response were the following :

1. "Do nothing": The NIS Directive would remain unchanged and no other measures of non-legislative nature would be taken to target the problems identified by the evaluation of the NIS Directive.
2. Option 1: There would be no changes at legislative level. Instead, the Commission would issue recommendations and guidelines (such as on the identification of operators of essential services, security requirements, incident notification procedures and supervision), upon consultation of the Cooperation Group, the EU Agency for Cybersecurity (ENISA) and, as applicable, the network of Computer security incident response teams (CSIRTs).
3. Option 2: This option entails targeted amendments to the NIS Directive, including an extension of the scope and several other amendments that would aim at guaranteeing certain immediate solutions to the problems identified, providing more clarity and further harmonisation (such as provisions to harmonise identification thresholds). The amended NIS Directive would however maintain the main building blocks, approach and rationale.
4. Option 3: This scenario entails systemic and structural changes to the NIS Directive (through a new directive) envisaging a more fundamental shift of approach towards covering a wider segment of the economies across the Union, yet with a more focused supervision targeting big and key players. It would also streamline the obligations imposed on businesses and ensure a higher level of harmonisation thereof, create a more effective setting for operational aspects, as well as establish a clear basis for enhanced shared responsibilities and accountability of various stakeholders on cybersecurity measures.

As it is clear from the previous presentation to option that was preferred was Option 3, including systemic and structural changes to the NIS framework. The choice was based on the need to reformulate and overcome the flaws emerging from the NIS 1 implementation, made even more evident from the impact of the COVID-19 pandemics.
The revision enhance the level of effectiveness improving the clarity of the scope of application, the coherence in the security requirements as well as the identification of the supervision and enforcement framework. However, the cost for businesses and Member States would increase in order to ensure compliance with the new legislative framework. However, the Commission underlines that it would also lead to efficient trade-offs and synergies, in order to ensure an increased and consistent level of cyber resilience of key entities across the Union that would eventually lead to cost savings for both businesses and society.[172]

171 Sandra Schmitz-Berndt · Pier Giorgio Chiara, One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive, Int. Cybersecur. Law Rev. (2022) 3, 310.

172 See the Explanatory Memorandum to NIS 2 Proposal, where the Commission affirms that "For essential and important entities, increasing the level of cybersecurity preparedness could result in mitigating potential loss of revenue due to disruptions – including from industrial espionage – and could reduce the large expenses for an ad-hoc threat mitigation. Such gains are likely to outweigh the necessary investment costs. Reducing fragmentation in the internal market would also improve the level playing field among operators.

For Member States, it could further reduce the risk of growing budgetary expenses for ad-hoc threat mitigation and additional costs in case of emergencies related to cybersecurity incidents.

For citizens, addressing cybersecurity incidents it is expected to result in reduced loss of income due to economic disruption."

3.15 Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (Machinery directive)

3.16 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on machinery products COM/2021/202 final (machinery regulation proposal)

3.17 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (PLD)

3.18 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products COM/2022/495 final (product liability directive update)

3.19 National discipline of the Ethical Committees and its most recent updates in the wake of the implementation of the Clinical Trials Regulation EU/2014/536, L 3/2018 and Law Decrees of 26, 27 and 30 January 2023

3.20 Italian tort rules applied to biorobotics devices and allied technology

3.21 Italian contractual rules applied to biorobotics devices and allied technology

3.22 Italian insurance rules applied to biorobotics devices and allied technology

In this subsection some EU and Italian documents will be analysed from the perspective of the Italian Insurance law. In particular, there will be a concise analysis of Regulation 445/2016 on the fair competition of personal protective equipment (PPE) supply (3.23.1) and the guidelines on the "Digital model for the actuation of the healthcare home assistance" Legislative Decree 29 April 2022 (3.23.2).

3.23.1. Regulation 445/2016 on the fair competition of personal protective equipment (PPE) supply Executive Summary

Regulation (UE) 2016/425 (hereinafter, "**EU Regulation**") pursues fair competition of personal protective equipment (hereinafter, "**PPE**") supply and protection of their users in the Union market. To this end, EU Regulation harmonizes *essential* health and safety requirements for PPEs, deferring their *technical* details to implementing

provisions (so called, “the new approach principle”). EU Regulation also bears economic operators with PPE compliance and ensures a traceability system to make its surveillance simple and efficient.

EU Regulation rules on PPE’s essential health and safety requirements (see Chapters 1 and 3). They are compulsory, although applied consistently with the corresponding product risk (*i.e.* general requirements; additional common requirements; additional specific requirements), according to the current state of art and practice (see Annex II). Following a conformity assessment procedure, the manufacturer states – and assumes responsibility for - their fulfillment by issuance of a declaration of conformity (see Annex IX).

The EU Regulation also sets out specific obligations for economic operators dealing with PPEs depending on their role in the distribution chain (*i.e.* manufacturer, authorised representative, importer and distributor). These duties mainly encompass product compliance (e.g. compliant design and manufacture; compliant placing; conformity measures, either corrective or recalling if not withdrawal; safe storage and transport; CE marking) and information transparency (e.g. draft and conservation of technical documentation; disclosure of information and documents requested by the competent national authority to prove PPE conformity; declaration of conformity; immediate notice of risks to competent national authority) (see Chapter 2).

Finally, the EU Regulation provides a conformity assessment procedure (see Chapter 4 and 5 and Annexes IV, V, VI, VII, VIII) based on risk categories (*i.e.* minimal risks, other risks and serious risks; see lists under Annex I) and carried out by a notified body. An exceptional arrangement is made for PPEs produced as a single unit to fit an individual user whereby classified as seriously risky (see Article 19 of EU Regulation). The EU Regulation imposes insurance liability on conformity assessment bodies, unless the Member State is vicariously liable, if not directly tasked with the conformity procedure (see Article 24, paragraph 9, of EU Regulation).

3.23.1.2. Analysis of the Legislation

3.23.1.2.1. Background of the legislative act

EU Regulation repeals Council Directive 89/686/EEC (hereinafter, “**Council Directive**”) with effect from 21 April 2018. Council Directive was meant to remove obstacles to trade in PPE in the internal market through a harmonized set of essential health and safety requirements. However, experience showed inadequacies in the provided product coverage and conformity assessment procedures. Inconsistencies also emerged in their implementation among Member States. Therefore, this made it necessary to revise, and enhance, the framework originally set by the Council Directive, as well as to replace this instrument to prevent divergent transposition. It is worth noting that EU Regulation also applies to the use by workers of PPE at the workplace (see recital no. 23 of EU Regulation with reference to Article 4 of Council Directive 89/656/EEC).

3.23.1.2.2. Analysis of specific issues

EU Regulation does not *directly* address insurance provisions – either facultative or compulsory - to economic operators dealing with PPEs. Despite postponing the issue for a deeper analysis of national legislation, it is worth noting that such a provision could neither be inferred *indirectly* from the insurance duty born by conformity assessment bodies (see above the said Article 24, paragraph 9, of EU Regulation), due to their third-party role. Indeed, they (together with their top-level management and personnel tasked) are necessarily other than economic operators; moreover, they shall be independent from both the organisation and the PPE assessed (see Article 24, paragraph 3 and 4, of EU Regulation).

3.23.1.2.3 Impact of legislation

Reference should also be made, among others, to Council Directive 89/656/EEC (on the minimum health and safety requirements for the use by workers of personal protective equipment at the workplace) and its implementation.

