



Offline Data



POSITION PAPER

GLOBAL

DATA

CONFERENCE

2023



GLOBAL DATA CONFERENCE

First Edition

SUMMARY

THE GLOBAL DATA CONFERENCE 2023 AND FUTURE EDITIONS	5
GDC 2023, OFFICINE DATI & INFORMATION SOCIETY LAW CENTER UNIMI	8
POSITION PAPER	11
1. EUROPEAN DIGITAL STRATEGY	11
A. Digital strategy and data governance	12
Executive summary	12
Three core pillars of the European digital strategy	12
Taking action under a regulatory perspective	12
Taking action from a technological point of view	13
Critical issues in the EU approach	15
B. Digital Sovereignty	17
Executive summary	17
The idea of "digital sovereignty"	17
Digital sovereignty in the EU: critical sparks	18
Digital sovereignty in other countries	19
Digital sovereignty from a technological point of view	21
C. European strategy and challenging goals	23
Executive summary	23
European digital strategy challenges	23
Conclusions	25
2. ROLES AND POWERS OF THE SUPERVISORY AUTHORITIES	27
A. Independence of Authorities	28
Executive Summary	28
Selection Criteria	28
Freedom from Influence	29
Organizational and Financial Autonomy	30
Sectoral Competence and Norm-setting Power	31
Anticipatory compliance	31
B. Plurality of Regulatory Authorities	32
Executive Summary	32
Proliferation of Authorities	32
Plurality of Competencies	33
Allocation of Competencies	33
Integration Among Authorities	34
Structural Asymmetries of Authorities	35



C. Cooperation Among Authorities	35
Executive summary	35
Introduction	35
Cooperation Among EU Authorities Responsible for the Same Subject Matter	36
Cooperation Among National Authorities Responsible for Different Subjects but Within the Digital Sphere	37
Cooperation Among EU Authorities, Responsible for Different Subjects but Within the Digital Sphere	38
D. Sanctioning Powers	39
Executive Summary	39
Internal Regulation of Supervisory Authorities	39
Modulation of Sanctions	40
Guidance on the allocation of sanction revenues	41
3. VULNERABLE SUBJECTS AND EFFECTIVENESS OF PROTECTIONS	42
A. Some critical aspects in the relationship between data protection and user/consumer protection (and some regulatory suggestions)	43
Executive summary	43
B. The world of healthcare: critical points on patient protection (and some proposals)	44
Executive summary	44
C. The centrality of the child in the information society (and its protection)	47
Executive summary	47
D. Worker protection in relation to data protection	49
Executive summary	49
4. DATA MONETIZATION	52
A. Data Valorization and Institutions	53
Executive Summary	53
Introduction	54
Building the European Market	54
Worries	56
B. Data Valuation from a Market Perspective	59
Executive Summary	59
Introduction	59
Data Valuation and Business Opportunities	60
Data Valuation and the GDPR	61
C. Data Valorization from the Jurists' Perspective	63
Executive Summary	63
Introduction	63
Transparency and Information Asymmetry	64
Economic Valorization of Personal Data and Legal Bases	65
The limit of the contractual autonomy of the parties in establishing a relationship for the provision of services in exchange for personal data	67
PARTICIPANTS	69
Roundtable 1 – European Digital Strategy	69
Roundtable 2 – Roles and powers of the Supervisory Authorities	71



Roundtable 3 – Vulnerables subjects and effectiveness of protections	73
Roundtable 4 – Data Monetization	75



Officine Dati





Officine Dati



THE GLOBAL DATA CONFERENCE 2023 AND FUTURE EDITIONS

The first edition of the Global Data Conference event, organized by the Officine Dati Association and the Information Society Law Center of the University of Milan, took place on February 9, 2023.

The initiative was held at the University of Milan, in Via S. Antonio, No. 5 - Aula Pio XII, and revolved around the work of four thematic tables that saw the participation of more than 80 experts from the professional privacy world and representatives from the institutional, academic and BigTech worlds.



Figure 1 - Morning plenary.

The GDC received the sponsorship of the Italian Data Protection Authority, the Municipality of Milan, the Milan Bar Association, and the Milan Order of Accountants and Bookkeepers.

The activity of each table focused on a specific topic.



- The discussion of Table 1 revolved around the 'EU Digital Strategy'.
- Table 2, on the other hand, addressed the topic of 'Role and Powers of National Independent Authorities.'
- The discussion at Table 3 dealt with the topic of 'Vulnerable Subjects and Effectiveness of Safeguards.'
- Finally, Table 4 focused on the topic of 'Data Monetization.'

The event was then complemented by international keynote speakers who addressed, from different continental aspects and viewpoints, the topic of digital, data and related challenges in China, the United States of America and Europe.

The work of the tables developed over the course of the morning.

In the afternoon, in the plenary session, the results of the day were presented to the audience by the individual co-hosts.

Following this, the Organizing Committee of the Global Data Conference processed the results of the day to produce this Position Paper, which is subsequently published by the organizers.

The Global Data Conference aims to become a reference point in the scientific-dissemination panorama related to the issues of digital transformation, data protection and the development of technological sensitivity in Italy. Hopefully, the lines drawn in this paper will be of help and guidance in advancing the government's agenda in these issues.

The Position Paper is to be understood as a collective 'policy draft' exercise of a dissemination forum consisting of representatives of institutions, researchers and university professors, and representatives of the professional world and large technology companies.

The document is structured as follows:

- The first section indicates the characteristics and rules of engagement of the Global Data Conference 2023 and introduces the two organizing bodies, the Officine Dati Association and the Information Society Law Center of the University of Milan.



Officine Dati



- Following are the abstracts of the papers from the individual tables and their respective analyses.
- Attached are the results of the survey preparatory to the proceedings.



Officine Dati



GDC 2023, OFFICINE DATI & INFORMATION SOCIETY LAW CENTER UNIMI

The Global Data Conference 2023 was held for the entire day on February 9, 2023, involving more than 80 leading Italian and European digital and data protection experts representing institutions, academia, and the professional world. Each table discussed a general theme divided into 3 or 4 more specific topics.

In the morning, after a brief introduction to the work in the Pio XII Hall by the Organizing Committee, 4 working tables met in two sessions of about 1.5 hours discussing analysis with respect to the topics covered by the initiative, either collectively or divided into sub-panels. In the afternoon, the tables met in the General Plenary in Pius XII Hall and the initiative opened to the public.



Figure 2 – Introduction of the GDC 2023 by the organizing committee.

The Organizing Committee then proceeded to conduct the collective session. First, the recorded speeches of 5 international Keynote Speakers were screened, bringing their views from different continental perspectives, and then with focus on the European Union and North America, read in



the context of global trends. After the Keynote speakers, the discussion coordinators at each table presented to the assembly the results of the morning's discussions, which were then analyzed, assembled, processed, and drafted for this Position Paper.



Figure 3 - Ann Cavoukian's speech..

Officine Dati was founded as a think tank aimed at stimulating discussions and insights and, more generally, broadening horizons and awareness on the topic of data (personal and non-personal) and their protection. Through events, discussion initiatives, moments of dissemination and research, the association wants to involve, in the most comprehensive way possible, as many private, public, institutional and academic stakeholders as possible, with the aim of disseminating knowledge in the issues related to data protection and valorization, AI, cybersecurity, protection of electronic communications and harmonization and development of the digital economy. Officine Dati aims to be a point of reference in a chaotic context, characterized by a strong background noise made of regulatory overproduction and many voices not always supported by a cognitive background. Thus,



Officine Dati



the Association's mission is to raise awareness that data protection is a fundamental individual right and a cornerstone of the very principle of democracy.

The **Information Society Law Center** is a multidisciplinary research center of the University of Milan established at the "Cesare Beccaria" Department. Established in 2017, it is a center dedicated to the study of legal, technological, political and social aspects of the Information Society. The Center's goal is to conduct research on issues related to the relationship between law and digital society, with particular attention to those changes - present and future - that will profoundly affect our society. The Department of Law "Cesare Beccaria" is structured around the idea, of Enlightenment origin, that the study of law cannot be separated from the analysis of basic socio-economic institutions, both of which are influenced by and shape the law itself. The department undertakes and promotes interdisciplinary research projects aimed at strengthening understanding of the multiple connections of law with the underlying socio-economic dynamics



Officine Dati



POSITION PAPER

1. EUROPEAN DIGITAL STRATEGY



The topic of the EU's digital strategy was addressed according to the following profiles:

Digital strategy and data governance

Digital Sovereignty

European strategy and challenging goals



A. Digital strategy and data governance

Executive summary

Three core pillars of the European digital strategy

The European Digital Strategy, as presented by the European Commission in February 2020, is based on three key pillars:

1. Technologies at work for people: this pillar places an emphasis on improving the digital skills of European citizens to ensure their ability to use digital technologies in an effective and knowledgeable manner. It also commits towards providing access to high-quality digital public services across the EU, ensuring inclusiveness and accessibility to all. This pillar also emphasizes the importance of protecting citizens' rights, including privacy and security of personal data.
2. A fair and competitive economy: this pillar focuses on promoting an environment conducive to digital innovation and the adoption of digital technologies by European businesses. It includes promoting investment in the emerging technologies such as artificial intelligence, the Internet of Things, blockchain, and others. It also commits to developing high-speed digital infrastructure across the EU, ensuring reliable and fast connectivity for all citizens and businesses. Further, this pillar also aims at creating a single European digital market by removing those barriers preventing the free flow of digital data and services between EU member states.
3. An open, democratic, and sustainable society: This pillar focuses on promoting European values in the digital sphere. It includes protecting citizens' fundamental rights in the digital environment, such as freedom of expression, protecting personal data, and combating online disinformation. This pillar also seeks cybersecurity by protecting digital infrastructure and countering cyber threats and exploits digital technology to address environmental challenges, such as the transition to a low-carbon economy.

Taking action under a regulatory perspective

The implementation of the European digital strategy involves a variety of measures, including the development of new laws and regulations, funding programs for digital innovation, public-private



collaborations, and international partnerships. The goal is to promote a shared vision of a European digital society and economy while ensuring inclusion, rights protection, and sustainability.

There are two distinct understandings of the European digital strategy, which complement each other.

Strictly speaking, the digital strategy refers to European rules governing data, including personal data. These rules balance the need to ensure the circulation of data as an essential prerequisite for an advanced digital society with the protection of personal data as a fundamental right. The General Data Protection Regulation (GDPR) is an important pillar of this framework. The GDPR establishes clear rules on the collection, processing, and storage of personal data, thereby protecting the privacy and rights of European citizens. This framework provides a consistent basis for data management within the EU.

In a broad sense, the European digital strategy extends beyond the regulation of personal data and includes the digital package, a set of European regulations that aim to regulate the digital society as a whole. This regulatory package aims to create common European regulation to foster digital innovation, ensure equitable access to digital services, promote a digital single market, and ensure cybersecurity. It also includes initiatives to improve digital infrastructure and connectivity across the EU.

These two interpretations complement each other: the regulation on personal data, as provided for in the GDPR and other related regulations, is a key component in ensuring the protection of individual rights in the digital environment. At the same time, the digital package encompasses a broader vision of the regulation of the digital society, including the promotion of innovation, the creation of a single European digital market, and cybersecurity.

In summary, the European digital strategy spans both the personal data discipline and the digital package. Personal data protection and promotion of the advanced digital society are closely intertwined goals within this strategy.

Taking action from a technological point of view

In her State of the Union Address in September 2020, President von der Leyen announced that Europe should ensure digital sovereignty with a common EU vision in 2030, based on clear goals and



principles. In response, the European Council called on the Commission to present a comprehensive Digital Compass by March 2021, outlining digital ambitions for 2030, establishing a monitoring system, and outlining key targets and the means to achieve them.

The strategy already outlined in a program of policy reforms, which began with the Data Governance Act, the Digital Services Act, the Digital Markets Act, and the Cybersecurity Strategy, also includes funding to build Europe's Digital Decade. Several Union budget instruments will support the investments needed to accompany the digital transition.

The EU's digital ambitions have been concretely translated into the Digital Compass setting concrete goals to be achieved by 2030. The main ones among these goals are:

- The Digital Single Market presupposes the free movement of data between member states and involves harmonizing regulations, reducing barriers, and promoting cross-border digital activities.
- In addition to the target on basic digital skills set out in the European Pillar of Social Rights Action Plan for 80 percent of adults to have at least basic digital skills in 2030, the target is to train 20 million employed ICT specialists in the EU, with convergence between women and men.
- All European households will be covered by a Gigabit network, with all inhabited areas covered by 5G.
- State-of-the-art, sustainable semiconductor manufacturing in Europe, including processors, account for at least 20 percent of the world's production by value (i.e., manufacturing capacity below 5nm targeting 2nm and 10 times more energy efficient than today).
- The proposed level of ambition is that by 2025, Europe will have its first quantum-accelerated computer paving the way for being at the forefront of quantum capabilities by 2030.
- 75% of European enterprises will adopt cloud computing, big data, and artificial intelligence services.



