Data as the Object of a Contract and Contract Epistemology

Carolina Perlingieri*

Abstract

The syntagma 'data' enters in the legal language, following the recognition of the right of each person to the protection of personal data and only successively is used also in juridical discipline for the flow of information not referable to the natural person.

The Regulations (EU) 2016/679 and 2018/1807 – that establish the free flow principle of different types of data and permit so to consider the data as intangible entities, and consequently goods – are the foundations of data, considered as a good, and establish the process of legal objectification of data as a good for specific legal purpose and worthy of protection depending on the different uses.

Nevertheless the statement of free flow of data raises the question whether the legal reception of unitary paradigm of data.

The use of the same syntagma 'data' must not obscure the fact that the data relating to the natural person is the object of legal protection as such; differently, the non-personal data can be object of protection only if in an aggregated form, as it is unsuitable of generating a utility if singularly considered, with the consequent exclusion of protection as a legal good.

The above observations, nevertheless, do not prevent to consider a different use of data, meaning finalized or not to circulation.

Therefore the sharing of a case method of analysis has allowed to analyze the different contractual models inherent to data and that have stemmed from the use of the new technologies.

I. Data as a Paradigm in the Definition of the Legal Regime of the Circulation of Information

The word 'data' entered in legal language following the recognition of the right of each person to the protection of personal data[1] and led to the introduction

* Full Professor of Private Law, University of Naples 'Federico II'. This is the text of the talk I gave at the Workshop '*Rechte an Daten*', held at the University of Bayreuth on 21-22 February 2019. I would like to thank the organizers of the Workshop and in particular Ms Pertot for the invitation and all the participants for their kind attention.

[1] The true extent and the real content of the right to data protection, with particular attention to its juridical nature, raised an intense debate by scholars. For an overlook cf G. Resta, 'Il diritto alla protezione dei dati personali', in F. Cardarelli et al eds, *Il codice dei dati personali* (Milano: Giuffrè, 2004), 16. The remedial approach focuses on the breach of behavioural duties and specific information duties of the controller. See A. Di Majo, 'Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela', in V. Cuffaro et al eds, *Trattamento dei dati e tutela della persona*

of legal protection of any information regarding the natural person, identified or identifiable,[2] capable of being processed wholly or partly by automated or not

(Milano: Giuffrè, 1999), 225. In contrast with this concept, others opt for a proprietary approach, qualifying the right to data protection as an intellectual property right. Cf for all V. Zeno Zencovich, 'Cosa' *Digesto delle discipline privatistiche, Sezione civile*, IV (Torino: UTET, 1989), 438; see also L.C. Ubertazzi, 'Riservatezza informatica e industria culturale' *AIDA*, 530 (1997); according to some others the right to data protection has a constitutive effect, creating a new immaterial good, which is the personal data: L. Mormile, 'Lo statuto giuridico dei dati personali', in R. Panetta ed, *Libera circolazione e protezione dei dati personali* (Milano: Giuffrè, 2006), 570; V. Cuffaro, 'A proposito del ruolo del consenso', in V. Cuffaro et al eds, *Trattamento di dati personali e tutela della persona* (Milano: Giuffrè, 1999), 121; for an interesting point of view, see P. Manes, *Il consenso al trattamento dei dati* (Padova: CEDAM, 2001), 13, who refers to the rules of copyright law (Arts 20 and 25 of the Act 633/1941), proposing the duplication 'of two different rights on immaterial goods, one of them patrimonial, *ie* the right regarding personal data, which refers to an economically relevant entity which is derived from the commercial and economic exploitation of some information; the other moral, consisting of one's right regarding his or her own information, a genuine personality right, which is inalienable and non-patrimonial and refers to some categories of personal information, the information regarding the most intimate sphere of a person and inseparable from it as an integral part of one's own personality in the same way as the name and the image' (the Author refers to '*due diversi diritti su beni immateriali, l'uno patrimoniale, il diritto sui dati personali, che ha ad oggetto un'entità economicamente rilevante che deriva dallo sfruttamento commerciale ed economico di alcune informazioni; l'altro morale, il diritto sulle proprie informazioni, vero e proprio diritto della personalità caratterizzato dai requisiti dell'indisponibilità e della non patrimonialità, che ha ad oggetto alcune categorie di informazioni personali, le notizie inerenti la sfera più intima della persona ed inscindibili da essa, perché integranti la propria personalità alla stessa stregua del nome e dell'immagine*'). Diametrically opposed to the idea of data as a legal asset, see D. Messinetti, 'Circolazione dei dati personali' *Rivista critica di diritto privato*, 350 (1998); A. Fici and E. Pellecchia, 'Il consenso al trattamento', in R. Pardolesi ed, *Diritto alla riservatezza e circolazione dei dati personali* (Milano: Giuffrè, 2003), 504. Lastly, the right to data protection is considered as an expression of the broader value of the person according to Art 2 of the Italian Constitution, a new personal right: another proof of the close connection existing between the regulation of data processing and the system of protection of personality is also the reference to the human dignity in Art 2, para 1 of the Italian Privacy Code. See G. Mirabelli, 'Le posizioni soggettive nell'elaborazione elettronica dei dati personali' *Diritto dell'informazione e dell'informatica*, 323 (1993); E. Giannantonio, '*Sub* Art. 1', in M.G. Losano et al eds, *La tutela dei dati personali. Commentario alla l. 675/1996* (Padova: CEDAM, 1999), 6.