3.23.1.2.4. Alternative Solutions/Policies

3.23.1.2.4.1. Listing of the Alternatives Considered

In this first analysis, the absence of specific provisions about insurance or financial security addressed to economic operators appears consistent with the European pressure to free trade of goods, hence the overall approach of regulation on defective products (see Council Directive 85/374/CEE). Even so, it could be worth pondering whether the specificity of PPEs may rise an issue of proper capitalization, considering their intrinsic design (*i.e.* often worn or held by a person) and their function (*i.e*. protective), together with the core interests at stake (*i.e.* personal health and safety).

3.23.2. “Digital model for the actuation of the healthcare home assistance” (Approval of the organisational guidelines concerning thr “Digital model for the enactment of home- assistance ”) Legislative decree 29 April 2022

3.22.1.1 Executive Summary

These organisational guidelines containing the digital model for the implementation of home care, which take the form of guidelines, constitute the "EUM6C1 - 4" milestone of Mission 6, component 1 of the National Recovery and Resilience Plan (M6C1 - PNRR).
This document is therefore part of the interventions foreseen in the afore-mentioned plan, also in coherence with the reform of territorial assistance, also a milestone of the PNRR.
All the interventions of the M6C1 are aimed at strengthening territorial care, and in particular at finalising the principle of 'home as the first place of care'.
The purpose of these organisational guidelines is to define in the described context the organisational model for the implementation of the various telemedicine services in the home setting, through the rationalisation of the processes of taking charge and the definition of the related operational aspects, enabling the provision of services through multi-professional teams in accordance with the provisions of current legislation, also at a distance.
In particular, the fundamental components of the home care organisational model, to which the guidelines refer, are:
- the home care service, which guarantees continuity of care in the manner indicated by current national and regional legislation
- the planning of home care access, developed over the entire week in accordance with the aforementioned regulations, taking into account the clinical-assistance complexity of the patients;
- the home care service integrated with remote telemedicine services.
In order to authorise adherence to home treatment also with telemedicine services, the patient is therefore required to fill in the necessary forms, which include the informed consent that the patient expresses following the appropriate information received that will be prepared by the Ministry of Health in collaboration with the Guarantor

Authority for the Protection of Personal Data and with the Regions/PA, authorising all the professional figures involved to said treatment

The following points of the decree are of interest: Point 2.1.2 in which home care is defined.
The reference figures are introduced, shedding light on their function and role.
Moreover, there is also mention of Telemedicine services. In fact, they are fully part of the home care pathway, whether they are a one-off activity, or whether they are developed as cycles of services (e.g. telerehabilitation) or in a continuous mode (e.g. telemonitoring). The following are involved in the process of taking care of the patient at home: the General Practitioner (GP)/Pediatrician of free choice (PLS) who has the clinical responsibility for the patient in the general process of taking care of the patient; the nurse as a member of the multi-professional team, who acts as a reference point for the family and for the other actors (PLS/MG, specialists, MCA, other professionals) in taking care of the patient. He/she is a liaison and facilitator of the organisation and involvement of the person, the family and the caregivers in the definition and implementation of the PAI. He/she may act as case manager in relation to the home care plan, facilitating the care pathway and thus ensuring its continuity.
In the same way, a role is also attributed to the Territorial Operations Centre (COT), which performs the function of coordinating the taking charge of the person and linking the services and professionals involved in the various care settings, and to the ADI Operations Centre, which receives all requests for the activation of integrated home care interventions and continuity of care, where present.
They are responsible for the organisation and tracking of the taking into care and any transitions between settings that may be necessary, providing the connection between the various subjects and care levels.

Another point of interest: the technological platform at point 2.1.3. By technology platform it is meant the IT infrastructure for the provision of telemedicine services, integrated with the digital health ecosystem (e.g. ESF) and interfacing with the National Platform for telemedicine governance and deployment to provide useful data for monitoring telemedicine use throughout the national territory, as well as verifying the use of solutions included in the national telemedicine catalogue. A local technical organisation is desirable for telemedicine services, e.g. a Service Centre or a Telemedicine Delivery Centre, or both, where they exist.
The Service Centre does not intervene at the level of clinical responsibility, it is accountable to the Provider Centre for the effective performance of all its tasks, in particular for the integrity and security aspects of the health and social health information transmitted during telemedicine activities. Like any computer system that handles sensitive data, it must comply with the legal requirements on the processing of personal data. The Service Centre where necessary, may also perform help desk functions for professionals and patients. The organisation of these functions is, however, left to each local organisation of these functions is, however, left to each individual local authority within the framework of the resources available under current legislation.
Finally, point 2.1.4. sheds light on the matrix of actors and responsibilities.
Furthermore, with reference to the use of telemedicine services, the following responsibilities are laid down:
- the responsibility for the provision of the service lies with the healthcare professional providing the service; the assessment of the level of achievement of the set objectives may be the responsibility of the home care team in charge of the patient or of the individual professional, depending on the case.
- To all the activities that are provided with services and in a telemedicine regime, the deontological rules of the health professions apply, taking into account the guidelines dictated by bioethics.
- Any technical aspects, e.g. equipment malfunctioning, that may affect the provision of the service are the responsibility of the Telemedicine Service Centre, as far as it is concerned.
competence, the Telemedicine Service Centre.
- Each actor participating in the telemedicine service provision must in any case be identifiable through appropriate digital systems and the relative hourly effort spent for each patient must be recorded through computerised systems, for the purpose of automated reporting of the activities performed.

The decree does not deal with the insurance profile, which, however, should undoubtedly be studied with regard to both the healthcare facility and the healthcare professionals involved in the implementation of the care project, as well as the telemedicine services in use.
In particular, the focus is on the figure of the nurse as a member of the multi-professional team, who acts as a reference point for the family and other players.

He is a liaison figure and organisational facilitator whose powers and obligations are not yet defined.

3.23.2.2. Analysis of the Legislation

3.23.2.2.1. Background of the legislative act

The main references that were looked to in constructing the decree and the guidelines were:

- State-Regions Agreement of 20 February 2014 (Rep. Atti n. 16/CSR) on the document, on "Telemedicine, national guidelines";
- State-Regions Agreement of 17 December 2020 (Rep. Atti n. 215/CSR), on the document bearing "National guidelines for the provision of services in telemedicine";
- State-Regions Agreement of 18 November 2021 (Rep. Atti n. 231/CSR), on the document bearing "National indications for the provision of telemedicine services and performances by the health professions';
- State-Regions Agreement of 4 August 2021 (Rep. Atti n. 151/CSR), on the document entitled "Proposal of minimum structural, technological and organisational requirements for authorisation to practise and additional requirements for the accreditation of home care, in implementation of Art. 1, paragraph 406, of Law no. 178 of 30 December 2020';
- Decree-Law No. 179 of 18 October 2012 on 'Further urgent measures for the growth of the Country', converted, with amendments, by Law 17 December 2012, . as amended
- Decree of the President of the Council of Ministers No 178 of 29 September 2015, on. "Regulations on electronic health records";.
- Decree of the President of the Council of Ministers 12 January 2017, on 'Definition and updating of the essential levels of care, referred to in Article 1, paragraph 7, of Decree Legislative Decree No 502 of 30 December 1992';
- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC; Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU of the Commission;
- Italy's National Recovery and Resilience Plan approved by Council Decision ECOFIN of 13 July 2021 and notified by note LT161/21, dated 14 July 2021 by the Secretariat General Secretariat of the Council

One can wonder whether the legislation is sufficient to deal with these issues and the reply is that it is Mission 6 of the National Recovery and Resilience Plan (NRP), dedicated to Health, mentioned in the decree stems from the need to bridge the gap between territorial disparities and to offer greater integration between health services in the various care areas. The guidelines aim, therefore, precisely at this and that is to increase the home care service, starting from the assumption that the home should be the first place of care.
The objective is to try to make telemedicine as widespread as possible only analyses and structures the strictly technical profile of the subject matter and only partly touches on the liability profile.

