Athens Journal of Law - Volume 10, Issue 1, January 2024 – Pages 47-62

Data Act:
New Rules about Fair Access to and use of Data

By Maria Luisa Chiarella[*] and Manuela Borgese[±]

Data-driven technologies are becoming more and more relevant every day. The constant increase in products connected to the Internet corresponds to an increase in the volume of data generated, the content of which represents a fundamental resource both for technological and economic evolution and with a high impact for businesses, citizens, and the public sector on the whole. This is the underlying motivation behind the approval of the Data Act, the new EU Regulation adopted on 27 November 2023 which aims to create a European regulatory framework based on clear rules on data sharing, a fair and guided data economy in the European Union.

Keywords: *Data economy; Market regulation; EU policies; Data Protection; Data Circulation; Access; Sharing; Interoperability.*

Introduction

This paper deals with the concept of data as a legal asset within the recent European legislation. Since the last century, Information and Communication Technologies (ICTs) have taken on a fundamental role in the lives of individuals and organisations. Contemporary society is generally now defined as an information society, since data is a central element and a precious resource both for technological and economic evolution with a high impact on businesses, citizens, and the public sector on the whole.[1] Further explained below in the investigation, data-based technologies and data access take on a more concrete relevance every day. The constant increase in Internet products corresponds to an increase in the volume of data generated, the content of which represents a fundamental development factor for technological evolution and with a high potential for businesses, citizens and for sustainable economic growth and recovery[2]. In general, it is related to the benefit of digitalisation in terms of security, geopolitical

[*]Ph.D., Associate Professor of Private Law, Magna Græcia University of Catanzaro, Catanzaro, Italy; authoress of paragraphs 1, 2 and 5.
Email: mlchiarella@unicz.it
[±]Ph.D., Professor by contract at postgraduate courses, Magna Græcia University of Catanzaro, Catanzaro, Italy; authoress of paragraphs 3 and 4.
Email: manuela.borgese@unicz.it

[1]See, among others, Stanzione (2022) at 1 et seq.; Ricciuto (2022) at 105 et seq.; Zeno Zencovich (2023) at 415 et seq.; Versaci (2020) at 27 et seq.; De Franceschi (2017) at 9 et seq.; Quarta & Smorto (2020) at XI et seq.; Dąbrowski & Suska (2022) at 1 et seq.

[2]See the European Parliament Resolution *European strategy for data* of 31.03.2021, in https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0098&from=EN.

https://doi.org/10.30958/ajl.10-1-3 doi=10.30958/ajl.10-1-3

resilience, and strategic autonomy of the Union[3]. At present, the advantages offered by the digital age are also balanced by the risks of the invasiveness of new technologies. In particular, those based on artificial intelligence have automated decisions with the added risk of significantly impacting the rights and freedoms of individuals.

The topic under investigation ranks highly among European policies in the digital world. In this field, Art. 8 of the European Charter of fundamental rights states that every individual is entitled to have their personal information protected (par. 1); this personal data must be treated in a fair and legal way for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law; these data are made available to individuals requesting copies, to be rectified if erroneous (par. 2); an independent authority is responsible for monitoring compliance with data protection rules (par. 3).

The protection of natural persons in relation to the processing of personal data concerning them is also protected in Article 16 of the Treaty on the Functioning of the European Union, which constitutes a specific legal basis for the adoption of legislative acts relating to data protection. Before the introduction of the European Charter, Art. 8 of ECHR protected the right to respect for family and private life. This right was further protected by the Council of Europe Strasbourg *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* of 1981 which was the first binding international document protecting the individual against possible abuses of collecting and processing personal data, processing of individuals' "sensitive" data in absence of proper legal safeguards. The Preamble of this Convention recalls "the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing." Art. 2 defines "personal data" as any information relating to "an identified or identifiable individual (data subject)." The Convention also preserved the individual's right to know that information on him or her is stored and, if necessary, to have it corrected. The Convention also admitted restriction on the rights in presence of overriding interests (e.g., State security, defence, etc.) and it imposed some restrictions on transborder flows of personal data to States in case of no equivalent protection. The European Court of Human Rights has brought the protection of personal data back to the protection of confidentiality by leveraging the Strasbourg Convention n. 108 of 1981[4].

In principle, the collection, storage, and any processing of "personal data" is an interference with "privacy" and the right to protection of "personal data" under both ECHR and EU law.

Nowadays, among European documents, there is another steppingstone to bear in mind: the *Declaration on European digital rights and principles*, approved in January 2023, which lays down a set of principles for the digital transition

[3]*Ibid.*.