[2] There is a broad definition of personal data, which includes elements of direct and indirect identification. The indirect identification and/or identifiability represents the more critical case, in which, in practice, different information regarding a user can potentially be used to identify him or her when it is combined (so-called phenomenon of 'unique combinations'): see Art 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 13. In particular: Case C-101/01 *Bodil Linqvist*, (2004) available at http://curia.europa.eu, which clarifies that 'the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data (…) within the meaning of Article (…) of Directive 95/46/EC'. For the qualification of the IP address as personal data see Case C-582/14, *Patrick Breyer* v *Bundesrepublik Deutschland*, Judgement of 19 October 2016, available at http:// curia.europa.eu, according to which the dynamic IP addresses are neutral information, that may constitute personal data, if they are combined with other information or subject to inferential analysis by means of Big Data analytics. Furthermore, the Proposal for the e-privacy Regulation of the European Commission of 10 January 2017, available at https://eur-lex.europa.eu, requires the consent of the subject of the data, which should be freely given, specific, informed, unambiguous and explicit, also for the processing of electronic communications

automated means.

Subsequently, the concept of 'data' has gone beyond the natural person and is now used in law to describe the flow of information not referable to the natural person.[3]

This has come about as a result of the digitalization of the economy and as a result of information and communication technologies which are at the base of the economic systems of societies. Consequently, specific attention is paid to electronic data that has the potential to create enormous value through creation and collection, aggregation and organization, processing, analysis, commercialization and allocation, and use and reuse.

Let us consider, for example, the aggregated and anonymous data used in Big Data analysis, such as data on precision agriculture which can contribute to monitoring and optimizing the use of water and pesticides, or data for the maintenance of industrial machines.

Regarding this topic, following the European Regulation (EU) 2016/679 of 27 April 2016, GDPR on the protection of natural persons[4] with regard to the processing of personal data and on the free movement of such data, the recent European Regulation (EU) 2018/1807 of 14 November 2018 creating a framework for the free flow of non-personal data entered in force on 18 December 2018.

Thus the rapid development of the economy of data and emerging technologies, such as Artificial Intelligence, products and services relative to Internet of Things, independent systems and 5G technology, has forced the EU to consider legal matters related to access to data and their reuse and accountability even when not relatable to natural persons.

II. The Difficult Qualification of Data as Personal or Non Personal

It is not always simple to recognize data as personal or non personal.

metadata (Art 3, letter *c*), as they may enable the subject's identification: data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication (points 2 and 14) may reveal extremely sensitive and personal information.

3 Generally, the digital processing of data does not allow the exclusion of so-called 'irrelevant data' as new electronic systems may get information from 'any kind of data'.

4 On the European Regulation (EU) 2016/679, cf F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo* (Torino: Giappichelli, 2016); S. Sica et al eds, *La nuova disciplina europea della privacy* (Padova: CEDAM, 2016); L. Bolognini et al eds, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali* (Milano: Giuffrè, 2016); G. Finocchiaro ed, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna: Zanichelli, 2017); A. Mantelero and D. Poletti eds, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa: Pisa University Press, 2018); G.M. Riccio et al, *GDPR e normativa privacy. Commentario* (Milano: Giuffrè, 2018), 3; V. Cuffaro et al eds, *I dati personali nel diritto europeo* (Torino: Giappichelli, 2019).

This overlap can easily be seen in the transition from anonymous data to personal data, with the consequent application of the GDPR. Let us consider an owner of an electric or hybrid car, and its component 'smart gateway'. This component contains the data relative to the engine, the performance of the car on the road, and the driver. Such data is gathered, organized and analyzed in an automated manner, by the car producer or by the computational company.