3.23.2.2.2 Impact of legislation

In the face of such an important technological advance, the jurist is called upon to assess first and foremost whether the legislation is adequate to define both the roles and tasks of those involved in telemedicine and telemonitoring and also the responsibilities and insurance profiles that arise. Both telemedicine but even more so telemonitoring can in fact make use of self-learning systems capable of performing operations autonomously and of communicating with other systems, extracting information and adapting to environmental conditions. Surely, therefore, the problem lies in identifying who is in control of these medical devices and thus who is primarily responsible if damage occurs.
The level of control that professionals maintain over intelligent medical devices will be decisive.
The scenario, as has already been hypothesised by scholars, will include cases where the level of transparency of smart device decision-making processes or the level of information provided by manufacturers may prove to be poor and practitioners will not be in a position to exercise effective control. In such situations, liability for damages related to the use of the device in a healthcare context will tend to fall on the manufacturers, or possibly on the healthcare facility, which may be called to answer for damages related to organisational shortcomings in the selection of the devices, with particular reference to the effectiveness of monitoring systems aimed at ascertaining their quality and safety, as well as for possible shortcomings in the training of physicians called upon to use smart devices appropriately.
All this will inevitably lead to the need to review the various insurance profiles, especially the content of single policies.

3.23.2.2.3 Alternative Solutions/Policies

a. Listing of the Alternatives Considered

Since the decree does not address the insurance profile, it might be useful to introduce this aspect by providing for a compulsory insurance system linked to the 'home as a place of care' project. It might therefore be useful to analyse the policies now in use in the healthcare system to verify their adaptability also in relation to this new scenario or, on the contrary, to proceed to envisage an entirely new policy content on the basis of the telemedicine system used and thus on the basis of the risks of the individual digital system in use, specifying which insurance obligations are for the healthcare system and which are envisaged for the individual citizen, and whether single policies can be envisaged to be able to cover this type of supplementary digital healthcare as well.
As far as to why some alternatives were chosen for further analysis while others were not, the decision to start with more technical guidelines was dictated by the need to first define the roles, tasks, and technologies to be used. However, it is necessary to implement this departure with the insurance profile by studying not only new solutions but also existing systems.

4 FIT4MEDROB SURVEY-TABLE RESULTS

The A4 group members decided to create a table with Word and to keep the questions/reply suggestions as much general as possible in order to have the highest possible reply rate and in order to let non-legal experts more free to actually report on their daily problems in the interpretation and the application of the relevant legal frameworks. The survey-table was firstly sent to the partners on 02 March 2023. There was a time to implement and suggest modifications to it until 13 March 2023. The partners could access the documents directly in a shared teams folder. If they experienced difficulties in accessing the Teams shared folder, it was possible from 10 March to also have access to a word copy of the survey -table document which could be filled in and sent to Dr Gennari so that she could upload the forms in the dedicated shared folder.

The text of the table in Italian (which can be found in the Annex) asked the partners. Here follows a synthesis of the questions and issues asked (the survey table text was in Italian)

- what was/were the activity/ies in which there were more problems
- partners were asked to describe the problem(s) connected to the application of the relevant legal framework
- it was asked whether the problem/s were solved
- And, if the reply to the previous question was yes, how they had managed to solve it/them
- there was another space called 'other' in which the partners could highlight all kinds of issues, and suggestions to the Activity 4 researchers group
- A dedicated space for suggestions and
- A dedicated space for documents (possibility to provide hyperlink) that might be useful to Activity 4 researchers
- The contacts of the responsible person for the partner institution

Six survey-tables were uploaded by the deadline of 31 March 2023.
On the one hand, the main issues concerned the legal application and/or interpretation doubts on

- the application of the employer's liability under Italian law when biorobotics devices and allied technologies were involved
- the application the research/hospital structure contractual liability for patients and third party damages
- whether there is the possibility to apply objective/strict liability rules to the research/hospital structure for dangerous activities while using biorobotics devices and allied technologies (Article 2050 of the Italian civil code)
- the application of extra-contractual liability rules (Gelli-Bianco law) to the single doctor work, especially if they used biorobotics devices and allied technology in their work
- the application of the EC conformity rules on medical devices under an insurance law perspective. More specifucally, the minimum requirements for insurance policy contracts are not clear. The survey participant interpreted extensively the Garante per la Protezione dei Dati Personali (Italian National Data Protection Authority (there is not an *ad hoc* document, hence the respondent had to apply in an analogue way what the Garante had established on the same problem but for pharmacological products
- the interaction of the Clinical Trials legislation with the GDPR. In particular, it was asked how to individuate the GDPR subjects (e.g. controllers, processors, third parties, recipients and data subjects)
- the lack of European enacting rules concerning the Early Feasibility Studies (EFS), which are admissible according to the Medical Devices Regulation (MDR) but have not been used yet in the EU.

On the other hand, the submitted suggestions were particularly interesting as they relied on taking into consideration for this deliverable

- The AI act proposal
- The GDPR application
- The update of the Machinery Directive, and, in particular, the agreement on its future update (Council agreement 7 February 2023), Directive EC/2006/42
- The update of the Product Liability Directive proposal

- To suggest a EU framework concerning an harmonized procedure for the Early Feasibility Studies (EFS in connection with the MDR)

Some survey-tables were not considered as they just stated the objectives stated in activity 1 and 2 (patients and health operators needs) and access problems.

5 SUMMARY CONCLUSIONS

At the end of the first iteration of this deliverable there are some summary conclusive remarks that one can point out.

The contents of section 2 concerning methodology and the contents of section 4, which focus on the explanation of how the bottom-up approach was used through the distribution of the survey-table are now more than clearly explained and do not need to be re-iterated in detail here. To be brief, the methodology employed included two complementary approaches (top-down and bottom-up) which led to prioritise quality over quantity by limiting the number of legislative acts and proposals analysed in section 3.

However, as far as section 3 is concerned, it is difficult to have common conclusions, given the wide array and content diversity of the proposal analysed and some important ones that are yet to be analysed, such as the GDPR, the Data Act and the European Health Data Space (EDHS). Difficult as it might sound, there is at least one common *fil rouge* among the different legislative initiatives analysed: the ones concerning medical devices in general (the MDR and the IVMDR) seem not to have a clear connection with the upcoming AI act regulation, and cybersecurity-at-large frameworks (NIS I NIS II and Cyber Resilience Act). Moreover, these regimes that pertain to the different parts of the biorobotic devices (including the software and the product parts that make them) do not mention how they connect to the legislative block pertaining to the use of personal and non-personal data (the GDPR, the Data Act and the Free Flow of Data Inititiative) that the biorobotic device manufacturer could take advantage of not only to make the device work but also to improve it. Furthermore, the experimental character of the design and production of biorobotic devices and allied technologies must also take into account that the implementation of the Clinical Trials Regulation in Italy is far from being completed and clear for medical practitioners and biorobotic engineers.