[4]See ***Copland v United Kingdom*** [2007] ECHR *62617/00* (*3 April 2007*): "[…] the Court considers that the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8" (par. 44).

according to European values. The Declaration illustrates the EU's commitment to a safe, secure, and sustainable digital transformation that puts people and human rights at the centre, in line with EU values and fundamental rights. The approval of this Declaration reflects the political commitment of the EU and its Member States to promote and implement these fundamental principles in all areas of digital environment and to achieve the objectives of the Digital Compass 2030. This Declaration aims to be a guide for the Digital Decade 2030 Strategic Agenda. Its political program establishes an annual cooperation cycle to achieve common objectives and targets, based on an annual cooperation mechanism involving the Commission and the Member States.

Returning to secondary European law, in the context of this research, it is useful to retrace the main stages in terms of data protection.

In the context of protecting individual rights, during the last decade of the 20th century the "Mother Directive" in data protection (n. 95/46/EC) had the merit of breaking down borders to guarantee a free flow of data for the first time in history, granting protection to natural persons in the balance between personal protection and free movement of data within the EU, in view of protecting innovation and the fundamental right of the individual to control information concerning him[5].

In 2002, we had the E-privacy Directive which pointed out more specific privacy rights in the field of electronic communications[6], including rules of any personal and non-personal data storing and access from terminal equipment. But it was not until 2018 that this made a determining turning point when, in fact, the GDPR (*General Data Protection Regulation* – Reg. UE 679/2016) came into effect: a strategic tool for the digital single market in Europe with the aim of regulating the right to protection of personal data considering its social function. The regulation entered into force on 24 May 2016 and has been applied since 25 May 2018. It repealed the "Mother Directive," deemed appropriate to better harmonise the regulation of personal data protection in the EU through a regulation (characterised by direct applicability throughout the EU territory without the need for transposition acts) rather than through a directive.

These EU acts provide the basis for sustainable and responsible data processing, combining in some cases personal and non-personal data.

In Italy, the adaptation of internal legislation to the GDPR took place with the Legislative Decree n. 101/2018 which modified the Privacy Code (Legislative Decree n. 196/2003) conforming it to the principles of the GDPR.

Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data is another important text in this field[7]. Furthermore, the EUDPR (*Data Protection Regulation for the*

[5]Rodotà (1995) at 19 et seq.

[6]Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[7]The directive entered into force on 5 May 2016 and EU countries had to transpose it into their national law by 6 May 2018.

European Union institutions, bodies, offices and agencies - Reg. UE 1725/2018) provided the rules applicable to the processing of personal data by EU institutions, bodies, offices and agencies in line with the high standards of data protection prescribed by the GDPR. It has been applied since 11 December 2018, when it repealed and replaced its predecessor, Reg. (EC) 45/2001[8]. Moreover, in 2018 the Regulation on free flow of data aims to ensure that electronic data, apart from personal data, can be processed freely throughout the EU[9].

Thanks to all these instruments, we have a European legislation and public enforcement for the protection of personal data and a European Data Protection Board (EDPB) responsible for ensuring the application of European rules (Artt. 63 to 76 and Recitals 135 to 140 of GDPR). The EDPB ensures that data protection law is applied consistently across the EU and it works to ensure effective cooperation amongst Data Protection Authorities. The Board adopts guidelines on the application of the GDPR and it also issues binding decisions on disputes regarding cross-border processing, thereby ensuring a uniform application of EU rules.

All this considered, we must bear in mind that, in the contemporary data driven economy, EU policies place their emphasis on data circulation, rather than focusing attention exclusively on data protection and data subjects' fundamental right to control. Precisely by virtue of recent political trends, in the European Union the attention to data regulation in the digital economy has undergone a decisive change. Recent regulatory interventions, fundamental pieces of the European data strategy[10], introduced by the Open Data Directive[11], aim to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to data reuse, with the aim of creating a single market for the exchange and reuse of data both in public and private areas[12]. Emphasis is placed on the circulation, sharing, interoperability (and not only portability) of data as the new challenges and pillars of the European data strategy. Once considered that the goal is "A Europe fit for the digital age"[13], new rules are always required for the benefit of the EU digital environment[14]. Thus, the focus is changed: the emphasis becomes more marked on data circulation and above all the model of reuse and sharing is defined, both in a public and private perspective.

[8]Regulation (EC) n. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

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

[10]In argument, see Cerrina Feroni (2022).