Such data can be considered either non personal or personal, depending on if the user behavior is stored. If it is considered to be personal, a question arises as to whether the ownership is the car producer's, considered as industrial data, or the car owner's in whose car the data is stored. In any case the natural person is the controller of the personal data and such data must be processed in a manner consistent with the law. In this regard, European Regulation (EU) 2018/1807 of 14 November 2018, establishes that, in the presence of personal and non personal data, the of non personal data cannot be differentiated, the GDPR will be applied exclusively.

It is also necessary to consider the distinction between personal data that is subject to the GDPR and that which is not. In this regard it is important to keep in mind the gathering and processing of online information derived from public sources. Such information is then grouped in order to identify and transfer personal data, without any authorization from the subjects of the data and from whom the information is taken and divided into areas of interests (car, make-up, travel), age, status and so on.

III. The Free Flow of Different Types of Data Set Forth by European Legislation and Their Legal Objectification

The GDPR prohibits Member States from restricting or barring the free movement of personal data within the Union for reasons of protection of natural persons in compliance with the processing of personal data; therefore it recognizes the availability of personal data and also the right of data portability. The European Regulation (EU) 2018/1807 of 14 November 2018 proclaims the same free flow principle of non-personal data within the Union, except when there is a restriction or a prohibition for public security reasons.

Thus, these two Regulations establish the free flow of different types of data, personal and non-personal, permitting consideration of the data as intangible entities and consequently goods, even where the principle of *numerus clausus* of the exclusive rights on the intangible entities is accepted. Since these Regulations are the foundations of data being considered as a good, they therefore establish the process of legal objectification of data as a good for specific legal purpose and worthy of protection depending on the different uses.

IV. The Issue of the Legal Recognition of a Unitary Paradigm of Data

1. Data as an 'Entity Susceptible of Observation and Computational Use'

Regardless of the specific Regulations, the principle of free flow of data, personal and non-personal, raises the question of whether the legal reception of the unitary paradigm of data or the non-recognition of data can be reduced to a single good. For this reason, it is necessary to ascertain if data is a paradigm capable of activating the operation of a regulatory discipline or only taking on a simple descriptive role.

The understanding of data as 'any observable entity', and as immaterial representation of an entity, which has a meaning for the natural person, is so extensive that it can be used for any information, therefore assuming no practical relevance. Every human action is likely to turn into personal data. This statement is demonstrated by a new form of capitalism, so-called surveillance capitalism,[5] which is not based on production of goods or on financial speculation, but based on collection of personal data and their commodification.

Technological development and in particular artificial intelligence, as well

[5] On surveillance capitalism cf S. Zuboff, *The Age of Surveillance Capitalism. The Fight For a Human Future at the New Frontier of Power* (London: Profile Book Ltd, 2019), 376, according to whom the digital architectures of surveillance capitalism – the Big Other – are designed to capture and control human behaviour in order to attain a competitive advantage within the new markets since internet users or 'internauts', crucially, are not products, but sources of an added value: objects of a technologically advanced and increasingly inevitable process of extracting raw material, despite themselves – producers of data. In this way, by intercepting personal data, the Big Other may have an impact on the users' behaviour and could threaten democracy. Also Z. Bauman and D. Lyon, *Liquid Surveillance* (Cambridge: Cambridge University Press, 2013) refer to a 'liquid surveillance'. Regarding interventions aiming to hinder surveillance capitalism, especially in America, see: G. Resta, 'La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE', in Id and V. Zeno Zencovich eds, *La protezione transnazionale dei dati personali dai "Safe Harbour Principles" al "Privacy Schield"* (Roma: RomaTre Press, 2016), 44-45, according to whom 'the search for a difficult point of equilibrium between protection of individual rights and the invasiveness of modern technologies of electronic surveillance' paves 'the way for actual forms of global cybersurveillance' in the face of 'local responses, such as the ones offered by the European legal system (…), which are partial and unsatisfactory' and requires 'the strengthening of the tools offered by the international law, in order to effectively implement the principles of art. 12 of the Universal Declaration of Human Rights and art. 17 of the International Covenant on Civil and Political Rights (…), where the privacy is elevated to the status of a human right, independent from national and territorial affiliation, and to adapt them to the reality of the technological context' (according to the Author, the '*ricerca di un difficile punto di equilibrio tra la tutela dei diritti dei singoli e l'invasività delle moderne tecniche di sorveglianza elettronica' pone 'le premesse per vere e proprie forme di global cybersurveillance' di fronte a 'risposte locali, quali quelle offerte dall'ordinamento europeo (…) parziali e insoddisfacenti' e richiede il 'rafforzamento degli strumenti offerti dal diritto internazionale, in modo da dare effettiva attuazione, adeguandoli alla realtà del contesto tecnologico, ai principi iscritti nell'art. 12 della Dichiarazione Universale dei Diritti Umani e nell'art. 17 del Patto Internazionale dei Diritti Civili e Politici (…), ove la riservatezza è elevata al rango di diritto umano, indipendentemente dalle appartenenze nazionali e territoriali*').

as products and services of the Internet of Things, lead to an understanding of data as an 'entity susceptible of observation and computational use', that is to say, capable of being the object of artificial and automated use.