- More than 90 percent of European small and medium-sized enterprises will achieve at least a basic digital intensity index¹.
- Europe will increase the number of its innovative scale-ups and improve their access to funding, leading to a doubling of the number of unicorns in Europe.

There is, of course, also a commitment with respect to the Public Administration

- 100% of key public services will be available online for European citizens and businesses.
- 100% of European citizens will have access to electronic health records.
- 80% of citizens will use a digital identity solution.

It's not possible to escape the highly challenging nature of these goals, and it is widely believed that they are unlikely to be achieved. The knowledge gap to catch up with respect to these issues is enormous: Europe realized in 2020 that a digital revolution that began in the 1980s is underway.

A digital revolution whose main ingredient is, unfortunately, the know-how.

And we say "unfortunately", only because that's something that cannot be bought but has to be acquired over the long term, with a lot of effort and by investing in training and research.

While the various issues related to digital technologies have always been the subject of the various EU-funded research programs, the perspective with which these programs were written was aimed at facilitating the adoption and use of these technologies, thus a "user" perspective of services.

Rather, with the European digital strategy, the emphasis is on the ability to "develop and deliver" services, a paradigm shift that can certainly be implemented if supported by the right investments, but certainly not within one or even two decades.

Critical issues in the EU approach

There are two major categories of technologies that distinguish the digital world: hardware and software. These two souls, which have characterized digital since its origins, complement each

¹ The Digital Intensity Index (DII) is a composite indicator derived from the Survey of ICT and E-Commerce Use in Business. With each of the 12 included variables having a score of 1 point, the DII distinguishes four levels of digital intensity for each enterprise: counting from 0 to 3 points implies a basic level of digital intensity, 4 to 6 - low, 7 to 9 - high, and 10 to 12 points - very high DII.



other; an efficient hardware or infrastructure loses all meaning when run by an inefficient operating system or software, and vice versa. A reading of the European strategy marks very clearly the accent put on making our continent assume some role in the context of hardware platforms and infrastructure, while neglecting the component that should manage these infrastructures: softwares. Until specific knowledge is developed in this context and EU-made software platforms are in place, Europe is unlikely to play a significant role in the context of digital transformation.

The regulations enacted and in the process of being enacted on the topic of digital, which are accompanying the digital strategy, are so many and so wide that is borderline unmanageable. Below are some comments on the topic that emerged during the discussion.

- The most obvious issue now is to figure out how to transition the regulatory effort into real innovation with the creation of a digital single market among EU member states. However, it seems clear that there is an underlying risk of a spillover of the opposite nature: an overly stringent regulatory framework blocks innovation and the economy. A sovereign policy seems therefore appropriate, yes, but not in absolute value: few but effective rules to serve as regulatory "nodes" in the "relationships" between data, technologies and data science and the digital market and services, for otherwise there is a risk of generating a strategy with limited degrees of freedom/development. The framework of the European legislature is consistent to the extent that the various regulations being enacted and introduced:
 - Can coexist without creating fragmentation at the Union level;
 - can be understood and effectively adopted by stakeholders, both European and non-European;
 - are quickly and progressively modifiable if inconsistencies emerge.
 - Excessive fragmentation of European regulation and an under-functioning package of rules can lead to the risk of uncertainty in the applicability of digital economy rules for both operators and users. This should be clarified in subsequent regulations or through guidelines issued by regulators.
 - Certainly, there is a lack of even internationally accepted regulatory approach and structure with systemic governance consistent with the purpose of use that can foster a global economy, but there is also a lack of governance of regulations with



European animus that can determine a different order of control so that the freedoms of the individual and their rights are never challenged.

- The European legislature is adopting regulations in several areas, according to a model based on risk management (e.g., AI regulation) and full accountability of private and public economic operators (e.g., GDPR accountability) established both in Europe and in third countries. As is well known, these are activities that involve numerous compliance tasks, from analyzing the risks associated with each business reality, to identifying and implementing technical and organizational measures (by design and by default), obtaining certifications, etc., activities that are very costly in terms of human and economic resources to be employed.

B. Digital Sovereignty

Executive summary

The idea of "digital sovereignty"

The expression “digital sovereignty” refers to the ability of a country, organization, or entity to exercise autonomous and independent control over its digital affairs, including digital data, infrastructure, technologies, and services. The goal of digital sovereignty is to ensure the ability of entities to independently take decisions and protect their interests in the digital environment, free from over-reliance on external actors.

Digital sovereignty implies several aspects:

- **Data Control:** Digital sovereignty requires that a country or organization have control over its data, including personal, corporate and government data. This means that data must be stored, processed, and controlled within national or corporate borders, ensuring data security and protection.
- **Digital infrastructure:** Digital sovereignty also involves access to and control of digital infrastructure, such as communication networks, data centers, and technology platforms. A



country or organization should be able to manage and control its own digital infrastructure, reducing dependence on external providers.

- Digital technologies and services: Digital sovereignty also involves the ability to develop and use digital technologies and digital services independently, without being overly dependent on foreign providers. This may include developing domestic technical skills, promoting domestic digital innovation, and adopting local digital solutions.

Digital sovereignty can be seen as a response to concerns about dependence on external actors, data security, privacy protection, and fair competition in the global digital marketplace. Many countries and organizations are seeking to promote their digital sovereignty through policies and strategies that foster digital autonomy and reduce dependence on external actors.

Digital sovereignty in the EU: critical sparks

While the expression digital sovereignty is rather fashionable, when referred to EU policies it sounds rather misleading.

In fact, EU policies aim to design a European model of digital society that can compare with the American and Chinese models.

The European digital society model relies on an approach designed to ensure a balance between digital innovation, the protection of citizens' rights and the promotion of the public interest. This model seeks to integrate the economic and technological aspects of digital transformation with social values, inclusion, human rights protection, personal data protection and cybersecurity.

A number of key principles characterize the European model of a digital society:

- Personal Data Protection: The European Union has adopted the General Data Protection Regulation (GDPR), which is one of the pillars of the model for a European digital society. The GDPR guarantees European citizens a high level of personal data protection and defines clear rules for the collection, processing, and storage of personal data.
- Fundamental Rights Respect: The European model of digital society is based on respect for fundamental rights, such as privacy, freedom of expression, non-discrimination, and



protection of intellectual property rights. It seeks to ensure that digital transformation does not undermine these rights but instead promotes and protects them.

- **Inclusion and accessibility:** The European model promotes digital inclusion and seeks to reduce the digital divide between different categories of citizens. It strives to ensure equitable and universal access to digital technologies, services, and digital opportunities for all citizens, regardless of their socio-economic background.
- **Cybersecurity:** European model of digital society places a strong emphasis on cybersecurity. Policies and standards are promoted to protect digital infrastructure, prevent cyber threats, and ensure data security. This includes the adoption of protective measures, international cooperation, and the development of cybersecurity expertise.
- **Sustainability and social responsibility:** The European model strives to promote sustainable digital innovation, taking into account environmental, social and economic aspects. It seeks to ensure that the digital society contributes to sustainability goals, promotes corporate social responsibility, and addresses environmental challenges through digital solutions.

These guiding principles of the European Digital Society Model reflect the European approach to digital transformation, which seeks to balance economic and technological aspects with social values, protection of rights and sustainability.

Digital sovereignty in other countries

There are some differences in the American model of the digital society compared to the European model. While both models aim to take advantage of the opportunities of digital transformation, some distinctive features are found in the American model:

- **Regulatory Approach:** In the U.S. model, the approach to regulation is generally more agile than in the European model. The United States tends to adopt a more free-market perspective, favoring minimal government interference in the digital sector. This has fostered a climate of innovation and rapid development of digital technologies in the United States.
- **Personal data protection:** Compared to the European model, the United States do not have a unified and comprehensive personal data protection law that can be compared to the



GDPR. In the United States, personal data protection is governed by several sectoral laws, such as the California Consumer Privacy Protection Act (CCPA) or the Health Insurance Portability and Accountability Act (HIPAA) for health data. This has led to greater regulatory fragmentation in the United States than the EU's harmonized approach.

- **Private sector initiative:** In the United States, the private sector, including Silicon Valley, has played a leading role in the development of the digital society. Many of the leading technology companies and digital platforms come from the United States, and the American model relies heavily on private sector innovation and entrepreneurship.
- **Focus on the digital economy:** The American model is often geared toward the digital economy, emphasizing the importance of innovation, competitiveness, and the creation of new economic opportunities through the digital sector. This has resulted in the rapid adoption of digital technologies and the expansion of technology companies.
- **Freedom of Expression:** The United States places paramount importance on freedom of expression, including in the digital realm. Protecting the right to free expression is seen as a central tenet of the American model of a digital society, often encouraging a less restrictive approach than some European regulations on online content moderation.

However, it is important to note that there are also areas of overlap between the two models, as both seek to promote digital innovation, equitable access to digital services, and address cybersecurity challenges. The main differences lie mainly in the regulatory approach and policy priorities in the area of digital transformation.

Chinese model of digital society presents significant differences from both the European and American models that also reflect marked political and cultural antinomies. While the European model emphasizes the protection of individual rights, privacy and the protection of personal data and the American model the free market, the Chinese model is based on a combination of state control, technological development, and mass surveillance. Here are some of the main differences:

- **State control and censorship:** The Chinese model is characterized by strong government control and supervision over digital activities. This is reflected in censorship and filtering of online content, which limits freedom of expression and access to information considered sensitive by the Chinese government.



- **Mass Surveillance:** China has implemented one of the most advanced mass surveillance systems in the world, with technologies such as facial recognition and massive collection of personal data. This has raised concerns about privacy and possible violation of human rights.
- **Control of technology platforms and enterprises:** The Chinese government plays a significant role in regulating and controlling the country's major technology enterprises, often requiring data sharing and adherence to government guidelines. This can affect competition and business freedom.
- **Data protection and privacy:** While the EU has adopted GDPR to protect the personal data of European citizens, China has data protection regulations that are more geared toward national security and government control. Individual privacy may be sacrificed to further the interests of the Chinese government.
- **Digital economy and innovation:** China made major advances in digital innovation, becoming a key player in the global digital economy. It has promoted the adoption of emerging technologies such as artificial intelligence and e-commerce on a large scale. However, its approach to competition and intellectual property may be different from the EU.

The adoption of a European regulatory framework for the digital society is an existential challenge for the European Union (EU). In lack of a unified approach, the digital transition could threaten the European single market both in traditional markets being transformed by digital innovation and in new digital markets.

If the EU won't act in a timely manner, member states could act individually, creating fragmentation in the single market and restoring regulatory barriers that were thought to be outdated. It is therefore essential for the EU to take the lead in ensuring a unified and consistent approach to regulating the digital society.

Digital sovereignty from a technological point of view

To also address the issue from a technological sovereignty perspective, the lack within the EU of a cutting-edge sector cannot be ignored. The EU's digital dependence concerns both hardware products (microprocessors, networking equipment, computers, etc.) and software products, such as browsers, search engines and operating systems, the majority if not all of which were developed outside the EU.



Wanting to be more concrete, a recent study commissioned by the Konrad Adenauer Stiftung (<https://digitaldependence.eu/en/>) showed to which extent European countries depend on foreign digital technologies through the so-called Digital Dependency Index (DDI).

The DDI systematically measures the degree and trends of national digital dependence that goes beyond particular sectors or certain technologies such as semiconductors. This index has values ranging from 0 (absolute independence) to 1 (maximum dependence), and the intermediate values of which are reported in the chart below. This study shows that the degree of digital dependence of most countries falls into the category of "high vulnerability."

European countries such as Italy (0.86), Germany (0.82), France (0.84), Estonia (0.8) and the United Kingdom (0.82) have remained very vulnerable over the past decade. China and the United States, meanwhile, are much less dependent on digital than other countries.

To achieve the ideal of digital "autonomy" that currently animates policy debates, EU countries would need to gain 10 percentage points on their DDI index over the next few years, something only China has succeeded in the past 10 years.

In other words, if Europe wanted to at least come close to an ideal of digital sovereignty, it should grow in the next 10 years as China did. Given the economic/financial trends of the two subjects over the past ten, it is believed that beyond good intentions and all efforts, digital sovereignty may not be the correct strategy for the EU to pursue.

Degrees of dependence	DDI value	The relation between domestic and foreign supply
Absolute independence	DDI = 0	Autarky.
Low sensitivity	$0 < \text{DDI} \leq 0,25$	Autonomy very high. Domestic digital technology is in a dominant position.
High sensitivity	$0,25 < \text{DDI} < 0,5$	Domestic supply delivers majority of digital tech. Considerable level of resilience.
Low vulnerability	$0,5 < \text{DDI} \leq 0,75$	Global markets supply majority of digital tech.
High vulnerability	$0,75 < \text{DDI} < 1$	Autonomy very low. Foreign digital technology is in a dominant position.
Absolute dependence	DDI = 1	Foreign digital technologies fully cover domestic demand.