Overall, A4 has now individuated the lack of explicit connection among these different legal regimes. The next steps and iterations of this deliverable will also need to investigate the remaining legal acts and proposals that could not be analysed at this stage. As a matter of facts, also this conclusion part of the deliverable has a 'living' character. With the better understanding of the interconnections between EU and Italian legislative acts and proposal to the design and construction of biorobotic devices and allied technologies, the structure of this deliverable will evolve and create a more biorobotic-devices-tailored legal analysis of the most relevant EU and national legislative acts and proposals. This deliverable will contribute to the Fit4MedRob bigger vision of having an integration between medicine, engineering and legal studies by outlining the legal framework from which it will be possible to realise legally and ethically compliant medical devices. Moreover, this deliverable is also a powerful tool from which Activity 4 might derive policy indications that can be addressed to the Italian legislator to better coordinate the different sets of EU rules and Italian rules concerning the regulation of Biorobotics devices and allied technologies.

6 REFERENCES

6.1 REFERENCES: THE RIGHT TO HEALTH AND THE MULTILEVEL HEALTHCARE DELIVERY

[1] Addis P., La Corte costituzionale, il diritto alla salute e la Convenzione ONU sui diritti delle persone con disabilità: alcune considerazioni sulla sentenza n. 236/2012, in www.osservatoriosullefonti.it, n. 2, 2013

[2] Aperio Bella F., L'accesso alle tecnologie innovative nel settore salute tra universalità e limiti organizzativi (con una postilla sull'emergenza sanitaria), in PA Persona e Amministrazione, n.1/2020, pp. 219-245.

[3] G. Arconzo, I diritti delle persone con disabilità, Milano, Franco Angeli, 2020

[4] Atripaldi M., Diritto alla salute e livelli essenziali di assistenza (LEA), in federalismi.it, novembre 2017, pp.1-18.

[5] Balduzzi R., Carpani G. (a cura di), Manuale di diritto sanitario, Il Mulino, Bologna, 2013.

[6] Balduzzi R., Servetti D., *Regionalismo differenziato e materia sanitaria*, in *Rivista AIC*, 2/2019.

[7] Bantekas I., Stein M.A., Anastasiou D.S. (a cura di), The UN Convention on the Rights of Persons with Disabilities: A Commentary, Oxford, Oxford University Press, 2018

[8] Barberis E., Colombo F., Kazepov Y., Saruis T., Istituzioni del welfare e innovazione sociale: un rapporto conflittuale?, in La Rivista delle Politiche Sociali, n. 1, 2019, p. 23

[9] Barnes C., The Social Model of Disability. Valuable or Irrelevant? In N. Watson, A. Roulstone, C. Thomas (a cura di), The Routledge Handbook of Disability Studies, London, Routledge, 2021, p. 112 ss.

[10] Barnes C., Capire il "modello sociale della disabilità", in Intersticios. Revista sociologica de pensamiento critico, Vol. 2, 1, 2008, p. 87

[11] Barranco Aviles M.d.C. , La disabilità intellettiva e la disabilità psicosociale come situazioni di vulnerabilita, in Rivista di filosofia del diritto, n. 2, 2018, p. 301

[12] Bianchi P., La tutela delle persone con disabilità nella prospettiva comparata, in C. Colapietro, A. Salvia, (a cura di), Assistenza, inclusione sociale e diritti delle persone con disabilità. A vent'anni dalla legge 5 febbraio 1992, n. 104, Editoriale Scientifica, Napoli, 2013, p. 379

[13] Binetti P., Abili, disabili, ma tutti diversamente abili, Roma, Edizioni Scientifiche Ma.Gi, 2021

[14] Borsay A., *Personal, Trouble or Public Issue?*, in L. Burton, M. Oliver (a cura di), *Disability Studies. Past, Present and Future*, Leeds, The Disability Press, 1997, p. 115

[15] Broderick A., Ferri D., *International and European Disability Law and Policy. Texts, Cases and materials*, Cambridge, Cambridge University Press, 2019

[16] Di Costanzo C., L'impiego delle nuove tecnologie nel settore della salute: problematiche e prospettive di diritto costituzionale, in Consulta online, n. 1/2023, pp. 214-229.

[17] De Burca G., The EU in the Negotiation of the UN Disability Convention, in European Law Review, Vol. 35, No. 2, 2010, p. 1 ss.

[18] Di Girolamo A. S., Livelli essenziali e finanziamento dei servizi sanitari alla luce del principio di leale collaborazione, in Le istituzioni del federalismo, n. 3/2007, pp. 482-505.

[19] Dossier Servizio Studi Camera dei deputati, I nuovi Livelli essenziali di assistenza (LEA), 29 settembre 2022.

[20] Ferioli E. A., L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano? in BioLaw Journal, n. 1/2019, pp. 163-175.

[21] Ferri D., La giurisprudenza costituzionale sui diritti delle persone con disabilità e lo Human Rights Model of Disability: "convergenze parallele" tra Corte costituzionale e Comitato ONU sui diritti delle persone con disabilità, in DirittiFondamentali, 1, 2020

[22] Ferri D., Broderick A., International and European disability law: Text, Cases and Materials (Law in Context), Cambridge, Cambridge University Press, 2019

[23] Ferri D., L'Unione europea e i diritti delle persone con disabilità: brevi riflessioni a vent'anni dalla prima 'Strategia', in Politiche sanitarie, n. 2, 2016, p. 118

[24] Kakouliss E., Ikeara Y., Art. 1, in I. Bantekas, M.A. Stein, D. Anastasiou (a cura di), The UN Convention on the rights of persons with disabilities, Oxford, Oxford University Press, 2018, p. 56
[25] Keynes S.E., Webber S.H., Beveridge K., Empowerment through care: Using dialogue between the social model of disability and the ethic of care to redraw boundaries of independence and partnership between disabled people and services, in ALTER, European Journal of Disability Research, 9, 2015
[26] Mainardis C., Il regionalismo italiano tra continuità sostanziale e le sfide del PNRR, in Le Regioni, n. 1-2, 2021, p. 139
[27] Morana D., La salute come diritto costituzionale, Giappichelli, Torino, 2021, pp. 115-119.
[28] O'Mahony C., Quinlivan S., The EU Disability Strategy and the Future of EU Disability Policies, in D. Ferri, A. Broderick, International and European disability law: Text, Cases and Materials (Law in Context), Cambridge, Cambridge University Press, 2019, p. 12
[29] Pajno S., Il sitema delle Conferenze e l'evoluzione delle relazioni istituzionali: un bilancio dell'esperienza repubblicana, in Un nuovo regionalismo per l'Italia di domani: le Regioni a 50 anni dalla loro istituzione, Presidenza del Consiglio dei ministri, 2022, pp. 1-23.
[30] Pioggia A., Diritto sanitario e dei servizi sociali, Giappichelli, Torino, 2012, pp.1-229.
[31] Rapporto GIMBE sul Servizio Sanitario Nazionale. Fondazione GIMBE: Bologna, n. 5/2022. Disponibile a: www.salviamo-ssn.it/5-rapporto.
[32] Report Osservatorio GIMBE, Livelli Essenziali di Assistenza: le diseguaglianze regionali in sanità. Fondazione GIMBE: Bologna, n. 2/2022. Disponibile a: www.gimbe.org/LEA_2010- 2019.
[33] Trapani M., Il sistema delle Conferenze e il regionalismo dimezzato: il difficile rapporto tra PNRR e Regioni alla luce delle recenti evoluzioni normative, in Rivista AIC, n. 4, 2021, p. 181
[34] Vimercati B., L'aggiornamento dei LEA e il coordinamento della finanza pubblica nel regionalismo italiano: il doppio intreccio dei diritti sociali, in Le Regioni, n.1/2017, pp.1-4.
[35] Waddington L., The European Union and CRPD: complexities, challenges and opportunities, in V. Della Fina, G. Palmisano, R. Cera (a cura di), The UNCRPD: a Commentary, Springer, 2017, p. 61 ss.