[11]Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast).

[12]Irti (2021) at 39; Poletti (2023) at 367 et seq.

[13]In argument, see https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en.

[14]We must remember also, in a different perspective, the important role played by the Digital Market Act, the Digital Service Act and the Data Governance Act. The Proposal for a Regulation on artificial intelligence is also headed to integrate with this legal framework. In argument, among the others, see Resta (2023) at 605 et seq. and, if you wish, Chiarella (2023), at 33 et seq.

European Data Strategy

Keeping this in mind, it is useful to point out that personal and non-personal (such as industrial or commercial) data represents a key element for the digital economy; it is an increasingly valued resource for the market and a tool to ensure green and digital transition, although most remain unused or accessible only to a small number of large companies. Economic growth and a competitive, multi-player and fair market economy need rules of interoperability and access to data for actors of all sizes, to contrast the market imbalances.

Accordingly, the European Commission Communication "*A European strategy for data*" (February 2020)[15] aims to establish the EU as a leader in the data-driven society. The Commission Work Programme 2020 sets out several strategic objectives, including the European strategy for data, adopted in February 2020. That strategy aims at building a genuine single market for data promoting transparency, security, non-discrimination, accountability, interoperability, sharing, access, and portability of data[16].

The protection of internal market, free competition and circulation are clearly the main goals of the Commission's action which works in different aspects: networks and services (with the Digital Services Act); platforms and competition (with the Digital Market Act); the sharing of personal and non-personal data between the public and private sectors (with the Digital Governance Act); and accessibility to the value represented by that data (finally, with the Data Act)[17].

In the Resolution of 31 March 2021 *European strategy for data*[18] the European Parliament welcomes the Commission strategy for data while believing "that the strategy will be a prerequisite for the viability of European businesses and their global competitiveness and for the progress of universities, research centres and nascent AI, and marks a crucial step towards building a data society rooted in rights and EU values, defining the conditions for and establishing of the Union's leading role in the data economy. This leads to better services, sustainable growth and quality jobs; considers that ensuring trust in digital services and in safe smart products is fundamental for the digital single market to grow and thrive, and should be at the core of both public policy and business models." The Resolution

[15]Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy for data* (Bruxelles, 19.2.2020): "The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. It should be a space where EU law can be enforced effectively, and where all data-driven products and services comply with the relevant norms of the EU's single market. To this end, the EU should combine fit-for-purpose legislation and governance to ensure availability of data, with investments in standards, tools and infrastructures as well as competences for handling data. This favourable context, promoting incentives and choice, will lead to more data being stored and processed in the EU".

[16]Cerrina Feroni (2022).

[17]*Ibid.*

[18]https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0098&from=EN.

also notes that "the Commission should ensure competitive markets through interoperability, portability and open infrastructures, and remain vigilant about any potential abuses of market power by dominant actors." Digital markets are in fact characterised by high entry barriers relating to access to and ownership of data. Regulating the sharing of data and unlocking data markets may represent one possible way to correct these shortcomings[19].

All this is considered in the European data strategy. A single market where data flows freely within the EU and across all sectors is seen as a benefit for businesses, researchers, and public administrations and this is the final goal of the model proposed by the EU. Data is assumed as a key building block of the digital economy and an essential tool to ensure green and digital transitions. Our society is more interconnected every day, with an incremental increase in devices and data produced by citizens and businesses. However, most of this data remains largely unused or accessible only to a small number of large companies, with a significant detriment to the potential value that would be derives from full use.

For these reasons, data is considered "the new oil" - as we also read in a widely referenced article by *The Economist*[20]. While the volume of data continues to rise and it is owned only by the large digital firms, the issue is how to manage data in a way that ensures adequate competition.

Bearing this in mind, the European strategy is aimed at creating a single market for data, to create a space where data is available for use in the economy and society, while maintaining the control of businesses and individuals generating the data and contributing to social improvement in important fields such as health care, sustainability, and energy efficiency.

Regulating data access and use is considered a fundamental step toward seizing the opportunities of the data driven society. In this context, the Data Act, the new EU Regulation adopted November 27, 2023 is a key pillar and the second major initiative in the data strategy (after the Data Governance Act). It contributes to the creation of a cross-sectoral governance framework for data access and use, by legislating on matters that affect relations between data economy actors, to build a horizontal data sharing system. The new regulation aims to create a European regulatory framework based on clear rules aimed at allowing the conditions for a fair and guided economy from data in the European Union.