The validity of this limitation of the legal notion of data is confirmed by the express application, *ex* Art 2.1 GDPR, which refers to

> 'the processing of personal data wholly or partly by automated means, but also to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'.

Therefore, when the data processing is non-automated, the application of this rule is possible only when its final use is as a listing in a database.

Similarly, the Council of Europe Convention on cybercrime (Budapest, 23 November 2001) defines the phrase 'computer data' as

> 'any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function'.

2. Insufficiency of a Qualification of Data Based on Computational Use for the Purposes of a Unitary Assessment of Data

This definition of 'data', anchored to a computational use, however, does not allow a unitary assessment of personal and non-personal data.

Personal data is protected as such, and is related to the essential characteristics of the natural person who, in compliance with the regulations in force, can consent to the processing of such data for an expression of self-determination.[6]

[6] Regarding the key role of consent for the handling of one's privacy cf M.G. Stanzione, 'Il Regolamento europeo sulla privacy: origini e ambito di applicazione' *Europa e diritto privato*, 1249 (2016); F.D. Busnelli, 'La persona alla ricerca dell'identità' *Rivista critica di diritto privato*, 7 (2010); S. Rodotà, *Il diritto di avere diritti* (Roma-Bari: Laterza, 2012), 397; E. Giannantonio, *'Sub* Art. 1' n 1 above, 10; F. Macario, 'La protezione dei dati personali nel diritto privato europeo', in V. Cuffaro and V. Ricciuto eds, *La disciplina del trattamento dei dati* (Torino: Giappichelli, 1997), 29, who sees consent as the 'general rule' for the processing of personal data by private persons and public economic bodies; see also G. Comandè, 'Commento agli artt. 11 e 12', in E. Giannantonio et al eds, n 1 above, 133. On the consent in general, cf V. Carbone, 'Il consenso, anzi i consensi, nel trattamento informatico dei dati personali' *Danno e responsabilità*, 23 (1998); D. Messinetti, 'Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali' *Rivista critica di diritto privato*, 350 (1998); F. Cafaggi, 'Qualche appunto su circolazione, appartenenza e riappropriazione nella disciplina dei dati personali' *Danno e responsabilità*, 615 (1998); S. Sica, 'Il consenso al trattamento dei dati: metodi e modelli di qualificazione giuridica' *Rivista di diritto civile*, 621 (2001); S. Niger, 'Il "mito" del consenso alla luce del codice in materia di protezione dei dati personali' *Cyberspazio e diritto*, 499 (2005); A. Fici and E. Pellecchia, 'Il consenso al trattamento' n 1 above, 504; S. Mazzamuto, 'Il principio del consenso e il problema della revoca', in R. Panetta ed, n 1 above, 996; G. Oppo, 'Sul consenso dell'interessato', in V. Cuffaro et al eds, n 1 above, 124.

Self-determination produces an 'intangible entity' suitable to generate utility[7] and to be the object of a right, different from the rights relative to the essential characteristics of natural person (personality rights).

The relationship of personal data to the essential characteristics of the natural person requires consideration of such data as an object of legal protection as such. Consequently the processing and the circulation of personal data must be in compliance with legal requirements that are, mainly, the self-determination of the subject of the data.[8]

[7] Cf G. Resta, 'La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della Carta dei Diritti)' *Rivista di diritto civile*, 808 (2002) according to whom 'whereas the principle of self-determination and the prohibition of commercial exploitation are explicitly accepted with regard to the body and parts of the body, this is not the case with regard to other attributes of the person, especially regarding personal data, which also receives a broad and specific guarantee of protection' ('*mentre rispetto al corpo ed alle sue parti è espressamente affermato, oltre al principio d'autodeterminazione, anche il divieto di sfruttamento commerciale, niente di simile è previsto in relazione agli altri attributi della persona ed, in primo luogo, ai dati personali, che pure sono destinatari di un'ampia e specifica garanzia di tutela*').