6.2 REFERENCES MEDICAL DEVICES REGULATION

[36] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, Document 31993L0042, ELI: http://data.europa.eu/eli/dir/1993/42/oj
[37] Consolidated text: Council Directive of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (90/385/EEC), Document 01990L0385-20071011, ELI: http://data.europa.eu/eli/dir/1990/385/2007-10-11
[38] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.)
[39] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.), OJ L 117, 5.5.2017, p. 176–332, ELI: http://data.europa.eu/eli/reg/2017/746/oj
[40] Yvonne Halpaus, 'Medical Device Directive 93/42/EEC CE-Marking What Manufacturers Need to Know & Do', 2015, QNET LCC
[41] Victoria Martindale, Andre Menache, 'The PIP scandal: an analysis of the process of quality control that failed to safeguard women from the health risks', May 2013, Journal of the Royal Society of Medicine
[42] Laura Maher, Niki Price, 'Ultimate Guide to IVDR for In Vitro Diagnostic Medical Device Companies', November 2022, Greenlight Guru
[43] Zaide Frias, 'Update on EMA role in implementation of new legislation for medical devices (MDR) and in vitro diagnostics (IVDR)', 20 November 2019
[44] S. Bowers, D. Cohen, 'How lobbying blocked European safety checks for dangerous medical implants' 2018

[45] Kosta Shatrov, Cart Rudolf Blankart, 'After the four-year transition period: Is the European Union's Medical Device Regulation of 2017 likely to achieve its main goals?', December 2022, Elsevier Health Policy, Volume 126, Issue 12, Pages 1233-1240
[46] MediCept, 'Eudamed Update: Implementation is Paused, MDR Compliance is Not', 29 April 2021
[47] MedTech, 'MedTech Europe Survey Report analysing the availability of Medical Devices in 2022 in connection to the Medical Device Regulation (MDR) implementation', 14 July 2022
[48] Oriel STAT A MATRIX Blog. 'Status of EU Notified Bodies Designated to EU MDR 2017/745 and IVD 2017/746', 21 April 2021
[49] MedTech Europe. The European Medical Technology Industry in figures; 2019
[50] C. Sorenson, M. Drummond, 'Improving medical device regulation: the United States and Europe in perspective', Milbank Q, 92 (1) (2014), pp. 114-150
[51] N. Martelli, D. Eskenazy, C. Déan, J. Pineau, P. Prognon, G. Chatellier, et al, 'New European regulation for medical devices: what is changing?', Cardiovasc Intervent Radiol, 42 (9) (2019), pp. 1272-1278, 10.1007/s00270-019-02247-0
[52] MDCG 2021-24 Guidance on classification of medical devices (October 2021)
[53] MDCG 2020-5 Clinical evaluation – Equivalence: A guide for manufacturers and notified bodies
[54] MDCG 2020-6 Clinical evidence needed for medical devices previously CE marked under Directives 93/42/EEC or 90/385/EEC
[55] Proposal REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards the transitional provisions for certain medical devices and in vitro diagnostic medical devices, Brussels, 6.1.2023, COM(2023) 10 final
[56] MedTech, 'MedTech Europe welcomes the adoption of amended transitional provisions of the Medical Devices Regulations and calls for continued work to address outstanding implementation challenges', 7 March 2023, MedTech Press Release
[57] MedTech, 'Recommendations on the use of Guidance Documents Related to the Medical Device Regulation (MDR) and In vitro Diagnostics Regulation (IVDR)', 28 June 2022
[58] D. Cohen, 'How a fake hip showed up failings in European device regulation', BMJ, 345 (2012), p. e7090, 10.1136/bmj.e7090
[59] Dhruva SS, Bero LA, Redberg RF. 'Strength of study evidence examined by the FDA in premarket approval of cardiovascular devices', JAMA. 2009;302(24):2679-2685
[60] Lenzer J, Brownlee S. 'The FDA is still letting doctors implant untested devices into our bodies', 4 January 2019, The Washington Post

6.3 REFERENCES IN VITRO DIAGNOSTIC MEDICAL DEVICES:

[61] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (Text with EEA relevance.), *OJ L 117, 5.5.2017, p. 176–332, ELI:* http://data.europa.eu/eli/reg/2017/746/oj
[62] Consolidated text: Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices, ELI: http://data.europa.eu/eli/dir/1998/79/2012-01-11
[63] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.), ELI: http://data.europa.eu/eli/reg/2017/745/oj
[64] 2010/227/: Commission Decision of 19 April 2010 on the European Databank on Medical Devices (Eudamed) (notified under document C(2010) 2363) (Text with EEA relevance), ELI: http://data.europa.eu/eli/dec/2010/227/oj

[65] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards the transitional provisions for certain medical devices and in vitro diagnostic medical devices, COM/2023/10 final
[66] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance)Text with EEA relevance, ELI: http://data.europa.eu/eli/reg/2017/745/2017-05-05
[67] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (Text with EEA relevance.), ELI: http://data.europa.eu/eli/reg/2017/745/oj
[68] MedTech Europe Survey Report analysing the availability of In vitro Diagnostic Medical Devices (IVDs) in May 2022 when the new EU IVD Regulation applies
[69] MedTech, 'Transition to EU IVD Regulation (EU) 2017/746 and considerations for non-EU regulatory authorities on managing the impact to product registrations', May 2022
[70] Dombrink, Isabel, Lubbers, Bart R., Simulescu, Loredana, Doeswijk, Robin, Tkachenko, Olga, Dequeker, Elisabeth, Fraser, Alan G, van Dongen, Jacques J. M, Cobbaert, Christa, Brüggemann, Monika, Macintyre, Elizabeth, 'Critical Implications of IVDR for Innovation in Diagnostics: Input From the BioMed Alliance Diagnostics Task Force', *HemaSphere,* 6(6):p e724, June 2022.*DOI:* 10.1097/HS9.0000000000000724
[71] British Standards Institution, 'A guide to the In Vitro Diagnostic Directive', 2012
[72] Victoria Martindale, Andre Menache, 'The PIP scandal: an analysis of the process of quality control that failed to safeguard women from the health risks', May 2013, Journal of the Royal Society of Medicine
[73] Laura Maher, Niki Price, 'Ultimate Guide to IVDR for In Vitro Diagnostic Medical Device Companies', November 2022, Greenlight Guru
[74] Zaide Frias, 'Update on EMA role in implementation of new legislation for medical devices (MDR) and in vitro diagnostics (IVDR)', 20 November 2019, Annual PCWP/HCPWP meeting with all eligible organisations
[75] MediCept, 'Eudamed Update: Implementation is Paused, MDR Compliance is Not', 29 April 2021
[76] MedTech, 'Industry Perspective on the Implementation Status of the MDR/IVDR', 14.06.2019
[77] MedTech, 'Transition to the IVD Regulation – MedTech Europe Survey Results for October 2022', Public report February 2023
[78] Motion 20.3211, 'Für mehr Handlungsspielraum bei der Beschaffung von Medizinprodukten zur Versorgung der Schweizer Bevölkerung', accepted by the Swiss National Council on Monday 28 November
[79] U.S Food & Drug Administration, Overview of IVD Regulation, https://www.fda.gov/medical-devices/ivd-regulatory-assistance/overview-ivd-regulation
[80] Government du Canada, 'Guidance Document: Guidance for the Risk-based Classification System for In Vitro Diagnostic Devices (IVDDs)', 2016-10-07