Data Act: Premises and Objectives

Over the last decade, there has been a significant increase in connected devices and greater human-machine interaction, which has corresponded to a proportional increase in data generated. This is a trend destined to grow. In fact, according to forecast estimates from the European Commission, by 2025 the global volume of data will increase by 530%, with an economic value of 829 million euros.

[19]Szczepański (2020).
[20]Humby (2017). In a critical perspective, see Martinez (2019).

Beyond strictly numerical indices, there is no doubt that data represents an element of essential strategic value in the digital economy, by virtue of its high potential in the context of the digital and ecological transition. For example, it has been observed that companies that base their innovation plans on data record a 5% - 10% faster growth in productivity than others.

In a context of undoubted opportunities, however, we observe that this potential is not fully exploited, due to various reasons.

First, the management of large data sources requires substantial investments for the maintenance of technological infrastructures for which proportional economic investments are also necessary. This limit is further hindered by the lack of specific incentives and ease of access to them, which represents a structural block for the acquisition of concrete tools.

Secondly, to take full advantage of data analysis, it is essential to have adequate skills, especially digital ones.

Further categories of causes are also of a regulatory nature, due to the lack of specific provisions regulating the standards and fundamental aspects underlying the interoperability of data and between data and services, as well as the concentrations of the same within the circle of large companies, even when due to contractual abuse. This last circumstance is partly due to the abuse of dominant positions or contractual positions unbalanced in the use and sharing of the data produced.

Despite the copious regulatory production, which will also be partially examined, the reviewed framework highlights the persistence of strong needs for intervention to implement the European strategies already examined. This need is therefore the basis of the new Data Act, as a key pillar of the European data strategy.

The distinctive element of the Data Act is to make available a greater quantity of data, personal and non-personal, relating to connected products or related services, making them accessible to users and usable through a clear system of rules, in all sectors/economies of the Union. The desired effect is therefore to expand the data market, including manufacturers of connected products and providers of related services. In addition to this commercial line, this legislation aims to promote a greater balance in the use of data, regulating a uniform distribution free of barriers or anomalous concentrations, respecting the rights of the parties involved, mainly data subjects and small and medium- sized enterprises[21].

These assumptions are the basis of the creation of a circular context, in which data are freer to circulate in interconnected and interoperable environments, according to certain, effective rules, all to create a reliable system that can generate confidence in the use of such systems.

This is a regulation developed following a complex process, starting with a legislative proposal formally presented by the Commission in 2022[22], following

[21]Poletti (2023).

[22]https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2022/0068/COM_COM(2022)0068_EN.pdf.

a specific public consultation phase[23], which has now finally been approved by Council of European Union and has reached the final approval phase[24]. After publication in the EU's official journal, it shall apply from 20 months from the date of its entry into force. However, the requirements for simplified access to data for new products (article 3, paragraph 1), shall apply to connected products and the services related to them placed on the market after 32 months from the date of entry into force of the regulation.

Access and Transparency at the Crossroads between user and Company Protections

Among the main objectives pursued is that of facilitating, for businesses and consumers, access to data obtained or generated by the use of a connected product or related service[25], with the possibility to use or transfer them to third parties indicated by the user.

For this purpose, the legislation sets up a system based on transparency and accessibility to information, dictating specific requirements starting from the design of the same, up to the transfer, in the cases provided for by the legislation.

In particular, it is established[26], by default, that connected product and related services are designed, manufactured and delivered in such a way that the product data and related service data, including relevant metadata necessary to interpret and use such data, are easily accessible in a secure, free manner, in a complete, structured, commonly used and machine-readable format and directly accessible to users.

However, the legislation intervenes in a very incisive manner in the information, pre-contractual and contractual context, in the cases of sale, rental or leasing of a connected product and with respect to the supply of connected services.

The emerging framework presents a strengthening of transparency requirements, not only with respect to the form but also with regard to the list of specific technical and informational details.

[23]https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases /F_en.

[24]https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act https://www.consilium.europa.eu/en/press/press-releases/2023/11/27/data-act-council-adopts-new-law-on-fair-access-to-and-use-of-data/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Data+Act%3a+Council+adopts+new+law+on+fair+access+to+and+use+of+data.

[25]On regulatory definitions, see the provisions of the Data Act (Art. 2): "product data" refers to data generated by the use of a connected product that the manufacturer has designed to be recoverable from the connected product by a user, a data owner or a third party, including, if relevant, the manufacturer; "related service data" refers to data that also represents the digitisation of user actions or events related to the connected product generated during the provision of a related service by the provider. Data generated by the use of a connected product or related service should be understood as intentionally recorded data or data that results indirectly from user action, such as data about the environment or interactions of the connected product.