© Center for Advanced Security, Strategic and Integration Studies (CASSIS), Rheinische Friedrich-Wilhelms-Universität Bonn

The Internet and information and communication technologies have the potential to bring to life a free, open, safe, and secure cyber space that can produce the greatest return in terms of positive



spillover effects on the entire planet if used to stimulate collaboration and cooperation across all entities that populate the network.

Working from a digital sovereignty perspective means giving up this potential and turning the global network into a web of closed networks that will communicate with each other only according to predefined agreements and protocols. Challenges exist that the network poses to us such as, for example, cybersecurity, which can only be solved through a joint effort and for which the digital sovereignty discourse is only deleterious. The hope, then, is that the EU will abandon this approach and become an advocate to other nations to promote the sharing of knowledge, values, and tools. An attitude that proved successful in overcoming the recent pandemic. This does not mean giving up one's dreams of independence but supporting them by promoting the development and adoption of products and solutions that can help improve the state of the global network, bringing to market products and solutions that help spread the principles of freedom, equality, dignity, and diversity of people in the network and that can counter the rise of a society of surveillance, control and social selection.

C. European strategy and challenging goals

Executive summary

European digital strategy challenges

The adoption of a European regulatory framework for the digital society is a major challenge for the European Union (EU), not least to counter some of the critical issues that have emerged during the transition.

The EU needs to consider several key aspects to address this challenge.

- First of all, appropriate skills are needed to manage digital transformation effectively. This requires significant investment in training and digital skills development for both citizens and businesses. In particular, it is important to spread a basic digital culture to ensure full and informed participation in the digital society.



- In addition, it is crucial to ensure adequate network service coverage in all areas, including rural areas, in order to avoid a "digital divide" and ensure that all citizens have equitable access to digital services and opportunities offered by the digital society. This requires significant investment in the digital infrastructure, such as broadband connectivity and the implementation of technologies such as 5G.
- Consistent and balanced regulation for the digital society is another critical element. The EU needs to develop a clear regulatory framework that promotes innovation, protects citizens' rights, and creates an environment of trust for business. This includes protecting personal data, cybersecurity, moderating online content, and promoting fair competition in the digital marketplace.
- It is also essential to adhere to the timelines of the National Recovery and Resilience Plans (NRPs), which are key tools for driving investment in digital transformation. The EU must ensure that funds under the NRPs are used effectively to support digitization and address identified challenges.
- As for public administration (PA), significant efforts are needed to ensure consistent interpretation of digital standards and to promote appropriate training for civil servants. In addition, it is important to develop specific digital skills within PA in order to facilitate the digital transformation of public services and improve efficiency and accessibility.
- However, there are also governance challenges to be addressed. There is a need to ensure adequate coordination among key players, both at the national and European level, to avoid fragmentation and duplication of efforts. In addition, it is important to promote interoperability between digital systems, both nationally and across borders, to ensure efficient communication and data exchange between different entities.
- Lastly, the fragmented cloud aspect poses a significant challenge. Common standards need to be promoted and interoperability among cloud services needs to be ensured in order to promote data portability and user choice. This will help avoid over-reliance on a limited number of providers and ensure greater security and autonomy in data management.



Conclusions

When the European "Digital Strategy" eventually becomes fully applicable, the question will be whether (and how) the new data protection framework will "withstand" the new pushes aimed at data sharing (including non-personal data).

While it is understood that the new set of European rules will have to be applied in parallel with EU Regulation 2016/679 and that the GDPR (one of whose peculiarities is that it is "technology neutral") may still be the reference text for data protection, it should also be taken into account that Article 97 gives the Commission the power to make appropriate proposals to amend the GDPR taking into account, in particular, developments in information technology and advances in the information society.

A further issue concerns the governance architecture of the existing Supervisory Authorities in order to avoid excessive fragmentation and overlaps with the new bodies introduced by the EU Digital Strategy: think, for example, of the "digital services coordinator" called to oversee compliance with the "Digital Service Act" or the European Digital Services Committee given that, for example, with reference to the subject of data protection, the individual Authorities already meet within the European Data Protection Committee.

Regarding the AI Act Supervisory Authority, the European Data Protection Board, and the European Data Protection Supervisor, in their joint opinion 5/2021, asked for more clarification on the governance. In addition, they reminded that data protection authorities are already applying GDPR, EUDPR and LED to artificial intelligence systems involving personal data, and therefore they should be reported as the National Supervisory Authority for the purpose of Article 59 of the AI Act.

Last but not least, an additional element cannot be ignored, consisting of the need to invest in raising the digital knowledge of citizens through adequate training on the proper use of digital platforms so that users become increasingly aware of their choices regarding data protection and contractual conditions of digital platforms with a view to privacy by design and by default.

The amendments made for the EU Parliament to the AI Act introduce the concept of AI literacy, i.e., the obligation on member states to promote literacy and education, and the teaching of basic notions and skills about AI systems and their operation.



Officine Dati



To summarize, the EU faces several challenges in creating its own regulatory framework for the digital society. It requires addressing issues related to skills, technology, regulation, public administration, and governance to ensure an effective, inclusive, and sustainable digital transition in the European single market.



Officine Dati



2. ROLES AND POWERS OF THE SUPERVISORY AUTHORITIES



The topic of the roles and powers of the Authority has been addressed based on the following aspects:

1. Independence of the Authorities
2. Plurality of Supervisory Authorities
3. Cooperation among Authorities
4. Sanctioning powers



A. Independence of Authorities

Executive Summary

The concept of "independence" of administrative authorities should be viewed in light of an experience that spans more than 30 years for authorities in general and 25 years for the Data Protection Authority throughout the European Union, including Italy.

While there is now a recognized need for reflection on this topic across the entire ecosystem of independent administrative authorities, the focus has been placed on the meaning of the concept with reference to the Data Protection Authority (in Italy, the Guarantor), in its present form and possible future developments.

The debate focuses on four interpretations of independence, considering it as:

1. The outcome of the selection criteria for the members of the Board and the Office.
2. Freedom from influence by other state functions and political power.
3. Organizational and financial autonomy.
4. Sectoral competence and norm-setting power.

Selection Criteria

1) Independence as the outcome of the selection criteria for the members of the Board and the Office

This interpretation of independence is significant from a national perspective. Indeed, Article 54 of the GDPR allows national states to define by law the qualifications and eligibility conditions required to be appointed as a member of the supervisory authority, as well as the establishment of relevant rules and procedures.

In Italy, the four members of the Board are elected by law by both branches of Parliament, following a consolidated practice that assigns two members to the majority and two to the opposition. On the other hand, the staff (Office) is composed of personnel who have won competitions directly at the Authority or at other administrations.



Article 153 of the Italian Personal Data Protection Code stipulates that Board members are elected from among those who submit their candidacy in a selection procedure, and that candidates can be appointed from individuals who ensure independence and proven experience in the field of personal data protection, particularly with reference to legal and computer disciplines. Just like for other independent authorities, nothing is specified about the process to follow for election. In practice, members are chosen after closed-door agreements between party secretaries and are voted on without debate on their profiles. After 25 years of the institution's life, reconsidering the concept of independence means asking whether it is time to make the selection of members of the independent authorities, and therefore also the Board of the Garante, more transparent, open to competition, and better defined in its investigative part.

Experts in the field should promote through all the intermediate bodies they belong to (parties, associations, committees, etc.) an integration of Article 153 of the Italian Personal Data Protection Code that imposes a more conscious and freer parliamentary choice.

As for the Office, the selection methods appear adequate to ensure independence.

Freedom from Influence

2) Freedom from conditioning from other state functions and political power

When the first independent authorities were established, subjection to the Legislative power was implicit (as long as it complied with European constraints, where applicable), while independence from the Executive could be guaranteed by unlinking the Authority's fate from that of the Executive and the supporting parliamentary majority, and more generally by giving it a predetermined duration and adequate financial coverage. This still appears important, although the considerable duration of the Garante's Board (7 years) could be reconsidered.

However, looking at Italy, the division of powers between the Executive and Legislative branches has become increasingly less clear over the past 25 years. We are experiencing a hypertrophy of the Executive: emergency decree-making has expanded excessively, and parliamentary initiative has been greatly reduced. Independence from the Executive power today may also mean the need for a new dialectic on legislative choices made substantially by the Government. There has been



discussion on the Garante's review of merit-based decisions made by the Legislature (increasingly often resulting from the initiative of the Executive).

The urgency to legislate can represent a situation where rights, freedoms, and the protection of personal data are objectively at risk. This was seen during the pandemic, with a sequence of regulatory acts that clearly affected aspects of personal data protection. It could be seen with the worsening and spreading of the conflict in Ukraine.

The supervisory authority neither can nor should review political choices; however, in the face of decisions that touch the essence of the relationship between citizens and the State, the Authority must not only play an advisory role to Parliament and the Government (letter c) of Article 57 of the GDPR) but also the **task of monitoring the application of the GDPR** (letter a) of Article 57 of the GDPR).

There is also questioning about the dual speed in the implementation of personal data protection legislation between the public and private sectors. There is unanimous appreciation for the depth with which the Garante has carried out investigations and proceedings in the public sector in specific areas of considerable importance. However, for the public sector (starting with the sectors of state administration), **in-depth investigations are hoped on organizational models and overall compliance choices, and an impetus for analysis and planning activities** (such as Impact Assessment) stemming from a risk-based approach.

Organizational and Financial Autonomy

3) Organizational and financial autonomy

The Italian experience on the front of the organizational and financial autonomy of the Data Protection Authority is a success story. However, there is **room for improvement on two fronts:**

- a) allocation of internal resources and compliance with procedural times;**
- b) service satisfaction.**

On point a), the Authority has regulated its operation in the Garante's Regulations but is unable to comply with the procedural times it has defined. This is likely due to a lack of human resources.



Transparency is desirable on the Authority's need for human resources, reporting on the criteria for the internal allocation of human resources, and the degree of compliance with procedural times (which is a qualifying element of the Guarantor's service levels).

On point b), it is believed that the Public Relations Office, especially as it is currently sized and functioning (even in opening hours), is not sufficient to bring the Authority closer to citizens. The first support to citizens and businesses should be considered as an essential public service. The Garante's autonomy would be strengthened if the RPO became a working counter, also through digital channels, in extended time slots, possibly introducing a ticketing system. Reflection should also be made on approaching communities of interest at the territorial level (for example, regional).

Sectoral Competence and Norm-setting Power

4) Sectoral competence and norm-setting power

The results of the Officine Dati questionnaire are a useful reference point. To the question of whether there is a risk of self-referentiality of the Authorities in this aspect, the majority of respondents (55%) argue that *"Yes, often the authorities base their decisions on their previous measures or guidelines that lack binding effectiveness for everyone."*

Authorities cannot be blamed for certain reverential fear of jurisprudence towards it. Nor can it be overlooked that the collapse and cost of the civil justice system further discourages challenges to Authority orders and the emergence of new legal interpretations. However, **a strengthening of the culture of advocacy is needed, both of Data Controllers, Data Processors and Data Subjects.**

A quixotic attitude toward data protection legislation harms the life of the law, creating a kind of perennial alternative between applying the Garante's guidelines or refraining from compliance. The industry professionals and scholars must **dare the interpretive challenge**. And work needs to be done on the mindset of Controllers and Processors and the judiciary to avoid interpretive flattening.

Anticipatory compliance

If traces can be found in the GDPR -as in the regulation of the principle of data protection by design- of so-called "anticipatory compliance," something similar could be hypothesized regarding the



authority's competence. By means of appropriate regulatory coverage, the procedural methods of independent supervisory authorities should be set up with possible future scenarios in mind, with greater recourse to ethical considerations and with greater attention to sustainability.

B. Plurality of Regulatory Authorities

Executive Summary

Over the past decade, we have witnessed a proliferation of independent authorities, also empowered with normative and executive powers, representing a new form of power in addition to the traditional three Montesquieuan sources. This proliferation process leads to a multiplicity of competencies and the decision on their allocation, often resulting in overlaps and the risk of conflicts. It highlights the need for a fast and appropriate process of integrating the activities of these authorities, capable of not penalizing the unity of overall decision-making processes in relation to advanced objectives and projects.

Proliferation of Authorities

With the enunciation of the Union's digital strategy and its first application phase, there is a proliferation of independent administrative authorities entrusted with supervising the individual topics of the specific EU regulation. The object of this regulation varies; it may consist of:

- **A good**, as in the case of the General Data Protection Regulation (GDPR).
- **A tool**, as with the proposed Regulation on artificial intelligence (AI Act).
- **A process**, as for the Regulation on data governance (DGA).
- **An impact**, as for the Digital Markets Act (DMA).

Generally, the prediction - hence, the establishment - of a specific supervisory authority "follows" the regulation and the scope of its application, resulting in an independent authority corresponding to each regulated phenomenon in the digital environment. This model inevitably triggers a process of **proliferation of authorities** and potential **overlapping of competencies**.