[8] Self-determination does not only refer to the power to decide in the initial moment if and how to make information about oneself externally available, but also to the power of control over the further circulation of this data. In Germany the transition from privacy in the sense of a trinomial idea 'person-information-secrecy' to a privacy in the sense of a quadrinomial idea 'person-information-circulation-control' can be traced back to the famous *Volkszählungsurteil*, *Bundesverfassungsgericht* 15 December 1983, 1 BvR 209/83, Neue juristische Wochenschrift, 419 (1984) with comment by S. Simitis, 'Die informationelle Selbstbestimmung – Grundbedingungen einer verfassungskonformen Informationsordnung' *Neue Juristische Wochenschrift*, 398 (1984). To understand the importance attributed to this decision, E. Kosta, *Consent in European Data Protection Law* (Boston: Brill Nijhoff, 2013), 51; P. Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' 38 *American Journal of Comparative Law*, 686 (1989). The abovementioned decision is the first of a series of decisions, confirming the safeguarding approach of the German courts in protecting the person from the technological progress. *Bundesverfassungsgericht* 27 February 2008, 1 BvR 370/07; *Bundesverfassungsgericht* 24 January 2012, 1 BvR 1299/05. In the Italian legal system the same transition happened some years later with the decision '*provvedimento*' of the Italian Data Protection Authority, 13 January 2000; see also Corte di Cassazione 4 January 2011 no 186, *Foro italiano*, I, 1120 (2011) which stated that the right to protect personal data is to be understood as 'one's right to maintain control over his or her information, which not only public figures or celebrities are entitled to, but 'anyone' (…) and 'every person' (…) in the different contexts and areas of life and which contributes to establishing a society respectful of one another and of one's dignity under conditions of equality' ('*diritto a mantenere il controllo sulle proprie informazioni che, spettando non solo alle persone in vista ma a 'chiunque' (…) e ad 'ogni persona' (…) nei diversi contesti ed ambienti di vita, concorre a delineare l'assetto di una società rispettosa dell'altro e della sua dignità in condizioni di eguaglianza*'); see also Corte di Cassazione 5 April 2012 no 5525, *Danno e responsabilità*, 747 (2012) according to which 'data may be stored also for purposes different from the ones originally justifying the processing, including the transfer from one archive to another, as well as being stored on the internet (eg online publications in the historical archives of newspapers). At the same time, the subject of data has a right to control in order to protect the dynamic projection of his own data and social image, which includes the right to ask for contextualisation or an update of the information (even when the information in question is true and *a fortiori* if it is news) and, if necessary, with regard to the purpose of archival storage and underlying interests, to ask for the erasure of the information relating to him or her' ('*se del dato è consentita la conservazione per*

It also must be acknowledged that in some instances personal data does not have an economic value as such. Let us consider, for example, the preferences of a specific consumer, which are useful only when they are processed as a whole, and in connection with the preferences of the other consumers. No one would be interested in buying the personal data of a single consumer.

By contrast, non-personal data is not protected as such, but rather only when it is in an aggregated form. Let us consider, for example, the data relative to the operation of a given device, an appliance that is an individually-owned object. The owner of the object has no rights regarding the operational data except for the personal data regarding his interaction with the object. Only the aggregation of non-personal data produces a good which is suitable to be the object of rights and disposition.

If the no personal data has legal relevance as such, then it is not a good, but an intangible entity which, considered individually, becomes a utility that must be treated with distinct and autonomous protection, in compliance with industrial property, intellectual property, industrial secrets, trade secrets, know how, and so on, and thus cannot be reified or commodified.[9]

Therefore, the use of the same syntagma 'data' must not obscure the fact that the data relating to the natural person is the object of legal protection as such; differently, the non-personal data can be object of protection only if in an aggregated form, as it is unsuitable of generating a utility if singularly considered, with the consequent exclusion of protection as a legal good.

V. Use of Personal Data Not-Intended for Circulation: Some Examples

The above observations, nevertheless, do not prevent consideration of different use of data, one that is finalized or not intended for circulation.

A) Personal data can be offered and consent for its use can be granted in order to ensure the exact execution of a contractual obligation, such that the creditor is required to meet the obligation of co-operation. In these cases, personal data is not intended for circulation and is not the object of the contract.