6.4 REFERENCES FREE FLOW OF DATA REGULATION

[81] Bauer et al (2016), Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, ECIPE Policy Brief, 3/2016
[82] Bird & Bird (2017) Data Flows - Future Scenarios, IPOL Study IP/A/ITRE/IC
[83] N Cherciu, T Chirvase (2020), Non data processing – why should we take it personally?, EJPLT 2/2020
[84] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, SWD(2017)304 final

[85] Commission Communication, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250 final
[86] FR Dal Pozzo, L Zoboli (2021), To protect or (not) to protect: definitional complexities concerning personal (and non-personal) data within EU, Eurojus 1/2021
[87] DG Connect Report (2017) Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, SMART number 2017/0084
[88] DG Connect Report (2015), Facilitating cross border data flow in the Digital Single Market, SMART number 2015/0016
[89] DG Connect Report (2015), Cross-border data flow in the digital single market: study on data location restrictions, SMART number 2015/0054
[90] J Drexl (2016) Designing Competitive Markets for Industrial Data: Between Propertisation and Access, Max Planck Institute for Innovation & Competition, Research Paper, No. 16-13
[91] J Drexl et al (2016), Data Ownership and Access to Data, Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the current European Debate, Max Planck Institute for Innovation and Competition Research Paper no. 16-10
[92] EU Data Protection Supervisor (2018), Comments of the EDPS on a Proposal of the European Parliament and of the Council on a framework for the free-flow of non-personal data in the European Union
[93] T Fia (2021), An Alternative to Data Ownership : Managing Access to Non-Personal Data through the Commons, Global Jurist 21(1)
[94] IMCO Committee (2018), Briefing - Optimal Scope for Free-Flow of Non-Personal Data in Europe
[95] A Kak, S Sacks (2021), Shifting Narratives and Emerging Trends in Data-Governance Policies, Yale Law School Report
[96] N Cori, L Dascoli (2021), How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, ITIF Report
[97] Osborne-Clarke LLP (2016) Legal Study on Ownership and Access to Data
[98] HC Scheu (2019), The Public Security Exception in the Law of the European Union, Security Theory and Practice 4/2019

6.5 REFERENCES AI ACT PROPOSAL

[99] European Commission, Artificial Intelligence for Europe, COM(2018) 327 final, 2018.
[100] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.
[101] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, COM(2020) 65 final, 2020.
[102] Commission Staff Working Document, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 final, PART 1/2 and 2/2.
[103] OECD, Recommendation of the Council on Artificial Intelligence, 2019
[104] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
[105] Proposal for a Directive of the European Parliament and of the Council on liability for defective products, COM(2022) 495 final.
[106] Proposal for a directive of the European Parliament and of the Council on adapting noncontractual civil liability rules to artificial intelligence (AI Liability Directive), COM(2022) 496 final.
[107] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final.
[108] Commission Staff Working Document, Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 final, PART 2/2, p. 35.
[109] European Commission, DRAFT Request on a standardisation request to the European Committee for Standardisation (CEN) and the European Committee for Electrotechnical Standardisation (CENELEC) in support of safe and trustworthy artificial intelligence, 5 December 2022.
[110] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (SocArXiv, 5 July 2021) <https://osf.io/preprints/socarxiv/38p5f/>.

[111] European Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, April 2021, p. 113 ff.

6.6 REFERENCES CYBER RESILIENCE ACT PROPOSAL

[112] Regulation (EU) 2019/1020 on market surveillance and compliance of products;
[113] Directive (EU) 2013/40 of the European Parliament and of the Council, concerning attacks against information systems;
[114] Directive (EU) 2016/1148 of the European Parliament and of the Council on the security of networks and information systems, also known as the "NIS directive";
[115] NIS2;
[116] Regulation (EU) 2019/881 of the European Parliament and of the Council, on cybersecurity and, in particular, on the certification of cybersecurity in order to improve TIC products, services, and processes;
[117] The EU's cybersecurity strategy for the digital decade;
[118] The Council's conclusions of 2 December 2020;
[119] The Council's conclusions of 23 May 2022;
[120] The European Parliament's resolution of 10 June 2021;
[121] Regulation (EU) 2016/679 of the European Parliament and of the Council, concerning the protection of personal data;
[122] Regulation (EU) 2017/745 of the European Parliament and of the Council, concerning medical devices;
[123] Regulation (EU) 2017/746 of the European Parliament and of the Council, concerning *in vitro* diagnostic medical devices;
[124] Regulation (EU) 2019/2144 of the European Parliament and of the Council, concerning the approval requirements for motor vehicles and their trailers, as well as systems, components and technical entities intended for such vehicles, with regard to their general safety and the protection of vehicle occupants and vulnerable road users;
[125] Regulation (EU) 2018/1139 of the European Parliament and of the Council, laying down common rules in the field of civil aviation;
[126] Directive 85/374 of the Council, concerning the approximation of the laws, regulations, and administrative provisions of the Member States on liability for defective products.

6.7 REFERENCES: NIS I DIRECTIVE

[127] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[128] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENTAND THE COUNCIL Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148concerning measures for a high common level of security of network and information systems across the Union, Brussels, 4.10.2017

[129] COMMISSION IMPLEMENTING REGULATION (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

[130] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, Bruxelles, 28.10.2019

[131] Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)- No. 2020-665, Final Study Report

6.8 REFERENCES NIS II DIRECTIVE PROPOSAL

[132] Explanatory memorandum of the Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final

[133] Sandra Schmitz-Berndt · Pier Giorgio Chiara, One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive, Int. Cybersecur. Law Rev. (2022) 3: 293-311.

[134] Thomas Sievers, Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. Int Cybersecur Law Rev (2021) 2:223–

6.9 REFERENCES INSURANCE LAW

[135] Buonanno, "Il PNRR potenzia l'assistenza domiciliare con la telemedicina", in Quotidiano Leggi d'Italia Professionale, 5 luglio 2022

[136] P. Cosmai, Il governo torna sulla telemedicina: fissati I requisiti funzionali e I livelli di servizio, Azienditalia, 2023, 1, 57

[137] G. Votano Intelligenza artificiale in ambito sanitario: il problema della responsabilità civile, Danno e Resp., 2022, 6, 669.