Additionally, EU law acknowledges the discretionary power of Member States to decide, for each of the reference application areas, whether to establish an ad-hoc authority or, alternatively, to merge the competencies provided by the regulation with those of an existing authority. This results in a **diversification of approaches** at the European level, with severe repercussions regarding the desired cooperation and synergy.

This trend - seemingly more due to a collateral effect than a strategic choice - risks nullifying the traditional effort of the European Union institutions towards greater harmonization at all levels.

The observation of the plurality of independent national regulatory authorities raises the question of the adequacy of this type of control framework concerning the governance of the phenomena these authorities are called upon to supervise.

Plurality of Competencies

The trend towards the proliferation of authorities accompanies the process of multiplying assigned competencies, **increasingly numerous and extensive, which often intersect and overlap**. This side also reveals emerging **risks of segmentation and jurisdictional conflicts** to the detriment of the unified governance of processes, such as those characterized by technological development and digital transformation.

Allocation of Competencies

The multiplication of competencies assigned to a plurality of authorities raises the issue of their distribution. The allocation of competencies must be clear - that is, easily recognizable - and specific, precisely identified, and corresponding to the purposes pursued by the authority's establishing regulation.

However, **the competency/authority duo**, if replicated numerous times, leads to a compartmentalization of expertise and a fragmentation of the overall decision-making process. These conditions, if consolidated, can slow down or even hinder **the goal-oriented approach** that is inherent in the business sector and broader economic development.



Integration Among Authorities

The aforementioned competency/authority duo also triggers a process of **verticalization of the intervention areas** of individual authorities, with the risk of segregating activities, if not even conflicts between them. This prompts a rethinking of the current model of articulating activities and tasks of authorities, promoting **new convergence models** aimed at **cooperation and efficiency** improvement.

Although the issue of cooperation among authorities is specifically addressed later, it seems appropriate to mention it also in discussions about the plurality of authorities.

In addition to the current **memorandum of understanding**, which do not seem to have produced significant results, a **Digital Services Conference** could be envisaged with a liaison body that envisions the establishment of a forum for constant comparison between the various authorities responsible for independent control of issues related to digital in a broad sense. A sort of "**integrated body**" - with fixed, unified, and recurring composition features - that performs a holistic, coordinated, and synergistic function, aimed at avoiding the aforementioned risks of duplications and/or fragmentations of functions attributed to different independent regulatory authorities.

A practical example in this direction concerns the construction of **cognitive cities** capable of using data to prioritize the needs of citizens and the surrounding environment, such as the NEOM project. To date, smart cities use only 1% of the data generated by residents. A cognitive city could exploit up to 90% of the data produced by the population. This would enhance citizen services, from access to education to improving digital health performance. The digital connection to the physical objects that make up our cities, allowing data calculation and analysis to contextualize needs more efficiently and facilitate decisions, cannot work without a **model of integrated cooperation among independent authorities**. Fundamentally, the rationale for this type of intervention would be to address issues such as resource dispersion, social disconnection, pollution, traffic, and the depletion of local and planetary resources.



Structural Asymmetries of Authorities

Undoubtedly, the mentioned proposals must take into account the structural asymmetries among the various authorities, determined by differences in available resources, attributed powers, and the same journey that these institutions have made over the years.

C. Cooperation Among Authorities

Executive summary

There is room for improvement in the cooperation among authorities related to the following scenarios:

- At **European level**, it is necessary to reduce procedural obstacles, created by the different legal traditions of Member States, through specific legislative projects.
- Similarly, at the **national level**, there is a need to prepare regulatory tools to make cooperation among authorities structural, defining, for example, joint cooperation structures (e.g., task forces).
- Finally, it is essential that Member States seize the opportunities offered by **new regulations in force** (e.g., Digital Services Act, Digital Markets Act) or those being drafted (e.g., Artificial Intelligence Act), identifying the correct placement of new competencies related to these regulatory acts.

Introduction

From the analysis of the responses to the questionnaire given to participants at the Global Data Conference, **collaboration among authorities is insufficient, but the number of currently existing authorities is considered adequate.**

Despite the efforts concerning cooperation among authorities, several aspects to improve have been identified. In general, the three possible cooperation scenarios can be qualified as follows:

1. Cooperation between independent national supervisory authorities from **different EU countries** responsible for supervising the **same area** (for example, concerning data



protection, collaboration between the French Data Protection Authority and the Italian Data Protection Authority).

2. Cooperation between independent national supervisory authorities responsible for **supervising different digital-related areas within the same EU country** (for example, a collaboration between the Italian Data Protection Authority and AGCM).
3. Cooperation between independent national supervisory authorities from **different EU countries** responsible for supervising **different digital-related areas** (for example, a collaboration between data protection authorities and telecommunications regulation and control authorities, such as a hypothetical collaboration between the French Data Protection Authority and AGCOM).

Cooperation Among EU Authorities Responsible for the Same Subject Matter

Cooperation between independent national control authorities from different EU countries responsible for supervising the same subject matter could refer to, in the context of data protection, collaboration between CNIL (French authority) and the Italian Data Protection Authority (Garante). Generally, cooperation between national independent authorities responsible for supervising the same subject **is structured, though improvable**.

From the perspective of the European Data Protection Board (EDPB), for instance, 639 final decisions (from 2018 to 31/12/2022) reached by consensus have been identified, of which only seven were subject to a binding decision by the EDPB, under Art. 65 of the GDPR. The types of cooperation identified can be summarized as follows:

- a) **Proactive cooperation**, aimed at preparing a joint and preventive interpretation on a specific agreed topic; in this sense, guidelines are the result of such cooperation.
- b) **Reactive cooperation**, aimed at resolving an issue that emerged concerning a specific case. For example, consider the activities carried out in connection with the EDPB's task force dedicated to complaints submitted by None Of Your Business (NOYB) regarding cookie management².

² Cfr. edpb.europa.eu, Report of the work undertaken by the Cookie Banner Taskforce, https://edpb.europa.eu/our-work-tools/our-documents/other/report-work-undertaken-cookie-banner-taskforce_en.



However, there are slowdowns concerning particularly complex issues, which do not reach a compromise quickly (e.g., data monetization). In this regard, cooperation could focus on priorities to support market companies affected by these slowdowns.

Additionally, there are **obstacles to cooperation**, particularly procedural within each Member State. These differences primarily stem from the different legal traditions of each Member State. These procedural differences have been acknowledged as a genuine barrier to the One Stop Shop mechanism promoted by the GDPR. Therefore, when managing a cross-border case, there are legal and operational barriers that create significant obstacles to cooperation. A possible solution to this inefficiency is the definition of legislative projects to improve cooperation. In this regard, the European Commission has included a project in its work program to eliminate (or at least reduce) legal and administrative obstacles in cross-border contexts³.

Cooperation Among National Authorities Responsible for Different Subjects but Within the Digital Sphere

Cooperation between independent national control authorities responsible for supervising different digital-related subject matters within the same European country could be a structured collaboration between the Italian Data Protection Authority and the AGCM.

There can already be cooperation between national control authorities responsible for supervising different subjects, but such **cooperation is not structured**.

In this context, we can mention the judgment of the **Council of State related to Facebook and AGCM**⁴ or, at the European level, the conclusions of the **Advocate General concerning a measure of the German competition authority against Meta**⁵. In these cases, there was an overlap between data protection and antitrust competencies, but without any communication between the relevant

³ Cfr. [europarl.europa.eu](https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-mff-mechanism-to-resolve-cross-border-obstacles), Legislative Train Schedule, Proposal for a Regulation on a Mechanism to resolve legal and administrative obstacles in a cross-border context, <https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-mff-mechanism-to-resolve-cross-border-obstacles>.

⁴ Cfr. Cons. Stato, Sezione VI, 29 marzo 2021 n. 2631, https://www.giustizia-amministrativa.it/portale/pages/istituzionale/visualizza/?nodeRef=&schema=cds&nrg=202001825&nomeFile=202102631_11.html&subDir=Provvedimenti.

⁵ Cfr. Advocate General Athanasios Rantos Conclusions, Causa C-252/21, <https://curia.europa.eu/juris/document/document.jsf?jsessionid=64A1E9F024B440B7EC7642BF7697B046?text=&docid=265901&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=209721>.



authorities. In this regard, even the Advocate General in stated that it would be necessary for the authorities to establish contact and consider their respective opinions. Examining the Italian case, there is no regulation requiring authorities to cooperate; therefore, collaborations are largely a voluntary act of the Authorities themselves, which define protocols for information sharing. In the absence of a regulating rule, there is a risk of conducting "photocopy" investigations, thus creating overlapping content.

It is desirable that **joint cooperation structures** be established at the regulatory level, to be initiated when it is necessary to deliberate on a specific case or to be started systematically and periodically.

Cooperation Among EU Authorities, Responsible for Different Subjects but Within the Digital Sphere

Cooperation between independent national control authorities from different EU countries responsible for supervising different digital-related subject matters could be a hypothetical collaboration between the French CNIL (privacy authority) and the Italian Authority for Communications Industries (AGCOM).

In this context, **there is not yet a defined level of cooperation**. Indeed, European Union law does not provide specific rules for cooperation between Authorities from different sectors.

Similar to what is indicated for cooperation between national authorities responsible for different subject matters, any cooperation to take into account their respective point of view is discretionary. Although recourse could now be made to the principle of loyal cooperation, greater enforcement is needed to systematize such collaborations.

It is hoped, therefore, that **rules will be adopted that determine functional cooperation structures**, operating preventively. These new rules would make cooperation a legal obligation. In this sense, some insights can be gleaned in the levels of cooperation defined in the Digital Services Act⁶, the

⁶ See 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), Chapter IV "Implementation, cooperation, sanctions and enforcement," <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065&from=IT#d1e4753-1-1>



Digital Markets Act⁷, as well as the proposals for a Regulation on Artificial Intelligence⁸ and a Data Act⁹. In this way, **it will be possible to structure functional forms of collaboration**.

D. Sanctioning Powers

Executive Summary

A sanctionatory system based solely on financial penalties, as provided by the GDPR, risks leading companies and organizations **to consider the sanction as a cost to be calculated in business activities** and could represent a disproportionate expense for SMEs, with **distorting effects on the market**, without ensuring effective protection of the rights and freedoms of the individuals involved.

The sanctions should not have a merely punitive function but should aim to **increase the level of accountability and encourage compliance** with the law. Consequently, the tools identified to pursue this purpose could be:

- internal regulation of supervisory authorities,
- modulation of penalties,
- transparency and allocation of revenues.

Internal Regulation of Supervisory Authorities

- **Better definition and transparency of internal sanctioning processes.** It is desirable to adopt new internal regulation tools for a more explicit assessment, verification, and contestation, to ensure:

⁷ See Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on fair and contestable markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), Articles 37-39, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925&from=IT#d1e3503-1-1>

⁸ See Proposal for a regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union, Title VI "Governance," Chapters 1 and 2, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=IT>

⁹ See Proposal for a regulation of the European Parliament and of the Council on harmonized rules for fair access to and use of data (Data Act), Chapter IX "Implementation and enforcement," <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0068&from=IT>



- respect for the right to defense (the Engel criteria, ref. European Court of Human Rights, Grande Stevens ruling),
 - effective protection of the individuals involved,
 - application of the law.
- **Certainty of timing.** It is desirable to adopt measures aimed at promoting greater transparency of the criteria followed by national authorities in managing administrative proceedings and greater certainty of the timing for concluding sanctioning proceedings.
- **EU harmonization of principles.** The regulation rules (criteria for determining sanctions, structure of inspection activity, identification of categories of subjects to undergo assessment, methods for initiating inspections, exercise of sanctioning power in general) should be placed in a context of harmonization at the EU level through verification by the European Data Protection Board.

Modulation of Sanctions

- **Use of alternative tools.** A different modulation of sanctions is desired. An action tool could be the creation of tables distinguishing the categories of violations, the range of sanctions, and the categories of subjects targeted by them. In particular, the position of SMEs should be subject to specific evaluation, to provide sanctioning criteria proportionate to the company's size. EDPB guidelines 04/2022 in the final version seem to go in this direction. The introduction of new tools could be evaluated, such as, following the model already adopted by antitrust authorities (Antitrust prov. 25/09/2018, res. SIAE), the imposition of symbolic sanctions to allow compliance tools to prevail over sanctioning ones, both towards private and public entities.
- **Increased use of warnings and requests for commitments.** A "phased" sanctioning approach is desirable, within which the financial penalty represents the last resort. Instead, an approach based on warnings is encouraged, which, following the finding of the violation, imposes commitments and plans for compliance, with strict feedback and enhancing the role of the DPO in these stages.
- **Promotion of accountability tools (Certifications and codes of conduct).** From this perspective, the promotion of accountability tools such as codes of conduct and



certifications could be valued, and the enhancement of the related monitoring and certification bodies to promote accountability further and prevent the need for a predominantly sanctioning system.