In particular, let us consider the therapeutic contract between patient and

finalità anche diversa da quella che ne ha originariamente giustificato il trattamento, con passaggio da un archivio ad un altro, nonché ammessa la memorizzazione (anche) nella rete di internet (es., pubblicazione on line degli archivi storici dei giornali), per altro verso al soggetto cui esso pertiene spetta un diritto di controllo a tutela della proiezione dinamica dei propri dati e della propria immagine sociale, che può tradursi, anche quando trattasi di notizia vera – e a fortiori se di cronaca – nella pretesa alla contestualizzazione e aggiornamento della notizia, e se del caso, avuto riguardo alla finalità della conservazione nell'archivio e all'interesse che la sottende, financo alla relativa cancellazione').

[9] Cf A. Appadurai, 'Definitions: Commodity and Commodification', in M. Ertman and J.C. Williams eds, *Rethinking Commodification: Cases and Readings in Law and Culture* (New York: New York University Press, 2005), 35; L. Bianchi, 'Dentro o fuori del mercato? *Commodification* e dignità umana' *Rivista critica di diritto privato*, 489 (2006).

doctor. A doctor cannot perform his contractual obligations with regard to pharmacology, surgery, or a preliminary diagnosis, if he does not pre-acquire patient data, even where the patient lacks legal capacity and so access to the necessary information is provided by a legal representative. The content of the information is closely related to the assessment of the risks related to the medical treatment, so it is in the interest of both sides in the contractual relationship to allow access to such information.

Just as the patient has the right to be informed about the medical treatment he will undergo, following his consent, the doctor must also inform the patient of the possible risks of a procedure and carry out the procedure precisely only if he has the necessary details of the personal data of the patient; otherwise he will incur legal liability for any harm suffered by the patient.

B) Personal data can be offered and consent for its use can be granted in order to ensure an accurate assessment of contractual risk. Again, in this hypothesis, personal data is not intended for circulation and is not the object of the contract.

Let us consider insurance contracts when the insurance company, in order to establish a 'tailor-made' premium, may request specific personal data. This information will not lead to a reduction in the insurance premium, and so does not constitute a part of the counter-performance owed by the insured, as it has been claimed,[10] because this 'tailor-made' premium always works in the interest of the insurer. The insurer can use the data provided to engage in a precise risk assessment and most of all prevent any fraud. It might also operate in the interest of the insured, when the data analysis does not entail a strong risk of discrimination.

C) Otherwise, data can be object of a contract even if is not intended for circulation, in order to assess whether or not a contract can be concluded. The data can also be used to evaluate the reliability of the opposing party in contracts that contain data and information not in the public domain which only the other party can provide.

In particular, let us consider the nondisclosure agreements[11] used to begin

[10] See A. De Franceschi, 'Il «pagamento» mediante dati personali', in V. Cuffaro et al eds, n 4 above, 1382.

[11] C. Rossello, 'Le clausole di riservatezza e i non *disclosure agreements*' *Il diritto del commercio internazionale*, 697 (2014) and in G. Alpa ed, *Le clausole dei contratti del commercio internazionale. Seminario del 20 giugno 2014* (Milano: Giuffrè, 2016), 79; A. Zimatore, 'Note sui cc.dd. accordi di riservatezza', in *Studi in onore di F. Capriglione* (Padova: CEDAM, 2010), 725. With special regard to the protection of trade secrets, cf most recently C. Galli, 'Potenziale perpetuità della tutela del *know-how* e contrattualizzazione degli impegni di riservatezza' *Diritto industriale*, 113 (2018), who states that an appropriate contractualization of privacy obligations is necessary in order to guarantee the protection of trade secrets and the validity of the privacy clauses depends on the provision of a *causa* which justifies the patrimonial attribution determined by them and on the context which they are part of and on their specific content. With regard to *devoir de confidentialité* and in reference to *responsabilité dans les conditions du droit commun*, cf A. Federico, '*Négociations* e obblighi di riservatezza' *Giurisprudenza italiana*, 1315 (2018).

or continue the necessary negotiations for the conclusion of a deal. Only the availability of data that is not readily accessible – containing the organization of the company, rights on tangible or intangible assets, inputs, relationships with suppliers, customers, banks, potential liabilities, litigation and so on – can allow an exact evaluation of the concrete economic operation.

Knowledge of non-public data, through its contractual reference, gives rise to specific behavioral obligations to act in good faith in the negotiation phase. Consequently, this contractual protection is joined to criminal and civil law, not only to the Italian Civil Code (Art 2598) but also to the European Parliament and Council Directive 2016/943 of 8 June 2016 (transposed by decreto legislativo 11 May 2018 no 63) that has amended Arts 623 Penal Code and 98-99 Industrial Property Code and reinforced the protection on scientific and trade secrets. The Paris Union Convention for the Protection of Industrial Property (Art 10 *bis*) and the TRIPs on Trade-Related Aspects of Intellectual Property Rights (Art 39) provide further protection.