[26]Art. 3, par. 1 Data Act.

With regard to pre-contractual obligations in relation to the purchase, rent or sale of a connected product, information relating to the characteristics, volume and methods of creation, saving, access and management of the data produced must be indicated. In this category, the fundamental request to make known to the user the forms of access, the conditions of use and the quality of the service is highlighted[27].

The same provisions are envisaged for related services, in relation to which all data produced by the digitalisation of user actions or events relating to the connected product, generated during the supply of the same, are placed. In addition to what has already been examined with regard to the nature and volume of the data, specific indications are imposed regarding the identity of the prospective data holder and the means of communications with which it is possible and easy to contact him, the methods with which the user can request that the data are shared with a third party and where applicable, end the data sharing.

With respect to this last aspect, also following the strong debates that took place during the negotiations, it was specified that it must be made known whether the prospective data holder is also the holder of the trade secret contained in the data that is accessible from the connected product or generated during the provision of a related service or otherwise the actual trade secret holder[28].

The legislation then provides a clear system of rules regarding the sharing of data obtained or generated by the use of related products or services, especially with regard to access and usage rights, providing for a mandatory obligation to make such data available. This access must take place in a simple manner, complete with all the elements necessary to interpret the data, to the same extent as those held by the data holder, without unjustified delay and upon simple request[29]. Any limitations must be contractually foreseen between the parties, except in cases specifically provided for by the law such as compromising the safety of the device or service itself[30].

Due to the strong margin of access rights, the need to protect trade secrets emerged already during the negotiations. The problem that emerged during the discussion was linked to the fact that blocking access on this point could have resulted in defeating the purpose underlying the entire legislation. On the other hand, allowing unconditional access would have compromised the business integrity of the companies involved. Therefore, the solution adopted is placed on a median level, generally providing that commercial secrets must be preserved and disclosed only if data holders and users adopt all necessary measures to preserve its confidentiality, especially with respect to third parties[31].

[27]Art. 3, par. 2 Data Act.
[28]Art. 3, par. 3, lett. h. Data Act.
[29]Articles 4-5. Data Act.
[30]Art. 4, par. 2 Data Act.
[31]Art. 4, par. 6 et seq. Data Act.

In the absence of such guarantees or if the user does not take the agreed measures, the law authorises the data holder not to communicate the requested information. However, given the extremely delicate nature of the matter in question, the legislator has admitted that the data holders can refuse the access request if they can demonstrate that it is highly probable that serious economic damage could result from the disclosure, despite the measures adopted.

This provision acquires an even more interesting connotation when one considers its dynamics in the case of a user's request to share data with third parties. The emerging risk is that of exposing potential trade secrets to other entities in a potential competitive position. In balancing this situation with the right to request transfer by the user, the law recognises a specific provision of protection, especially due to the possible obvious exposure of the contents of the trade secret to potential competitor companies. With respect to this need, a specific protection is in fact specifically provided for[32], where disclosure is limited only to cases in which it is necessary to fulfil the purpose agreed upon between the user and the third party. If so, the data holder or the trade secret holder shall identify the data which are protected as trade secrets and provide appropriate measures for the transfer. Even in these cases the exceptions already observed with regard to the opposition apply, in cases where the disclosure could lead to serious economic damage for the company or suspension, if the third party does not implement the identified measures or undermines the confidentiality of the trade secrets.

The Protection Needs of Smaller Companies in the Context of Access to Data

On the basis of a real and fair sharing context, it is essential that there are no prevarications or imbalances that jeopardise the rights of contractually weaker counterparties. In particular, in order to rebalance the negotiating power in contracts between professionals, especially to protect microenterprises, small and medium-sized enterprises[33], often compromised by contractual imbalances in data sharing contracts, the Data Act imposes a margin of protection against unfair contractual clauses imposed by a stronger contractual counterparty[34].

In relations between companies, the legislation unequivocally clarifies its position as a guarantee towards an exchange of data based on equity and correctness, imposing fair, reasonable, non-discriminatory, and formulated terms and conditions in a transparent manner. Furthermore, to avoid abusive contractual conditions[35] with respect to access or use of data or the limitation of liability and recovery and protection tools, it must be considered non-binding or non-applicable, where contrary to a right of the user.