Guidance on the allocation of sanction revenues

- **Training for companies.** Finally, the importance of directing the revenues from sanctions towards the promotion of training platforms and interventions to help operators increase the level of awareness and compliance with the law is emphasized.
- **Raising awareness among those concerned.** The funds derived from sanctioning activities would find their natural destination in adopting awareness initiatives for those concerned, with the aim of promoting digital education and providing them with better tools for managing their personal data.



3. VULNERABLE SUBJECTS AND EFFECTIVENESS OF PROTECTIONS



The table discussed, first in specific 'vertical' subgroups and then in plenary session, the critical relationship between certain categories of data subjects considered particularly 'sensitive' and the common data processing activities that take place in today's digital society and, above all, on platforms.

After an analysis of the state of the art and a preliminary regulatory reconnaissance, as well as an obligatory attention to the pronouncements (and sanctions) of the Supervisory Authorities throughout Europe, the members of the subgroups began to list, and formalise, the main points of discussion, putting some possible 'solutions' alongside the 'problem'.



A. Some critical aspects in the relationship between data protection and user/consumer protection (and some regulatory suggestions)

Executive summary

The first discussion focused on the **protection** of the **data subject/user/consumer** in the electronic society, in e-commerce, on platforms and in the use of apps.

Many critical points were identified in this sensitive area, also drawing on the experience of consultants and DPOs of large companies, platforms and services.

A first point: the lack of 'compliance' incentives

In primis, the lack of incentives (in addition to Article 166, c. 7 of the Italian Privacy Code, D.L. 196/2003) was pointed out in the current framework, which could prompt a data controller to launch campaigns to make consumers aware of and responsible for data protection.

This would be an important step: it would make it possible to interpret enforcement and compliance not as an annoying burden but as a corporate 'value', a new and modern business opportunity, and a reputational value to be 'played' on the market.

The working group found critical precisely this widespread lack of the idea of quality in creating and managing a relationship with the stakeholder made up not only of answers but also of collateral activities to maintain a correct and, in some cases, even proactive relationship.

Last but not least, this first point reflected on the option of strengthening certain sustainability parameters by integrating them with the essential principles of personal data protection.

The proposal, in particular, is to include these principles in the **valuation parameters** to be taken into account by investors.

A second point: anticipating protection (and compliance...)

The discussion then shifted to the more specific point of the protection of vulnerable persons, envisaging two quite distinct needs.



The first is to **increase protection in advance**, working on the creation and application of **best practices, codes of conduct** (an example that was given concerned, for example, the well-known sectors of telemarketing and teleselling) and the provision of **incentives** for both companies and institutions.

The second is to guarantee at all times **better management** of the automated **exercise of rights** and greater clarity also on the part of the authorities on the essential elements to be implemented and guaranteed.

A third point: the definition of *ad hoc* communication standards

The last suggestion that came out of the discussion on this point is related to the possibility of **defining *ad hoc* communication standards** that are obviously designed for the benefit of those concerned.

In particular, the participants in the group saw a clear need for the development of more **transparent** and **easily accessible** communication standards, tailored to the platform and its importance, for consumer information.

At the same time, a stronger focus on **fairness and transparency requirements** appeared necessary in **explaining** the criteria for the operation of automated decision-making mechanisms and predictive analytics, and in how to **respond** to rights exercises, along the lines of what other supervisory authorities have envisaged.

The **platform** environment, clearly, was seen by all the participants at the table as **the most suitable** to make clear a now pressing need to strengthen **awareness** obligations towards the millions of users.

B. The world of healthcare: critical points on patient protection (and some proposals)

Executive summary

Once the very constructive discussion on the role of the platform user was over, it seemed natural to reason about the **data subject/patient**, i.e. a type of subject who finds himself in a **very**



vulnerable context: often ill or worried and in an environment that suggests him and where he feels weak.

The preliminary analysis started from a reflection on the **legislative framework**, and helped to immediately highlight a basic problem: the legislative framework, in the interpretation of the scholars in this group, is still very **consensus-centred** (i.e. with consensus being seen as a sort of **panacea**) and such an approach is even more evident, and 'exalted', in the field of medical research.

A first point of discussion: are we sure that consent is (still) the correct legal basis?

The debate was sparked during a common reflection on the fact that consent (as a legal basis), in reality and in many medical contexts, does not present itself as such a correct and 'ideal' legal basis, precisely because of the fact that the patient is in a position of **psychological weakness** and **vulnerability**.

How, for instance, can one identify the presence of a **fully free consent** in such traumatic situations?

A second discussion point: do we adopt a more modern vision?

Having highlighted the critical issues of consensus, the working group constructively reflected on three possible remedies that would ensure a more modern vision of this sphere.

The first is the abandonment of this consensus-centric cultural heritage that prevents the valorisation of other legal bases, or even the design of new ones, and which, in any case, should always be accompanied by an information system (transparency and usability) that truly enables a real understanding on the part of the patient of his or her future data processing (even by using infographics and legal design principles).

This openness to other legal bases must in no way be seen as a diminution of protection for the patient: the protection of the patient in fact does not pass through a favouring of one legal basis over others, but takes the form of greater awareness and understanding on the part of the patient as to how his or her data are processed, thus also enabling him or her to exercise his or her rights properly. In this respect, a strengthening of information should be promoted in the health sphere, also using innovative and more incisive tools such as (for example) the use of legal design.



The second brings with it a better theoretical elaboration of the idea of the '**consumer-patient**' or '**patient-consumer**' as the case may be. A rationale for the protection and safeguarding of the 'consumer-patient' has never been fully developed, nor has the provision of **associative and consumer protection** instruments that are not applied to the world of healthcare today but which would be perfect for protecting the patient as a consumer and user of services as well.

The third remedy requires an increase in **awareness and sensitivity** to data protection issues both on the side of the professional world and on the side of patients. One thinks of the recurrent **confusion** between 'informed consent' and 'privacy consent', or of the chronic lack of effective and well-structured **training plans** for all categories involved in data processing.

A third discussion point: can we really talk about privacy by design in healthcare?

Returning to the issue of skills and training, it became clear to the study and research team how essential it was to reflect on the aspect of skills and real awareness of the issue of data protection in healthcare, also referring to the principles of privacy by design and the idea that these concepts are, so to speak, 'embedded' in the system itself.

Two critical elements were shared among the participants.

The first highlights a very low level of knowledge/awareness on the part of the medical profession, healthcare management and decision-makers on data protection issues.

There is therefore an immediate need to raise the level of awareness and managerial competence on data protection issues also, for example, of individual doctors, who must be more forward-looking, especially with regard to digital technology and its use.

At the same time, a lack of awareness/knowledge among those producing technologies in the health sector was highlighted during the discussion.

There is a widespread growth of attention for digital but not, unfortunately, from the data protection point of view, with many native technologies in China and the United States with examples of privacy by design and by default not respected or, in any case, embracing conceptually different canons on data protection (think of a 'proprietary' view of data still widespread in many countries).



C. The centrality of the child in the information society (and its protection)

Executive summary

The child and his or her data are, for many interpreters, the future of e-commerce, social and platform activity and, therefore, data processing.

The age of first access to online services has dropped significantly, to almost 5/6 years today.

At the same time, the data of minors online is increasing significantly in both quantity and quality, with the possibility of profiling never having been so precise.

The protection of minors online represents one of the most topical challenges and needs in relation to many aspects.

Indeed, in the present technological set-up, along with the undeniable benefits, new modes of unlawful behaviour have also found fertile ground, from which minors need to be safeguarded.

Often, however, efforts in this regard tend to focus exclusively on technological resources, for the provision of stricter controls, and on legislative interventions, for the repression and punishment of certain conducts.

In reality, the aspect that should be focused on most is the educational and cultural one: that is, minors should be provided with the knowledge and tools they need to protect themselves in the virtual world as much as in the real one.

This digital education should not only concern the child, in order to make him or her more aware of the risks and advantages of the Internet, as well as of the rights that can be exercised with regard to data processing; on the contrary, it should concern the entire integrated educational system of stakeholders that contribute to the growth and development of the child itself and towards whom the youngest adopt imitative behaviour (parents, teachers, etc.).

Often, in fact, it is precisely adults who do not behave in a virtuous manner in the digital field, with the consequence of transmitting wrong patterns to those who learn and learn from such behaviour.



Therefore, the approach to be adopted on this point is extra-normative: the legislation on the subject, in fact, is extensive and well-structured; what is needed is to bring it to the attention of those to whom it is addressed and educate them on their rights and how to exercise them.

To this end, it could be particularly effective to use educational methods based on the strategy of 'nudging', i.e. gentle nudging: in this way, minors would not perceive the adoption of certain conducts (or cautions) as a compulsion from outside, but rather as a conscious choice, the result of awareness and voluntary adherence to specific patterns of behaviour.

Standards, extra-regulatory environment, information, political vision, incentives and a 'facelift' to Article 9 of the GDPR are the six critical elements that were raised during the meeting in the discussion among participants.

First point: are we sure about the effectiveness of the current legislation?

Is the legislation protecting minors, both with regard to data protection and with reference to, for example, cyberbullying, proving effective, or not? What should be done, concretely, to try to improve the situation and the 'digital' framework? Increase sanctions? Better describe the offences to be prohibited or punished?

Second point: what if the problems are meta-legal?

Perhaps the problem is not the legislation: what if the legislation is sufficient or even too detailed, but what is missing is extra-normative?

Shortcomings in psychological and pedagogical approaches can lead to harmful consequences for minors, as well as possible imitative behaviour (the minor 'imitates' the use of the parent's data and devices) up to a complete lack of direction towards the youngest on the responsible use of technologies and the protection of their data.

Third point: do minors know? Are they properly informed?

If we consider the legal framework sufficient, and well structured, how much of this content actually reaches minors and is understood by them? In the group's view, in many cases there is a lack of real information to minors, including on how to educate them about their rights and how to exercise them. Hence an unavoidable need to 'make culture'.



Fourth point: what about politics? Do we have an adequate and complete political 'vision'?

According to the working group, there are important gaps related to the lack of a systemic political vision on everything concerning the presence of children online and the processing of their data.

One thinks, for instance, of the debates on the age of access to platforms and various services and, above all, on its actual verification.

Fifth point: the need, also in this area, for incentives to understand the legal framework and data protection rules.

The group assessed the need for 'gentle nudges' that bring minors closer to both understanding the architecture behind the processing of their data and the protection of their data. Rewarding, positive and not prohibiting incentives.

Sixth point: what if we tweaked Article 9 of the GDPR?

Also discussed during the discussion was the possibility of a facelift to Article 9 of the GDPR to make it more up-to-date but, above all, to make clear the vulnerability of the child and, therefore, the need for greater protection. This would also help the person himself to perceive greater, and immediate, means of protection in the legal framework.

D. Worker protection in relation to data protection

Executive summary

The group's work concluded with an analysis of the delicate relationship between employer, **employee** and data protection regulations.

The method used was a point-by-point analysis of individual aspects to then draw conclusions also in the light of the current legal and regulatory framework.

The discussion covered, in particular, **eight points**.

First point: a special feature of this area, namely the combined protection



The protection for the weaker party exists and must exist, in this case, in the combination of data protection legislation, regulations of the Workers' Statute, civil code regulations, software ergonomics regulations and anti-discrimination decrees.

Second point: translating work into data

Work and business are increasingly translated into data, and this brings with it the need to protect all that is contained within the more complex world of work itself.

Third point: the new dimensions of space and time

The who, what, where, when, space and time become the most important parameters for legal analysis. One thinks of the centrality of the problem of duration of performance in the digital society.

Fourth point: the (new) value of information

The group highlighted a fundamental, and central, value problem. We refer, as is clear, to the value of the information produced by work, which in so many cases now involves the value of work itself and presents the interpreter with new perspectives that are not easy to resolve (think of the concepts of supply and demand in the digital society).

Fifth point: the delicate relationship between the worker and the tool he uses

A progressive impoverishment of the professionalism of the worker was noted during the proceedings, as well as very delicate aspects in the relationship between the worker and the tool he or she uses, to the point of posing the risk of this value being lost without, at the same time, any protection for the worker himself or herself.

In the digital society, the concept of dignity should be revised or its content expanded.

Seventh point: setting limits to automation?

During the discussion there was a lack of limits in establishing what can be automated and, above all, what can be introduced to avoid the impoverishment of professionalism.

Eighth point: fluid fragility?



The concept of a 'fluid' worker fragility, similar to the phenomena seen in the digital society, was discussed in the group.

How can the current framework help?

At the end of the discussion, again on the subject of the worker in the digital society, some **further observations** and **examples** were brought up that helped to make the picture even clearer.

One thinks, inter alia, of the need to adapt the entire legal framework to the new (now) **data-driven** work, the need to rethink the **original function** of labour law and the **legal notion** of work as an instrument of social mobility on which our legal system is based.