D) Furthermore, data can be object of a contract even if is not for circulation, in order to be filed and stored. One example of such a contract would be one involving cloud computing,[12] which offers a remote storage service with access to hardware and software. This kind of contract allows creation, modification and display of content, guaranteeing security of stored data, usually upon payment of a fee.

E) Data can also be used for the conclusion of smart contracts,[13] if translated into algorithms. In these cases, however, data is not the object of the contract and not intended for circulation, but it is instrumental in the configuration of these procedures for concluding the contract. For example, it is possible to conclude a Digital Rights Management contract for the purposes of managing, delivering and accessing certain multimedia services, only if the choice corresponds to

[12] See eg L. Valle et al, 'Struttura dei contratti e trattamento dei dati personali nei servizi di *cloud computing* alla luce del nuovo Reg. 2016/679 UE' *Contratto e impresa/Europa*, 343 (2018). See also D. Mula, 'Il contratto di fornitura di servizi *cloud*', in C. Perlingieri and L. Ruggeri eds, *Internet e Diritto civile* (Napoli: Edizioni Scientifiche Italiane, 2015), 549; M.C. De Vivo, 'Il contratto ed il *cloud computing*' *Rassegna di diritto civile*, 1001 (2013); A. Mantelero, 'Il contratto per l'erogazione delle imprese di servizi di *cloud computing*' *Contratto e impresa*, 1216 (2012). On this topic see also C.A. Rohrmann and J. Falci Sousa Cunha, 'Some Legal Aspects of Cloud Computing Contracts' 10 *Journal of International Commercial Law and Technology*, 1, 37 (2015).

[13] Cf P. De Filippi and A. Wright, *Blockchain and the Law. The Rule of Code* (Cambridge: Cambridge University Press, 2018), 72; B. Carron and V. Botteron, 'How smart can a contract be?', in D. Kraus et al eds, *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Cheltenham, Nothampton: Edward Elgar Publisher, 2019), 101; G. Lemme, '*Blockchain*, *Smart Contracts*, *Privacy*, o del nuovo manifestarsi della volontà contrattuale', in E. Tosi ed, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (Milano: Giuffrè, 2019), 308; P. Cuccuru, 'Blockchain ed automazione contrattuale. Riflessioni sugli *smart contract*' *Nuova giurisprudenza civile commentata*, 107 (2017); D. Di Sabato, 'Gli *smart contracts*: robot che gestiscono il rischio contrattuale' *Contratto e impresa*, 378 (2017).

the value connected to the service purchased. In this way the use of the service is dictated by algorithms that prevent it from being accessed when the deadline has expired or a new smart contract is offered as long as the choice is made within a deadline or by a specific device.

VI. Use of Personal Data Intended for Circulation and Data as a Good

In all these contracts the provision of data is not intended for circulation since it is exclusively instrumental to a particular purpose – with the configuration of contractual liability for all uses aimed to different purposes – or to the conclusion of the contract.

Therefore, the identification of data as a good takes place only in contracts for data circulation, which become tools for configuration of a single digital market.[14] Such contracts allow the realization and the implementation of free flow of data, personal and not, and only in these circumstances they acquire value not individually but only if aggregated. On the contrary, the data assumes an individual relevance, but not value, in those contracts examined above.

VII. The Different Nature of Consent to Data Processing Depending on Their Different Use. Some Examples of Contracts for the Circulation of Data

The traditional doctrinal approach that leads to the right to the protection of personal data within the personality rights – characterized as absolute, non-transferable, and not prescribed by law – usually barred consent when revealing data would lead to contractual value. The modern approach, however acknowledges an authorization[15] which allows the processing of the subject's data without the

[14] Cf A. De Franceschi ed, *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution* (Cambridge: Cambridge University Press, 2016), 1; A. Boerding et al, 'Data Ownership – A Property Rights Approach from a European Perspective' 11 *Journal of Civil Law Studies*, 2, 328 (2018).

[15] For this point of view see D. Messinetti, 'Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali' *Rivista critica di diritto privato*, 350 (1998), who states that the 'subject of the data's consent, characterized as authorization, forms the instrument which has the power to put an end to the intimate data being subject to the logic of repression by every cognitive process taking place' ('*il consenso dell'interessato, nella sua caratterizzazione di permesso autorizzativo, costituisce lo strumento che ha l'efficacia di rendere i dati intimi della persona non più assoggettati alla logica della repressione di qualunque circuito conoscitivo posto in essere*'). Critically, G. Oppo, 'Sul consenso dell'interessato' n 6 above, 124, according to whom describing consent as an authorization does not solve the problem of the legal qualification 'because it still requires establishment of the impact of the 'authorization' in the legal sphere of the one who gives it. Where does this impact come from if not from an act of will? Is it consequently an act of disposition?' ('*perché si tratta comunque di giudicare della*

natural person losing his essential characteristics.