[32]Art. 5, par. 9.
[33]The European Commission defines micro, small and medium-sized enterprises (SMEs) in the EU Recommendation 2003/361.
[34]Scientific debate on this issue is very wide; see, among the others, Roppo (2010) at 19 et seq.; Di Raimo (2003) at 159 et seq.; Chiarella (2016) at 45 et seq.
[35]Art. 8 Data Act.

Especially with regard to the regulation of contractual relationships between companies, the legislation contains a specific provision of those cases in which a contractual clause must be considered, respectively, abusive or presumably abusive[36].

To safeguard this framework of guarantees, the right to reasonable compensation for companies for making data available is also specified, which must be fair and non-discriminatory, as well as providing for adequate dispute resolution mechanisms[37].

A further aspect concerns the obligations to share and use the data held by companies, by public bodies and institutions, agencies or bodies of the Union. This provision certainly includes all those in which circumstances arise that justify an exceptional need for data. However, they can also refer to all those hypotheses in which the mandatory sharing of data between companies and public administrations is justified in order to support public policies and services based on concrete, effective, efficient and results-oriented data. This is another area heavily discussed in the dialogue phase, since on the one hand greater openness towards this type of sharing brings undoubted advantages but can, at the same time, be unsustainable for data holders. Therefore, to safeguard these conflicting needs, the most correct choice is to precisely limit the categories[38] of cases of access to such data and impose specific obligations of justification in the request for access by authorised public entities[39].

Interactions with other European vertical regulations

The rich framework of facilitations for access to data provided by the Data Act involves the inevitable interaction with many vertical regulations, including the Data Governance Act[40], the Data Base Directive[41], the Regulation on free flow of data[42] and the GDPR, most of which we already mentioned before, and on which we will focus more carefully.

Before proceeding with this analysis, we can only start from the consideration that the Data Act is part of an enormous European regulatory context, part of the European data strategy[43], within which it must be examined and considered.

[36]Art. 13 Data Act.
[37]Art. 9 Data Act.
[38]Art. 15 Data Act.
[39]Art. 17 Data Act.
[40]Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724.
[41]Directive 96/ 9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
[42]See Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast).
[43]See the European Parliament Resolution *European strategy for data* of 31.03.2021, in https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0098&from=EN.

First, we can consider the innovative force dictated by the Data Governance Act ("DGA"), which has the merit of creating the processes and structures to facilitate the sharing of data by companies, citizens and public enterprises. Among these, it is interesting to observe, for example, the rules relating to the so-called "data altruism"[44], the reuse of data held by public bodies, intermediation services and one-stop shops for data. The DGA has therefore created the basis on which the collection flow set by the Data Act is based, with its rules aimed at making an even greater number of data available and usable, in particular that generated by the use of connected products and related services, identifying the categories of subjects authorised to access, use and dispose of such information.

With regard, however, to some specific regulations of more immediate convergence, the Data Act directly provides for specific provisions, aimed at identifying the relationships of possible interaction, for a more harmonious regulatory application.

In this sense, we can consider all the cases in which the provisions of the Data Act prevent any prejudice to aspects already regulated by further regulations, including those on the protection of intellectual property rights[45], on the use and access of data for statistical purposes[46].

However, the hypothesis of Directive 96/9/ EC, relating to the legal protection of databases, established the so-called *sui generis right*[47], which protects the contents of databases.. This right in particular has been declared inapplicable in eliminating the risk that owners of data may claim the sui generis right.

Although apparently pervasive, it should be highlighted that the exercise of this right could in fact represent an obstacle to the exercise of the rights recognised by the Data Act, thus nullifying its innovative significance. However, recital 112 specifies that this right continues to operate outside the scope of application of the Data Act, provided however that this does not result in a violation of protection within the scope guaranteed by the law.

Another regulation that deserves a comparative analysis with the Data Act is the regulation on the free circulation of non-personal data[48], a regulatory act of great importance in the European data economy.

---

[44]"Data altruism" is referred to in art. 3 of the DGA. We can also consider the mechanism for voluntary data sharing based on the consent granted by the interested parties to the processing of personal data concerning them, or on the authorisations of other data owners aimed at allowing the use of their non-personal data, without requesting or receiving compensation that goes beyond compensation for the costs incurred in making their data available, for objectives of general interest, established in national law, where applicable, such as healthcare, the fight against climate change, improving mobility, facilitating the processing, production and dissemination of official statistics, improving the provision of public services, the development of public policies or scientific research in the general interest.