Indeed, '**dataisation**', repeatedly mentioned in the discussion, has an impact on the market level because productivity (in the relationship with digital technology) changes (value problem), on the level of supply and demand and also in the relationship between worker/user and between worker and community.

The fear, as is clear, is that the digital transformation may entail the **progressive impoverishment** of the worker's professionalism, all the more so since, from a regulatory point of view, a fundamental profile is missing: to establish what can be **automated** ('automation') and what to introduce in order to avoid the paradox of the **impoverishment** of professionalism through the performance of the service ('augmented' technique choices).

In this framework, both the regulation on **artificial intelligence** (seen as a 'ceiling' and not a 'floor') and the previous legislation are not seen as measures capable of enhancing **inclusiveness** (whereas an interdisciplinary training plan, for example, could do much as an enabling measure to ensure the inclusiveness of workers and also of SMEs).



Officine Dati



4. DATA MONETIZATION



The panel discussed the European prospects for creating a single digital market and Europe's position in the global context regarding the valorization of personal data.



A. Data Valorization and Institutions

Executive Summary

The panel did not attempt to share scenarios and assessments regarding a topic that is constantly trying to find a delicate balance between underlying interests, both at the European and national levels.

The first topic concerns the need to increase awareness of data's value among stakeholders and organizations, which often are unaware of the value of data and how it can constitute a real asset. This assumption goes beyond the personal/non-personal data dichotomy, as the lack of awareness cuts across all fields.

A second aspect pivots around the concept of data valorization, which takes on a much broader meaning beyond mere monetization. Valorization aims to involve the data subject in the processing of their data, and in the case of personal data, it does not deprive them of their self-determination and control over their information assets. Involving the data subject also means making them perceive the effects and benefits of data sharing on the community and the economy.

In this context, the digitalization of electrical networks was cited as an example, which allowed the network's modernization by operators while enabling users to inject energy into the grid, encouraging energy savings and sustainable energy production. The positive effects on the community were the subject of specific informational campaigns by energy providers, leading many users to accept data sharing, producing positive effects on the energy system.

A final aspect the panel focused on is the question of whether there is a need to resort to legal bases other than the data subject's consent to adapt the specific context of data processing (e.g., the online context) to the needs of users. This would facilitate the development of the digital market in the European Union, benefiting European businesses and enabling them to compete with non-EU players, especially those from the United States.

The alternative, if a strict policy were to be pursued, especially in light of geopolitical turbulence, would be to assert digital sovereignty, as seen in other contexts, such as cybersecurity regulations for critical infrastructure. The balance between market forces and the uncompromising protection of the right to personal data protection, as highlighted in the jurisprudence of the Court of Justice



and supervisory authorities, appears precarious, and the Union will be forced to formalize a position while assessing its effects in various sectors.

Introduction

The panel coordinated by deputy Giulia Pastorella highlighted the contradictions that Europe faces regarding the valorization of personal data. During the discussion, the speakers examined the pressures on the European market, balancing the push toward data valorization and concerns related to unregulated market developments. They pointed out the risks of overregulation, which, while aiming to protect entrepreneurial freedom and competition among operators, may inhibit the growth and scalability of European players, potentially relegating Europe to a marginal position in the digital market. The discussion among the speakers also touched on competitive aspects and market construction that have led Europe to its current situation, potential challenges, and concerns regarding developments that may deviate from European principles due to market pressures. This led to considerations on finding a balance between market protection and individual protection, acknowledging that there is no one-size-fits-all solution in a fragmented and rapidly changing technological, market, social, and geopolitical environment.

Building the European Market

From the outset, it became evident that Europe's position regarding personal data protection and the current structure of the internal digital market are a result of the European Union's evolution as an international legal entity, influenced by various stages in the construction of the single market. European regulations were developed with the aim of protecting the Union's market while balancing the rights of small and medium-sized enterprises to conduct business, and the power of large companies to prevent potential market abuses, by imposing regulatory obligations in various sectors (consumer rights, product safety, data protection, and the environment). Big tech companies also had to justify their actions in the Antitrust field concerning other regulatory areas (such as consumer relations, unfair commercial practices, deceptive advertising, and data protection) that could impact the market due to their dominant position¹⁰.

¹⁰ Please see the pending case before the Court of Justice of the European Union: Case C-252/21 - Meta Platforms Inc., formerly Facebook Inc., Meta Platforms Ireland Limited, formerly Facebook Ireland Ltd., Facebook Deutschland GmbH



One uniquely European feature has been the focus on building a single market and considering the right to do business as secondary to other rights, despite legislation stating that rights must be balanced. The right to personal data protection, due to its cross-cutting nature, has been identified as a means through which the European Union can maintain market balance. However, this has made it difficult for European companies to scale within the digital market and compete with other global players. Compliance requirements under European regulations are manageable for large enterprises investing in Europe, but they represent a barrier for small and medium-sized European enterprises looking to allocate capital for business growth.

The years under the old data protection directives were characterized by fragmented regulations, along with stringent interpretations by the Court of Justice, focusing on individual rights, and supervisory authorities, focusing on data subjects. These factors created compliance costs that hindered the growth of European companies and left the digital market open to investments from large U.S. companies at a time when the digital market was developing. The entry into force of the European Regulation 2016/679, the GDPR, managed to standardize many aspects of the regulations and establish mechanisms for cooperation in enforcement. However, this uniformity arrived when the digital market was already dominated by other players, leaving the impression that the opportunity for personal data valorization and European market development was missed and difficult to recover.

The discussion then turned towards the valorization of non-personal data, questioning whether Europe will ensure a space for their valorization and free circulation to develop a market of domestic operators capable of scaling at the European and extra-European levels, or whether the focus will be on regulating what other jurisdictions are achieving by different standards. The Digital Governance Act (Reg. EU 2022/868) seems to move in this direction, prohibiting exclusive agreements on the use of public data and promoting reuse, sharing, and interconnection, as well as providing rules to support startups and small and medium-sized enterprises.

Moreover, the Data Governance Act suggests privileged ways to share and exploit data held by public authorities, including solutions like anonymization, pseudonymization, or processing in

v. Bundeskartellamt with the intervention of: Verbraucherzentrale Bundesverband It is possible to find more information about this case at the following link: [C-252/21 Case Details](#)



secure environments controlled by public bodies. While anonymization undergoes continuous monitoring due to the evolving reuse techniques, which may render the information in the data useless for the purpose requested by the data subject (for instance, in scientific research), other solutions may facilitate the development of a digital market within the scope of the regulation.

However, it was pointed out that new European regulatory proposals may hinder the free circulation of data. An example is the proposed changes to the Data Act, which, if adopted, would allow smart device manufacturers to deny users access to and sharing of data if the manufacturer demonstrates that such disclosure could cause economic harm. This limitation on data access and sharing was included following concerns expressed by stakeholders during consultations with the market held by the Commission in the regular legislative process, in relation to the possible circulation of industrial secrets.

Another factor that could impede the development of the digital market within the European Union is the ongoing expansion of categories of high-risk AI systems in the annex to the proposal for an Artificial Intelligence Regulation¹¹. Developing European players in cutting-edge areas such as Artificial Intelligence will require efforts from the Commission to provide viable solutions for European small and medium-sized enterprises investing in these systems. The combination of compliance obligations under various regulations, which have various impacts on the data market in a broad sense, may have implications for European companies in terms of the development and scalability of the internal market.

Worries

The panel is aware that the enthusiasm surrounding the predictions for the possible developments of the European digital single market is accompanied by concerns regarding what Shoshana Zuboff has defined as "surveillance capitalism"¹². The theme of mass surveillance, in fact, brings to mind the dramatic historical events that led to the founding of the European Union, which emerged from the ashes of the Second World War and from what was a real mass profiling based on membership

¹¹ Proposal for a regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union - COM/2021/206: [Link to the proposal](#).

¹² Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Luiss University Press, 2019."



in a particular religious confession, non-conforming sexual orientation, or health conditions, which resulted in the discrimination and persecution of millions of European individuals.

The consequences of the Holocaust were disastrous on all fronts, primarily the humanitarian one. Consequently, the fear that new technologies may carry the risk of dystopian and discriminatory developments is very much present in the minds of European legislators and jurists, just as the past of Europe has influenced the spirit of treaties and constitutional documents of the member states, becoming an inspiration for constitutions adopted subsequently in other parts of the world. The "school effect" of the constitutional documents born after the Second World War has led the European Union, in the context of its legislative activities, to assess the possible impacts on the rights and freedoms of individuals.

The geopolitical context has repeatedly prompted the Old Continent to question its founding principles and the pillars on which it has built its identity. Terrorism, in all its forms and patterns, has often made Europeans wonder about the legitimacy of emergency legislation and the extent to which an emergency can derogate from democratic freedoms¹³. Examples have been cited where, invoking declared emergency purposes, such as terrorism or the protection of public order, various municipalities have considered and adopted video surveillance solutions with facial recognition systems, materializing the risks of mass surveillance¹⁴. On this occasion, the Data Protection Authority intervened, reminding the administrations involved of the danger of mass profiling. Furthermore, the European Parliament adopted a moratorium on biometric facial recognition surveillance systems, which allowed stopping some requests for the adoption of such systems in European cities and even led to the exit of some facial recognition industry players from the European market, in safeguard of the fundamental rights of human beings, which are foundational reasons for the European Union.

Similarly, another emergency, the pandemic, required human rights activists and personal data protection institutions to demand guarantees for the rights and freedoms of individuals in the

¹³ Consider Rodotà's interventions on the topic of terrorism and emergency legislation: [Link to the document](#).

¹⁴ Sanction by the Italian Data Protection Authority (Garante) against Clearview AI: [Link to the document](#).



implementation of contact-tracing solutions to avoid monitoring the movements, contacts, and indiscriminate profiling of the health data of Italian and European citizens¹⁵.

The awareness of the complexity of the phenomenon has raised examples of positive discrimination that, however, are not without concerns about possible negative consequences. Reference is made to the social credit score systems announced by the Foundation for Sustainable Development, the Ministries of Ecological Transition and Infrastructure, the Municipality of Bologna, and Fidenza, projects that were halted following the announcement of the initiation of an inquiry by the Data Protection Authority¹⁶. The systems involved assigning scores and rewards to virtuous citizens through a social credit mechanism. Although the purpose was positive, linked to encouraging socially positive behaviors such as the use of public transportation or proper waste sorting, there were ¹⁷potential negative discriminatory outcomes, for example, for citizens who could not benefit from the advantages given by the scoring as they needed to use a car. Similarly, in France, there are pushes for companies to disclose their carbon footprint to promote environmental sustainability policies and achieve emission reduction targets set for 2040. However, the fear that the pursuit of these sustainability goals could later be extended to individual behaviors remains, even though it seems excluded as of today.

References to emergency situations are also found in the new regulatory packages. For example, the Data Act provides tools that allow public authorities to access data held by private entities in exceptional circumstances such as earthquakes and floods¹⁸. The scope of the provision also includes any personal data generated by the devices subject to regulation in the Data Act, which will be accessible by public authorities in exceptional circumstances, as long as guarantees for the data subjects are in place.

What has struck some interpreters in the reading of the regulation proposal is that the definition of exceptional circumstances has been left to the member states. However, the recent pandemic

¹⁵ It is possible to access the Italian Data Protection Authority's intervention on the proliferation of contact tracing apps at the following link: [Link to the document](#).

¹⁶ <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9778361>.

¹⁷ France clamps down on 'zero carbon' advertising to avoid greenwashing: <https://www.rfi.fr/en/france/20220416-france-clamps-down-on-zero-carbon-advertising-to-avoid-greenwashing>.

¹⁸ Regulation Proposal of the European Parliament and of the Council on Harmonized Rules for Fair Data Access and Utilization (Data Legislation) - COM(2022) 68 final. You can find the document at this link: [Regulation Proposal](#).



experience and the geopolitical tensions caused by ongoing conflicts, including those at the borders of the European Union, raise concerns that the definitions developed by the member states may go beyond the narrow scope of natural disasters. Consider the concerns raised by some policies adopted in Poland and Hungary, which have worried EU institutions, and how these definitions could shape the exceptional circumstances justifying the access power of public authorities to the data regulated by the Data Act and held by private entities.

B. Data Valuation from a Market Perspective

Executive Summary

Among the solutions identified by the panel of professionals, there is a strong need for cooperation not only among authorities but also with businesses and over-the-top companies to find a balance that protects the interests of individuals while also considering legal provisions and civil and consumer protection. Promoting dialogue between Italian authorities (Antitrust/Privacy Authority/AGCOM) and industries through regulatory sandboxes or sectoral working groups could be a turning point. Cooperation should ultimately aim to assist companies in approaching data valuation properly because the mere existence of a "valuation principle" is not sufficient. These considerations should take into account the context in which valuation would be applied and acknowledge that the legal basis of consent may not fully meet the requirements of Articles 6 and 7 of the GDPR. For some professionals, obtaining consent from a data controller runs the risk of often being interpreted as a "green light" to carry out more invasive activities. For others, consent is the only available legal basis but must be closely tied to transparency to make it clear and intuitive.