[138] PPE Regulation Guidelines - Guide to application of Regulation EU 2016/425 on personal protective equipment (available here https://ec.europa.eu/docsroom/documents/29201)

7 ANNEX

7.1 ANNEX I. SURVEY-TABLE

Fit4MedRob – Missione 1
Scheda di segnalazione nodi e problematiche per Attività 4

DATA	
ATTIVITA' COINVOLTA (breve descrizione del caso con indicazione degli elementi ritenuti caratterizzanti)	
PROBLEMA INCONTRATO – NODO DA SCIOGLIERE	
RISOLTO? (si o no, anche provvisoriamente)	
SE SI, **COME?**	
ALTRO (segnalare qualsiasi cosa si ritenga rilevante inclusi suggerimenti o documenti di riferimento)	
• **SUGGERIMENTI** (es.: utile una modifica normativa, la predisposizione di linee guida da parte del tale soggetto istituzionale, di faq, etc…)	
• **DOCUMENTI** (es.: legge xy, circolare kz di tizio, polizza jnf, etc…)	
REFERENTE (indicare indirizzo e-mail e/o telefono per eventuali chiarimenti o approfondimenti)	

7.2 ANNEX II. SURVEY FEEDBACKS

Fit4MedRob – Missione 1
Scheda di segnalazione nodi e problematiche per Attività 4

DATA	
ATTIVITA' COINVOLTA (breve descrizione del caso con indicazione degli elementi ritenuti caratterizzanti)	Identificazione dei bisogni dei pazienti e degli operatori Dare priorità ai bisogni più importati per i pazienti e focalizzare su questi i primi trial da avviare
PROBLEMA INCONTRATO – NODO DA SCIOGLIERE	Necessità di raggiungere questo obiettivo entro maggio e quindi senza passare dal CE (non ne avremmo il tempo)
RISOLTO? (si o no, anche provvisoriamente)	no
SE SI, **COME?**	
ALTRO (segnalare qualsiasi cosa si ritenga rilevante inclusi suggerimenti o documenti di riferimento)	Saranno inviati i consensi comunemente compilati nei centri clinici ed un form di survey
• **SUGGERIMENTI** (es.: utile una modifica normativa, la predisposizione di linee guida da parte del tale soggetto istituzionale, di faq, etc…)	
• **DOCUMENTI** (es.: legge xy, circolare kz di tizio, polizza jnf, etc…)	
REFERENTE (indicare indirizzo e-mail e/o telefono per eventuali chiarimenti o approfondimenti)	Don Gnocchi (Roma) Unipv

Fit4MedRob – Missione 1
Scheda di segnalazione nodi e problematiche per Attività 4

DATA	08/03/2023
ATTIVITA' COINVOLTA (breve descrizione del caso con indicazione degli elementi ritenuti caratterizzanti)	Indagine generale del panorama normativo
PROBLEMA INCONTRATO – NODO DA SCIOGLIERE	• Responsabilità del datore di lavoro nell'ipotesi di danni al lavoratore da apparecchiatura robotica e valutazione dell'attuale idoneità a regolamentare la tematica da parte del **TU in materia di sicurezza 81/08**; • Nel caso di **danni a pazienti o a terzi**, si potrebbe profilare una problematica inerente alla responsabilità della struttura e alla eventuale normativa applicabile. Dal punto di vista civilistico, ci si può chiedere se, oltre alla responsabilità ex art 1218 c.c. e 1228 c.c. - rispettivamente, per colpa propria e dell'operatore sanitario – la struttura possa anche rispondere ai sensi dell'art. 2050 c.c., per esercizio di attività pericolosa. In quest'ultimo senso può profilarsi la problematica concernente il perimetro delle misure di diligenza necessarie per escludere eventuali responsabilità; • Si potrebbe profilare un problema della **responsabilità del medico**, civile e penale, nel caso di danno a paziente. In quest'ultimo senso, si potrebbe valutare la possibile applicazione della L. n. 24/2017 (c.d. Gelli-Bianco) e la necessità di predisporre delle apposite **linee guida** che il medico possa seguire per andare esente da eventuale responsabilità.
RISOLTO? (si o no, anche provvisoriamente)	no
SE SI, **COME?**	
ALTRO (segnalare qualsiasi cosa si ritenga rilevante inclusi suggerimenti o documenti di riferimento)	○ Non si riscontrano testi normativi di carattere locale. ○ Rimane fermo che la normativa interna risulterà inevitabilmente condizionata dalla normativa europea che, una volta entrata in vigore,

	porterà il legislatore interno ad adeguarsi attraverso la modifica degli attuali testi di legge.
• **SUGGERIMENTI** (es.: utile una modifica normativa, la predisposizione di linee guida da parte del tale soggetto istituzionale, di faq, etc…)	Nella previsione di condurre uno studio normativo su robotica che si serva dell'intelligenza artificiale (AI), si segnalano: ○ la proposta di regolamento del Parlamento Europeo del 21 aprile 2021 sul **regolamento dell'intelligenza artificiale**; il documento dovrebbe essere approvato entro la fine del 2023. Allo stato attuale sono incorsi i negoziati interistituzionali e il documento più recente che si riscontra è **l'orientamento generale del Parlamento Europeo del 25 novembre 2022**. ○ Sempre con particolare riferimento alle AI, **Regolamento n. 649/2016 sul trattamento dati personali (c.d. GDPR)** e problemi relativi al trattamento dei dati c.d. particolari dei pazienti (in particolare dati sanitari).
• **DOCUMENTI** (es.: legge xy, circolare kz di tizio, polizza jnf, etc…)	• **Direttiva macchine 2006/42/CE**, attualmente in vigore; • **Accordo provvisorio del 7 febbraio 2023 r**isultante da negoziati interistituzionali per il **nuovo regolamento macchine (***Regulation of the European Parliament and of the Council on machinery*), che, una volta terminato l'iter di approvazione, sostituirà l'attuale direttiva macchine 2006/42/CE; • La **Proposta di una nuova direttiva per la responsabilità da prodotti difettosi** del 28 settembre 2022, che dovrebbe applicabile a robot, droni, sistemi di domotica, AI.
REFERENTE (indicare indirizzo e-mail e/o telefono per eventuali chiarimenti o approfondimenti)	COT

Fit4MedRob – Missione 1
Scheda di segnalazione nodi e problematiche per Attività 4

DATA	13.03.2023
ATTIVITA' COINVOLTA (breve descrizione del caso con indicazione degli elementi ritenuti caratterizzanti)	Sottomissione documentazione CE competente/istruttoria pratica AC

PROBLEMA INCONTRATO – NODO DA SCIOGLIERE	Individuazione dei requisiti minimi per l'emissione di polizze assicurative studio-specifiche e relativa tempistica.
RISOLTO? (si o no, anche provvisoriamente)	Provvisoriamente.
SE SI, **COME?**	Applicando per analogia la normativa del DM 2009 in materia farmacologica e proponendo la sottomissione di un preventivo e non della polizza già emessa (in modo da attivarla solo ad avvenuto ottenimento del parere del CE competente).
ALTRO (segnalare qualsiasi cosa si ritenga rilevante inclusi suggerimenti o documenti di riferimento)	/
• **SUGGERIMENTI** (es.: utile una modifica normativa, la predisposizione di linee guida da parte del tale soggetto istituzionale, di faq, etc…)	Aggiornamento normativo e emissione di linee guida da parte del Ministero della Salute e/o Centro Nazionale Coordinamento dei CE.
• **DOCUMENTI** (es.: legge xy, circolare kz di tizio, polizza jnf, etc…)	DM 14.07.2009, Requisiti minimi per le polizze assicurative a tutela dei soggetti partecipanti alle sperimentazioni cliniche dei medicinali.
REFERENTE (indicare indirizzo e-mail e/o telefono per eventuali chiarimenti o approfondimenti)	La Nostra Famiglia

Fit4MedRob – Missione 1
Scheda di segnalazione nodi e problematiche per Attività 4

DATA	13.03.2023
ATTIVITA' COINVOLTA (breve descrizione del caso con indicazione degli elementi ritenuti caratterizzanti)	Sottomissione documentazione CE competente/istruttoria pratica AC
PROBLEMA INCONTRATO – NODO DA SCIOGLIERE	Identificazione dei ruoli privacy in ambito di indagini cliniche.