[45]Recital 13 of the Data Act.

[46]Regulation (EC) 23/2009.

[47]Art. 7 Directive 96/9/EC.

[48]The Regulation (EU) 2018/1807.

Among the most important elements, it is highlighted that this Regulation, through specific provisions aimed at digital service providers, has imposed the commitment to develop and implement self-regulatory codes of conduct to facilitate the change of providers of services and the porting of date.

Despite the excellent premises, the conditions envisaged by this Regulation have not brought the desired results, as there has been neither a high rate of adoption of these self-regulatory tools nor an increase in open standards and interfaces; hence, the central importance of the Data Act in providing for minimum regulatory obligations directed at suppliers of data processing services, aimed at eliminating those barriers, of a technical or contractual nature, which limit or hinder the transfer of user data and the switching from one processing service to another. The Data Act, therefore, complements the regulatory approach envisaged by the General Data Protection Regulation[49], adding generally applicable obligations on the transition to the cloud.

The Data Act and Relations with the Regulations on the processing of Personal Data

Due to the common object that unites them, the processing of data for data subjects, the Data Act is intimately linked to the current legislation on the processing of personal data and the protection of privacy in the electronic communications sector, referred to in the Regulation 2016/679 and Directive 2002/58/EC. In fact, the use of a connected product or a related service, in case of personal data referable to a natural identified or identifiable person[50], make the privacy legislation applicable. Already in the first recitals of the Data Act, the relationship with this legislation is examined, addressed as the first methodological premise underlying the entire legislation.

The absolute absence of any prejudice with respect to the regulations on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment is therefore preliminarily established[51], especially with regard to the areas of competence of the supervisory authorities and the rights recognised to data subjects.

Since at the basis of the proposed Regulation of the Data Act, the expansion of the data produced is associated with a rigid regulation of access systems, it is precisely on the rights of the interested parties, specifically those of access and portability[52], that these two regulations must intertwine more often.

In fact, given the multiple provisions contained in the Data Act, sometimes even restrictive to protect the interests of the parties involved, as in the case of contexts in which trade secrets are present, the need to frame the interested

[49]Art. 1, par. 7 Data Act.
[50]See Art. 4 GDPR and art. 2, lett. a Directive 2002/58/EC.
[51]See the express referring, in Art. 1, par. 5, of Data Act, to regulations (EU) 2016/679 and (EU) 2018/1725 and Directive 2002/58/EC.
[52]Articles 15 and 22 GDPR respectively.

party's power of control over his/her own personal data emerges[53]. For this reason, the Data Act provides that when users are also data subjects, therefore recipients of the rights provided for by articles 15 and 20, in the event of conflict with the provisions of the Data Act the provisions of the GDPR will instead prevail[54].

A further, very significant clarification, highlighting the supremacy of the current privacy legislation, is the explicit provision that the Data Act cannot be considered a legal basis pursuant to art. 6 of Regulation (EU) 2016/679 for the collection and creation of data by data holders[55]. Therefore, the initial requirement to be satisfied is always that of compliance with the processing of personal data, precisely the principle of lawfulness of the processing[56] which therefore represents the prerequisite on which the structure envisaged by the Data Act is based. On the basis of this premise, we also understand the reference to the necessary application of minimisation in the context of the application of the principle of *privacy by design and privacy by default*[57], as a tool to safeguard the protection of the data being processed.

The framework reviewed therefore represents the governance context of this new category of data, both with regard to their qualitative and quantitative structure and with regard to the rights recognised to data subjects. The aim is to fill the information gap of the interested party, now faced with a new category of data and to make him/her a conscious and active part of the application of the rights that are recognised by the GDPR and which the Data Act Proposal does not intend in any way to compromise. The circulation of such data, however, in which the personal component is largely combined with a prevalent amount of non-personal data, is also a direct fulfilment of the data holders and data recipients, i.e. those actors in the commercial circulation segment, called to correctly manage the most relevant phase, that of production and use, in the context of their exploitation and valorisation.

Conclusion

The goal of the European Data Strategy is the construction of a Digital Single Market that puts the person at the centre of digital transformation and makes the European digital space safe and competitive. Accordingly, the European Declaration on digital rights and principles for the digital decade is a suitable tool for enhancing and defending democratic and personalistic values online as well as offline (art. 1).

[53]Poletti (2023).
[54]See Recital 7 Data Act.
[55]See rec. 7, 34, 35 and art. 4.12, 5.7.
[56]Art. 5 GDPR.
[57]On the principles of minimisation and privacy by design and by default, compare art. 5 and 25 GDPR.