Introduction

The panel, coordinated by Dr. Layla Pavone, included professionals who have been dealing with data protection issues for years and analyzed the topic of data valuation based on their professional experience. Professionals introduced the theme starting from the concept of a digital civilization: consider the use of technology to build a true digital twin, such as the project initiated by the Municipality of Milan. The purpose of this data collection and processing project (non-personal data) is to provide the municipal administration with detailed information about the fabric of the city's territory to address the "modern" challenges of public space management. The Digital Twin



represents the first step in making Milan a smart city in every respect, thanks to a comprehensive overview of the existing data and insights that can be used to improve municipal management for the benefit of all citizens in terms of economic and social sustainability. The coordinator of the Board for Technological Innovation and Digital Transformation of the Municipality of Milan, Layla Pavone, indeed asserts that digital innovation and advanced technology can improve city governance.

This is a technological advancement with enormous potential for services offered to citizens, in terms of sustainability, efficiency, and safety. The discussion took into account the importance of open data and the role they could play at the institutional level, as well as the progress that could be achieved in urban planning, environmental, and mobility through efficient and secure data utilization. Data valuation is a challenge that does not concern only institutions, but requires the collaboration of all players, including citizens. Data valuation plays a central role in promoting new business opportunities in the corporate sector, without neglecting the importance of ethics, necessary to set limits and avoid social disparities, as well as optimizing the benefits of technology for society and the economy, in ways that strengthen the rights and freedoms of individuals.

Data Valuation and Business Opportunities

Data valuation has long been a challenging issue for businesses. On one hand, it allows users to access services they wouldn't have access to on their own, and on the other hand, it can be discouraging for small and medium-sized enterprises (SMEs) that lack the resources to invest in digital technologies and are unable to expand their business without access to data. SMEs often struggle due to a lack of training in the use of software and tools. In this scenario, culture, strategic approach, and digital skills play a central role in the effectiveness of digital transformation. Many companies aim to promote digital solutions that allow B2B customers to handle personal data digitally while focusing on transparency to remain competitive in the market and enable users to make informed choices. In recent years, many companies have invested heavily in the principle of transparency by creating more user-friendly information from a legal design perspective.

One aspect the professionals have focused on is the legality of data valuation, an issue that does not have a unified vision to date. In many cases, using legal bases other than consent, such as a contract or legitimate interest, is not feasible. However, according to the professionals at the table, strategies could be devised to allow users to make informed choices, for example, to decide whether



to use a subscription with a lower cost compared to the premium subscription without profiled advertising (compensation that takes into account the economic loss).

When it comes to balancing data protection and economic freedom, the stakes become much higher when considering the industry. There is also an issue of information pluralism: a publication that cannot "monetize" data does not survive and is more susceptible to influence¹⁹. According to the professionals, over-protection limits businesses, on one hand by destroying the business, and on the other hand, limits user freedom. In the view of the working group participants, there is a need to promote, from a scientific standpoint, data valuation business models that allow for a concrete assessment of risks to data subjects to adopt appropriate technical and organizational security measures to guarantee an adequate level of security based on the risk. In terms of security measures, anonymization techniques were also discussed. However, it is well known that anonymization constitutes subsequent processing of personal data and, therefore, like any processing, it needs to be regulated, both technically, in line with the requirements²⁰, and in compliance with data protection provisions (e.g., the data controller will need to identify the appropriate legal basis and provide evidence to data subjects, in line with the transparency principle).

According to the professionals, there should be greater awareness among institutions and all stakeholders of the historical responsibility regarding the creation of a digital development model to propose, allowing for the strategic survival of sectors that also represent bulwarks of constitutional freedoms (e.g., journalism). In fact, as mentioned earlier, in the case of newspapers, in addition to the balance between data protection rights and economic freedoms, there is also a broader issue related to the industry.

Data Valuation and the GDPR

The reflections related to the actual possibility of data valuation led professionals to briefly discuss the comprehensiveness and complexity of the GDPR. According to some professionals, the GDPR is not entirely sufficient but provides a solid foundation to find solutions that respect fundamental principles, including security. According to others, an intellectual evolution is needed to find

¹⁹ Cookie wall: *all'esame del Garante privacy le iniziative degli editori [doc. web. 815415]*.

²⁰ Working Party articles 29 "Parere 05/2014 sulle tecniche di anonimizzazione".



solutions that can meet market needs. The transparency innovation strategy is certainly a pillar that must accompany digitization, making users aware of how their information is used to dispel the fear of non-compliant use of their personal data. In this scenario, it must also be taken into account that the regulatory framework needs to be extended, also thanks to the e-privacy Regulation that will govern these aspects.

According to the professionals, the valuation of personal data is a concept experienced differently by some European states compared to our national legal system. In fact, many European players have always carried out valuation while considering the user's awareness of the choices made. According to the professionals, the mistake might be considering users in Italy incapable of understanding and, therefore, needing protection *a priori*.

In Italy, the first cookie guidelines in 2014 created a high level of protection²¹. Europe has created different ones.

The GDPR is not interpreted uniformly by all Data Protection Authorities. Some authorities have a more restrictive orientation, and therefore, the view of valuation/monetization is different within Europe. The need represented by the professionals at the table, is to reach a uniform approach at the European level, regarding data valuation to avoid forum shopping and competitive disadvantages. Interpretive inconsistency is already visible with the Meta case. The Irish Data Protection Commissioner had to adapt to the conclusions of the European Data Protection Board (EDPB), which disagree with, instructing Meta to pay 390 million euros for violating European privacy rules.

In relation to this provision, the European Data Protection Board did not consider the contractual legal basis applicable. In fact, according to the Committee, it would not be suitable for this purpose for various reasons, ranging from the lack of transparency with which Meta represented this fact to the data subjects, to the dubious validity of a contract entered into at least in the presence of significant information asymmetry between the parties, to the fact that most users of Facebook and Instagram have never even realized that they have entered into a contract with Meta. But above all, the contractual basis in this case is not applicable because the processing in question does not

²¹ Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014



actually appear necessary to execute the contract that binds Meta to its users, as the contract can be executed regardless of profiling for targeted advertising and, in fact, Meta has never assumed any specific obligation to provide users with such advertising²²."

C. Data Valorization from the Jurists' Perspective

Executive Summary

The panel concluded the discussion with the sharing of some key points and operational proposals, starting with the premise of maintaining a distinction between valorization and monetization, and considering the exclusion of monetizing rights as a fundamental point. More specifically, proposals were put forward to resolve or at least alleviate the issue of informational asymmetry among the involved parties. In this regard, it was suggested to incorporate information about the processing of personal data within the contract, emphasizing details to make the data subject/consumer/user aware of aspects related to the handling of their personal data. Another proposed solution was to encourage the use of hyper-simplified disclosures. Regarding the second topic discussed, namely, identifying the legal foundations for data circulation in the context of valorization. It was agreed that the GDPR already provides legal bases that can be considered in the context of data valorization. A model was proposed that takes the legal bases of the GDPR as a starting point in relation to various vertical business models. Finally, the discussion returned to the need for a balance between the right to personal data protection and other rights.

Introduction

The panel, coordinated by Lawyer Panetta, saw the participation of important professionals, who deliberated on the issues of data valorization and monetization to identify potential solutions and provide legal answers to what appears to be a growing practice. Specifically, the panel's discussion focused around three main areas: a) informational asymmetry between parties in the construction of contractual relationships underlying the provision of digital services, and possible tools to reduce this asymmetry; b) the economic valorization of personal data, and the legal bases on which it can

²² Pubblicità online, Scorza: "Ecco i tre scenari dopo la maxi multa a Meta" - Intervento di Guido Scorza <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9844860>.



be grounded; c) the limits of the contractual autonomy of parties in building relationships based on the provision of services in exchange for personal data.

The discussion began by considering the role of the jurist, who must take into account the evolving nature of society. It was immediately recognized that creating awareness among data subjects/users/consumers is necessary, and it was highlighted that three values—economic, social, and personalistic—should be considered to guide the regulatory framework.

Transparency and Information Asymmetry

The first significant issue discussed was the informational asymmetry between parties in the construction of contractual relationships underlying the provision of digital services. On one side, service providers have a comprehensive view of the processing of personal data, while on the other, data subjects, users, or consumers are often not placed in a position to fully understand how their personal data will be utilized. The issue of transparency needs to be correctly framed, and evaluations should be made regarding the means of conveying information. Questions were raised about the role of information notices on personal data processing, with many pointing out their inadequacy in effectively reducing informational asymmetry. Some judgments have already highlighted the need to provide additional information beyond what is included in the privacy notice, although the specific details were not mentioned²³. In some sectors, such as banking, the

²³ See also the "Telepass" judgment (Lazio Regional Administrative Court, judgment no. 603/2023). In this case, the Lazio Regional Administrative Court highlighted that, in the context of the placement of insurance services on behalf of partner companies, they received, without consumers being adequately informed, flows of information regarding the user's data requesting a quote. This conduct was followed by a process of sharing such information among Telepass group companies and insurance companies or insurance intermediaries, without potential policyholders being adequately informed about the collection and how their data were used for commercial purposes by the companies involved. Furthermore, it was found that Telepass, Telepass Broker, and partner insurance companies shared a dedicated database for the management and acquisition of insurance data, different from the platform through which the petitioner manages user data and owners of specific devices for highway payment services. A completely separate and autonomous database in which all customer information that had taken out insurance policies or saved a quote was shared and stored, once again without any information to consumers about the use of their data for commercial purposes. The consumer, if reassured by information related to the specific area concerning the confidentiality of personal data, was, on the other hand, entirely unaware of the methods of management, storage, and use of their data for the aforementioned commercial purposes. Claims on the website or in the procedure activated with the APP did not in any way reveal the further use of the data, which would have been included in shared databases with partners for the purpose of commercial services related to insurance services.



issue has been addressed, and regulations on information have been introduced to rebalance the disadvantage. Achieving balance requires a fundamental role for transparency in information.²⁴

The role of various authorities (the Data Protection Authority and AGCM) is also essential because issues related to transparency cut across data protection, consumer protection, and antitrust and may fall within the intersection of multiple authorities (for example, the abusive use of large databases may lead to an abuse of dominant position).²⁵ Another aspect that emerged in the discussion is that informational asymmetry is also present in the placement of information. The idea that emerged from the discussion is that one possible solution is to include information directly in the contract, alerting to possible risks (e.g., for profiling) and highlighting specific information in bold to mitigate the asymmetry. This does not mean imposing prohibitions but rather subjecting certain elements to greater attention, similar to what is already done for unfair terms. Another potential solution to help data subjects/users/consumers understand the received information could be to provide hyper-simplified disclosures.

Economic Valorization of Personal Data and Legal Bases

The second theme discussed in the panel was the presence or absence of suitable legal structures in positive law to guide the change. It was noted that the GDPR already provides legal bases that can serve as a reference point. In the past, there have been measures by the Data Protection Authority that had aspects related to data valorization. For instance, in the decision on loyalty cards (Fidelity Cards), the Data Protection Authority determined that personal data of data subjects could be used for three purposes: 1) collecting points to earn rewards, which falls under "loyalty" in the strict sense and uses the legal basis of the contract; 2) direct marketing; and 3) profiling.²⁶ For these

²⁴ On this point, it's also worth noting the attention given by the European legislator to the theme of transparency in a broad sense, as exemplified in Article 24 of the Digital Services Act, Transparency of online advertising. This article provides that online platforms that display advertisements on their online interfaces ensure that service recipients can clearly and unambiguously identify, in real time, for each individual advertisement shown to each individual recipient: a) the advertising nature of the displayed information; b) the natural or legal person on whose behalf the advertising is displayed; c) relevant information.

This provision emphasizes the need for clear and real-time transparency in online advertising, ensuring that users are informed about the advertising nature of the content they encounter and who is behind it. This aligns with the broader discussions on transparency and data privacy in the context of digital services and advertising.

²⁵ In the United States, for example, the Federal Trade Commission (FTC) is responsible for data protection, among other things.

²⁶ "Fidelity card" e garanzie per i consumatori. Le regole del Garante per i programmi di fidelizzazione - 24 febbraio 2005.



latter two purposes, the legal basis was identified as consent. This led to further reflections on the limits of using these legal bases. It was emphasized that data valorization results from choices made by the data controller and should remain a core aspect of personal data protection, referring to the legal basis of consent. However, the use of aggressive or unfair practices is considered unacceptable. Therefore, returning to the core issue and considering it as an evolving problem, it was highlighted that the economic valorization of personal data from a legal perspective can follow several paths: 1) consent; 2) slightly "encouraged" consent to allow data use as an alternative to payment (e.g., the "paywall" for which an investigation is underway by the Data Protection Authority concerning certain online news outlets);²⁷ 3) legitimate interest, which does not require a prior manifestation of will. The use of this legal basis can provide a gateway for balancing the right to personal data protection and other interests, and it can be seen as a basis for sustainability and "recycling" of data. However, conditions must be set for its use; 4) contractualization. This goes beyond using data for the strict necessity of the service and can involve two scenarios: a) an obligation on the part of the data controller, who commits to doing something with the data (e.g., a personal shopper asked to understand a customer's preferences); b) the possibility for the data subject to provide a license for the use of their personal data. The latter solution is closer to strict monetization and is also the riskiest.