RISOLTO? (si o no, anche provvisoriamente)	Provvisoriamente.
SE SI, **COME?**	Applicando per analogia lo schema suggerito dal Garante Privacy (risalente al 2008) in tema di sperimentazioni farmacologiche – ossia la titolarità autonoma tra Promotore e Centro Clinico.
ALTRO (segnalare qualsiasi cosa si ritenga rilevante inclusi suggerimenti o documenti di riferimento)	/
• **SUGGERIMENTI** (es.: utile una modifica normativa, la predisposizione di linee guida da parte del tale soggetto istituzionale, di faq, etc…)	Normativa specifica o pronuncia del Garante Privacy in linea con il GDPR.
• **DOCUMENTI** (es.: legge xy, circolare kz di tizio, polizza jnf, etc…)	Garante Privacy, Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008.
REFERENTE (indicare indirizzo e-mail e/o telefono per eventuali chiarimenti o approfondimenti)	La Nostra Famiglia

Fit4MedRob – Missione 1
Scheda di segnalazione nodi e problematiche per Attività 4

DATA	22.3.2023
ATTIVITA' COINVOLTA (breve descrizione del caso con indicazione degli elementi ritenuti caratterizzanti)	Tentativo apertura link per compilazione scheda segnalazione partner
PROBLEMA INCONTRATO – NODO DA SCIOGLIERE	All'apertura della pagina viene chiesto nome utente e password con template di mail santannapisa.it

RISOLTO? (si o no, anche provvisoriamente)	no
SE SI, **COME?**	
ALTRO (segnalare qualsiasi cosa si ritenga rilevante inclusi suggerimenti o documenti di riferimento)	
• **SUGGERIMENTI** (es.: utile una modifica normativa, la predisposizione di linee guida da parte del tale soggetto istituzionale, di faq, etc…)	
• **DOCUMENTI** (es.: legge xy, circolare kz di tizio, polizza jnf, etc…)	
REFERENTE (indicare indirizzo e-mail e/o telefono per eventuali chiarimenti o approfondimenti)	Fondazione Mondino

Fit4MedRob – Missione 1
Scheda di segnalazione nodi e problematiche per Attività 4

DATA	27/03/2023
ATTIVITA' COINVOLTA (breve descrizione del caso con indicazione degli elementi ritenuti caratterizzanti)	Early feasibility studies (EFS). Gli EFS sono studi circoscritti fatti per raccogliere informazioni su dispositivi clinici o tecnologie durante le prime fasi di sviluppo, al fine di valutarne la sicurezza clinica, la funzionalità e introdurre eventuali modifiche o miglioramenti prima di passare a indagini cliniche più ampie.
PROBLEMA INCONTRATO – NODO DA SCIOGLIERE	○ Il MDR europeo indica in maniera generale che per gli EFS è necessario fare riferimento - oltre che all'impianto generale della normativa europea - anche al quadro normativo dello Stato Membro in cui lo sponsor desidera svolgerli. Il problema è che al momento **nessun Paese europeo ha implementato una procedura standard o leggi o regolamenti nazionali per questo tipo di studi**. ○ In alcuni Stati Membri, come l'Italia, le procedure per l'autorizzazione delle indagini cliniche non hanno il livello di **interazione tra autorità competenti e sponsor** che sarebbe invece necessario negli EFS, dove le modifiche al protocollo o dispositivo sono più frequenti rispetto ad altri studi. Inoltre, dal momento che l'esperienza dei Paesi europei con gli ESF è limitata, spesso chi dovrebbe valutare e seguire questi studi non ha le **competenze tecniche** per farlo. ○ Di conseguenza, **gran parte degli EFS vengono svolti al di fuori dell'UE**, specialmente negli USA, dove la FDA ha introdotto nel 2013 un programma ad hoc per gli EFS per agevolare e facilitare le procedure per fare domanda e svolgere tali studi. ○ L'assenza di un framework standardizzato per gli EFS rischia di **ridurre l'attrattività dell'UE** per gli studi clinici iniziali e gli investimenti in R&D e di **limitare o ritardare l'accesso a tecnologie mediche innovative** da parte dei pazienti europei.

RISOLTO? (si o no, anche provvisoriamente)	No. In Italia c'era stato un tentativo di formulare un programma per gli EFS che però non ha portato a sviluppi concreti.
SE SI, **COME?**	
ALTRO (segnalare qualsiasi cosa si ritenga rilevante inclusi suggerimenti o documenti di riferimento)	Si intende far riferimento ad alcune proposte progettuali europee che sono focalizzate sul problema specifico (es.: bandi IHI, call 2)
• **SUGGERIMENTI** (es.: utile una modifica normativa, la predisposizione di linee guida da parte del tale soggetto istituzionale, di faq, etc…)	Sarebbe utile sviluppare un **programma EFS europeo** con una procedura amministrativa ad hoc e un quadro normativo standard per lo svolgimento di EFS in Europa. Un programma europeo contribuirebbe inoltre a rafforzare l'interazione tra le parti coinvolte durante tutto il processo, promuovendo maggiore flessibilità nel caso di modifiche necessarie e uno scambio più proficuo di informazioni riguardo all'innovazione e ai dati raccolti.
• **DOCUMENTI** (es.: legge xy, circolare kz di tizio, polizza jnf, etc…)	• *L' Articolo 62* nel MDR sulle prescrizioni generali relative alle indagini cliniche non fornisce alcun dettaglio sulla procedura per gli EFS, ma rimanda, tra gli altri, al seguente Allegato; • l'*Allegato XIV "Valutazione clinica e follow-up clinico post-commercializzazione",* di cui *l'Articolo 1(a)* precisa che i fabbricanti devono avere "un piano di sviluppo clinico indicante la progressione da indagini esplorative, quali studi first-in-man, studi di fattibilità e studi pilota, a indagini di conferma, quali indagini cliniche di conferma (pivotal), e un PMCF […]". L'allegato tuttavia non fornisce ulteriori informazioni sulla metodologia per eseguire tali studi. • Il documento del Medical Device Coordination Group intitolato "*Regulation (EU) 2017/745 – Questions and Answers regarding clinical investigation*" specifica che il quadro normativo deve essere scelto in base al piano di sviluppo clinico e all'uso che si vuole fare dei dati clinici: se i dati clinici servono per la valutazione di conformità, l'indagine clinica deve seguire la procedure nell'Articolo 62, altrimenti si potrà seguire la procedura normativa nazionale dello Stato Membro (Articolo 82 MDR) in cui si intende condurre l'indagine clinica (e dunque l'EFS).

REFERENTE (indicare indirizzo e-mail e/o telefono per eventuali chiarimenti o approfondimenti)	Don Gnocchi