Following the Data Governance Act, Data Act regulation is a tool to consolidate the role of the EU and to compete on a global scale with world economic giants. In particular, the removal of barriers that currently limit the interoperability of data represents a fundamental development factor for the internal digital market, to the advantage of competitiveness, innovation, and sustainable economic growth. To create such a framework, EU politics opts for legal harmonisation – through the introduction of an EU regulation – bypassing the fragmentations of national legislations, with clear rules regarding the identification of who has the right to use the data collected, obtained or otherwise generated by connected products or digital services. The huge scope of this new legislation already highlights the first undisputed advantage in favour of SMEs, today in fact limited by the benefits deriving from access to such data both due to the lack of digital skills to collect, analyse and use them and due to the non-existent information interoperability with the operators who hold them. The EU recently adopted its position on this issue, providing for more measures to allow users to access the data they generate and increasing the guarantees of data sharing agreements between companies. In conclusion, the EU Data Act appears suitable to rebalance the negotiating power to protect weaker companies, identifying greater protection with respect to possible contractual imbalances with companies in a dominant position. The regulatory process still provides for several steps. However, we can already speak of a framework based on clear rules that lay the foundations for concrete growth with real advantages for citizens, businesses and the public administration[58].

References

Cerrina Feroni, G. (2022), 'Luci e ombre della Data Strategy europea', in *Agendadigitale.eu*, 12 May 2022.

Chiarella, M.L. (2016). *Contrattazione asimmetrica. Segmenti normativi e costruzione unitaria.* Rome: Giuffrè.

Chiarella, M.L. (2023). 'Digital Market Act (DMA) and Digital Service Act (DSA): New Rules for the EU Digital Environment', in *Athens Journal of Law*, 9(1): 33-58, and in Frenkel, D.A. (ed.) (2023), *A Current Anthology of Law*, pp.33-57. Athens, Greece: Atiner.

Dąbrowski, Ł.D. & M. Suska (eds.). (2022). *The European Union Digital Single Market. Europe's digital Transformation.* London and New York: Routledge.

De Franceschi, A. (2017). *La circolazione dei dati personali tra* privacy *e contratto.* Naples: Edizioni Scientifiche Italiane.

Di Raimo, R. (2003). *Autonomia privata e dinamiche del consenso*. Naples: Edizioni Scientifiche Italiane.

Irti, C. (2021). *Consenso negoziato e circolazione dei dati personali*. Turin: Giappichelli.

Humby, C. (2017). 'The world's most valuable resource is no longer oil, but data', in *The Economist*, 6th of May.

[58]In a critical perspective, about a negative assessment of Data Act, see Kerber (2023) at 120 et seq.

Kerber, W. (2023), 'Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives', in *GRUR International* 72(2):120-135.

Martinez, A.G. (2019). *'No, Data Is Not the New Oil',* in *Wired*, February 26th 2019.

Poletti, D. (2023). 'Il controllo dell'interessato e la strategia europea sui dati' in *Osservatorio sulle fonti*, 2:367-378.

Quarta, A. & G. Smorto (2020). *Diritto privato dei mercati digitali*. Florence: Le Monnier.

Resta, G. (2023), 'Pubblico, privato, collettivo nel sistema europeo di governo dei dati' in G. Resta & V. Zeno Zencovich (eds.), *Governance of /trough Big Data*, II, Rome: RomaTre Press.

Ricciuto, V. (2022). *L'equivoco della privacy. Persona* vs *dato personale*. Naples: Edizioni Scientifiche Italiane.

Rodotà, S. (1995). *Tecnologie e diritti*. Bologna: il Mulino.

Roppo, V. (2010). 'Regolazione del mercato e interessi di riferimento: dalla protezione del consumatore alla protezione del cliente' in *Rivista di diritto privato* 1:19-35.

Stanzione, P. (2022). *I poteri privati delle piattaforme e le nuove frontiere della privacy.* Turin: Giappichelli.

Szczepański, M. (2020). 'Is data the new oil? Competition issues in the digital economy', European Parliament Research Service: January 2020.

Versaci, G. (2020). *La contrattualizzazione dei dati personali dei consumatori.* Naples: Edizioni Scientifiche Italiane.

Zeno Zencovich, V. (2023). *'Do "data markets" exist?'*, in G. Resta & V. Zeno Zencovich (eds.), *Governance of /trough Big Data*, I, Rome: RomaTre Press.