All the possibilities mentioned above pose a risk to the right to personal data protection. Therefore, an absolute availability is not suggested but rather a form of "accordion of relative unavailability" that needs to be balanced. Heavier or lighter restrictions should be imposed depending on the case. There is a feeling that there are various vertical business models within data valorization (in relation to the chosen legal basis) that should be examined separately, identifying risks and opportunities to determine an acceptable risk for each model. Moreover, we should not abandon a case-by-case approach alongside the model-by-model approach. It emerged from the discussion that the model that refers to the valorization of personal data through the use of different legal bases, as described above, may be complex and suitable for large players but not for smaller ones. A proposed solution to make the model a reference point for all entities is to introduce standard templates (similar to

²⁷ See press releases from the Italian Data Protection Authority on October 18, 2022, October 21, 2022, and November 12, 2022.



the SCCs) in which, for certain scenarios of legal bases related to vertical models (among those listed above), guidance is provided for smaller players.

The standardization should present immutable minimum scenarios but remain open to variations that deviate from the standard while respecting the principle of accountability. However, this open-to-variations solution may not achieve the effectiveness of Standard Contractual Clauses (SCCs), which derive their strength from being unmodifiable. Another critical aspect was found in the use of legitimate interest and determining the threshold at which the balance can be considered adequate.²⁸ In any case, the proposed solution is concrete and builds upon tools already available in our legal system.

The limit of the contractual autonomy of the parties in establishing a relationship for the provision of services in exchange for personal data

With respect to the latter issue, it's important to consider the legal tools already available, some of which are effective and some that are not. It is considered advisable to maintain a distinction between two categories: monetization (where the data subject provides data in exchange for payment) and data valorization (which is already happening). Monetization and valorization should, therefore, be kept separate.

Furthermore, a consensus among all panel participants was the exclusion of monetizing rights. A possible parallel was drawn with Article 97 of the Copyright Act concerning the exploitation of the right to one's image. In this case, the right remains with the individual while the image is used.

Regarding the limits on the reuse of personal data, it was discussed that such reuse should not be prevented when it protects higher interests, such as public or collective interests.

On this point, the panel participants agreed that there should be positive legal norms that set limits. They also emphasized that the right to personal data protection is a fundamental right, as established in Article 8 of the Charter of Fundamental Rights of the European Union, and that the key to data valorization is balance. Data undeniably holds economic value. However, there is

²⁸ e.g. the VoetbalTV case in which the Dutch Data Protection Authority stated that the pursuit of profit cannot be considered a legitimate interest. This position was criticized by the European Commission.



currently no positive legal norm that places data as an equivalent.²⁹ Therefore, it is essential to both give individuals control over their personal data and restrict its circulation. A balance must be found between these two needs, as the risk of imposing very high "barricades" is that they may not be respected.

²⁹ In the debate, consideration was also given to Article 135-octies, paragraph 4, of the Consumer Code, which states: the provisions of this chapter shall also apply in the event that the professional provides or undertakes to provide digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the professional, unless the personal data provided by the consumer are processed exclusively by the professional for the purpose of providing digital content or a digital service, in accordance with this chapter or to enable the professional to fulfill its legal obligations, and the professional does not process such data for purposes other than those provided.



PARTICIPANTS

Roundtable 1 – European Digital Strategy

TAVOLO 1	Strategia Digitale dell'UE
<u>Coordinatore: Perri - Conduttori: Bruschi, Diomede, Orofino</u>	
Claudio Ardagna	Professore di Informatica UNIMI – Direttore Laboratorio CINI Big Data
Simone Bonavita	Head of IT Law - Perani Pozzi Associati - EXC Director at ISLC - UNIMI
Danilo Bruschi	Professore di Informatica UNIMI - Direttore Laboratorio di Sicurezza e Reti
Diego Dimalta	Co-fondatore Privacy Network
Nicla Ivana Diomede	Direttore del Dipartimento di Cybersecurity e Sicurezza di Roma Capitale
Giulia Escurole	Avvocato – DPO - Dottore di Ricerca – Research Fellow ISLC
Simona Klimbacher	Avvocato - General Counsel BSVA - Studio Legale Associato - Research Fellow ISLC
Paulina Kowalicka	Assegnista di ricerca in Informatica Giuridica UNIMI - Research Fellow ISLC
Gianluigi Marino	Partner, Head of Digitalisation Osborne Clarke Italia
Francesco P. Micozzi	Professore di Informatica Giuridica UNIPG - Leader Modulo Jean Monnet CIBER (2020-2023)
Juri Monducci	Partner Fondatore MPSSLAW Monducci Spedicato e Associati - DPO
Mattia Monga	Professore di Informatica UNIMI
Marco Orofino	Professore di Diritto Costituzionale – Dip. Studi Internazionali, Giuridici, Storici e Politici UNIMI
Pierangela Samarati	Professoressa di Informatica UNIMI - Direttore Laboratorio Sicurezza e Protezione Dati
Onofrio Signorile	Capo Ufficio Tecnologie e Innovazione - Direzione Regionale Piemonte Agenzia delle Entrate



TAVOLO 1	Strategia Digitale dell'UE
Federico Marengo	Senior Consultant White Label Consultancy
Stefano Petrussi	Partner Floreani Studio Legale Associato
Tommaso Stranieri	Partner Risk Advisory Corporate, Public & Private Market Leader Deloitte
Stefano Zanero	Professore di Cybersecurity POLIMI - President & Founder Secure Network
Alessandro Trivilini	Head of SUPSI Digital Forensics Lab



Roundtable 2 – Roles and powers of the Supervisory Authorities

TAVOLO 2	Ruolo e poteri delle Autorità di controllo
<u>Coordinatore: Imperiali - Conduttori: Faggioli, Fulco, Rigoni, Vintiadis</u>	
Antonio Bianchi	Docente universitario diritto delle imprese – Università Suor Orsola Benincasa
Cristina Cabella	Head Data Protection Compliance & Group DPO UniCredit
Carlo Rossi Chauvenet	Managing Partner CRCLEX - Professore Aggiunto di Privacy & Protezione Dati UniBocconi
Nicola Fabiano	Founder Studio Legale Fabiano - Prof. a c. UniOstrava - Già Presidente Garante privacy San Marino
Gabriele Faggioli	CEO P4I & Co-CEO Gruppo Digital360 - Presidente CLUSIT - Professore a contratto UniPavia
Umberto Fantigrossi	Avvocato Studio Legale Fantigrossi
Carolina Foglia	Head of Activity for Legal Coordination EDPB Secretariat
Carmelo Fontana	Senior Regional Counsel Google - Docente & MCE Digital Economy, Legal e Tax SDA Bocconi
Diego Fulco	Partner netforLegal - Professore a contratto IULM
Giovanni B. Gallus	Partner Array Law - Membro Commissione Surveillance CCBE - Fellow Nexa Center for Internet & Society
Corrado Giustozzi	Partner Fondatore Rexilience - Professore Aggiunto in Security presso LUISS
Giovanni Guerra	Founder Studio Legale Avvocati Guerra Ricchiuto
Laura Liguori	Partner Portolano Cavallo
Cristiana Luciani	Funzionario Autorità Garante per la Protezione dei Dati Personali
Andrea Monti	Founder Studio Legale Monti - Professore a contratto Università degli Studi di Chieti
Enrico Pelino	Partner Grieco Pelino Avvocati
Andrea Rigoni	Government and Public Services Global Cyber Leader Deloitte



TAVOLO 2	Ruolo e poteri delle Autorità di controllo
Fabrizio Vigo	Co-Founder e CEO presso SevenData
Marianna Vintiadis	CEO di 36Brains



Roundtable 3 – Vulnerables subjects and effectiveness of protections

TAVOLO 3	Soggetti vulnerabili ed effettività delle tutele
<u>Coordinatore: Ziccardi - Conduttori: Egitto, Sala, Stefanelli</u>	
Sergio Aracu	Partner Fondatore Area Legale
Marcello Bergonzi Perrone	Avvocato Studio Legale Bergonzi Perrone
Rossella Cerchia	Professore di Diritto Privato Comparato UNIMI - Of Counsel DLA Piper
Chiara Ciccia Romito	Avvocato e PhD Candidate LSI, Fondazione Marco Biagi
Luca Egitto	Partner IP & Technology RP Legal&Tax Studio Associato - Research Fellow ISLC
Riccardo Giannetti	Presidente Inveo Group - Docente di corsi Auditor EPE e Maestro Privacy - DPO
Silvia Gorlani	DPO Mediamarket
Matteo Giacomo Jori	Avvocato - Professore a contratto di Legge IT e Informatica Giuridica UNIMI
Licia Liguori	Senior Legal Counsel UK&I and Data Privacy Specialist Avanade
Francesca Marinelli	Professoressa Diritto del Lavoro UNIMI
Giulio Messori	Managing Director - Sweet Legal Tech
Andrea Michinelli	Avvocato Studio Legale d'Ammassa & Partners - Of Counsel 42 Law Firm
Massimiliano Nicotra	Senior Partner QUBIT Law Firm - Digital Lawyer - Co-Founder Legal Hacker Roma
Giulia Pesci	Assegnista di ricerca in Informatica Giuridica UNIMI - Research Fellow ISLC
Fabio Rastrelli	Avvocato - Intesa San Paolo
Gianluigi Maria Riva	Avvocato, Data Protection Specialist - PhD in Privacy, Etica e Nuove Tecnologie UC Dublin
Marianna Sala	Avvocato fondatore Studio Legale Sala - Presidente Corecom Lombardia
Alessandra Salluce	Avvocato specializzato in protezione dei dati personali - DPO - Research Fellow ISLC



TAVOLO 3	Soggetti vulnerabili ed effettività delle tutele
Andrea Stanchi	Managing Partner Stanchi Studio Legale - Avvocato di diritto del lavoro
Samanta Stanco	Avvocato, Assegnista di ricerca in Informatica Giuridica UNIMI - Research Fellow ISLC
Silvia Stefanelli	Senior Partner Studio Legale Stefanelli&Stefanelli - Docente



Roundtable 4 – Data Monetization

TAVOLO 4	Monetizzazione del dato
<u>Coordinatore: Cataleta - Conduttori: Panetta, Pastorella, Pavone</u>	
Ernesto Belisario	Senior Partner E-Lex Studio Legale
Rebecca B. Aspetti	Research Officer European Centre on Privacy & Cybersecurity Maastricht University
Luca Bolognini	Partner Fondatore ICTLC - Presidente Istituto Italiano Privacy e Valorizzazione dei Dati
Vincenzo Colarocco	Capo Dipartimento Compliance, Media e Tecnologia, e Capo Dipartimento Diritto della Proprietà Intellettuale, Diritto di Internet e concorrenza sleale - Studio Previti
Fernanda Faini	Research Fellow e Professoressa a.c. UniPisa e UniCatt – Funzionario legislativo-legale Regione Toscana
Ada Fiaschi	General Counsel & Compliance ITA Airways
Camilla Giannecchini	Senior Legal Counsel TikTok
Arianna Greco	Senior Vice President Head Global Commercial Legal Alnylam Pharmaceuticals
Anna Paola Lenzi	Group DPO & Head Compliance TeamSystem
Melissa Marchese	Counsel Gianni & Origoni
Gianluca Marmorato	Avvocato Studio Legale Boglione
Massimiliano Masnada	Partner Hogan Lovells
Luigi Neirotti	Avvocato e DPO, Senior Legal Counsel, IT Law & Data Protection Law Leader, EYLaw
Giangiacomo Olivi	Partner presso Dentons – Europe Co-Head IP, Data and Technology
Valentina Pagnanelli	Avvocato, Privacy Officer e Consulente Privacy - Docente Diritto informatico - PhD candidate - Università di Firenze
Rocco Panetta	Founder & Managing Partner Panetta Studio Legale - Country Leader Italia IAPP - DPO
Giulia Pastorella	Deputata della Repubblica Italiana - PhD London School of Economics



TAVOLO 4	Monetizzazione del dato
Layla Pavone	Coordinatrice Board Innovazione Tecnologica e Trasformazione Digitale Comune di Milano Presidente Onorario IAB Italia e ConDirettrice e Professoressa del Master Digital Communication Almed-UniCatt
Chiara Petruzzo	Data Protection Officer ARERA - Member of Board of appeal on the EU Agency for the Cooperation of Energy Regulators (Acer)
Lucio Scudiero	Avvocato Legance - Direttore Generale Lex Digital