If we can consider consent as authorization for those contracts where personal data is exclusively instrumental to a particular purpose, it is not simply an authorization but becomes consent with contractual value if that consent is for the circulation of personal data. The principle of the free flow of personal data allows any natural person, within regulatory limits, to give the right of use,[16] for a consideration or free of charge, of his personal data in accordance with the specific aims underlined in the act of disposition. The contractual clause considers personal data as part of an exchange, in other words a remuneration for services, such as access to online platforms.

A) Let us consider contracts concluded between online service providers and users and, in particular, the economic transaction through which the user, in order to have access to network research, websites and social networks, allows the collection, use and sharing of his personal data. An exchange takes place between the operator of the search engine, website or social site and the user, not only on a '*de facto*' level or in a merely economic sense, but also 'in legal terms'.[17]

incidenza della "autorizzazione" nella sfera giuridica di chi la concede. Questa incidenza da che può essere determinata se non da un atto di volontà? Si tratta allora di un atto di disposizione?'). According to S. Mazzamuto, n 6 above, the essence of the authorization is not only to legitimate the processing of data, but also to regulate cases of circulation of data with regard to the development of personality without acts of dispositive nature.

[16] Cf V. Cuffaro, 'A proposito del ruolo del consenso' n 1 above, 121; V. Zeno Zencovich, 'Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali' *Rivista trimestrale di diritto e procedura civile*, 740 (1998); G. Resta and V. Zeno Zencovich, 'Volontà e consenso nella fruizione dei servizi di rete' *Rivista trimestrale di diritto e procedura civile*, 412 (2018).

On the more general topic of data as a legal asset see, P. Perlingieri, 'L'informazione come bene giuridico' *Rassegna di diritto civile*, 331 (1990), who states that 'the relevance of an asset rises not only from the holding of an interest and the protection accorded to its holder, but also when the asset's protection is given to qualified third parties getting (not only economic) utilities from keeping it. This means that not only patrimonial, but also non patrimonial assets, ie assets which are protected independent of their economic relevance, may be legally relevant. The relevance may also arise from the regulation of the asset's circulation, the modalities of access, or from the regulation of the facts regarding it' ('*la rilevanza di un bene è data non soltanto dalla titolarità dell'interesse in cui si sostanzia e nella protezione riservata al titolare ma anche quando la tutela del bene è riservata a terzi qualificati che ne ricavano comunque un'utilità, e non necessariamente economica, dalla conservazione del bene medesimo" e quindi sono "giuridicamente rilevanti non soltanto i beni patrimoniali ma anche quelli non patrimoniali; cioè quelli che sono protetti a prescindere dalla loro eventuale rilevanza economica. La rilevanza si può configurare anche nel regime di circolazione del bene, delle modalità di accesso, ovvero nel regime delle vicende che lo interessano*').

[17] C. Perlingieri, *Profili civilistici dei social networks* (Napoli: Edizioni Scientifiche Italiane, 2014), 88-89. Subsequently, the continuing increase in contracts concluded online with regard to the exchange and the processing of data is highlighted by C. Langhanke and M. Schmidt-Kessel, 'Consumer Data as Consideration' *Journal of European Consumer and Market Law*, 218 (2015); M. Schmidt-Kessel and A. Grimm, 'Unentgeltlich oder entgeltlich? Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten' *Zeitschr für die gesamte Privatrechtswissenschaft*, 84 (2017); A. De Franceschi, 'Il «pagamento» mediante dati personali' n 10 above, 1381.

This definition is confirmed by:

a) analysis of clauses that recur within the principal search engine and social networks' terms and conditions of use, according to which the user grants the operator of the search engine or social network a non-exclusive, transferable licence over IP content, which may in turn be transferred as a sub-licence, free from royalties, and valid throughout the world, as consideration for the personal, global, royalty-free, non-transferable, and non-exclusive licence which the operator grants to the user in order to use the software provided by the search engine or the social network. The waiver of privacy rights and personal data is in return for gaining access to the search engine or social network platform. The user has the right to use the platform – and the operator is obliged to consent to the usage – on the grounds that the operator is permitted to collect and exploit the user's personal data. This conclusion raises serious doubts about the claim that the operator is not obliged to provide the service and does not have to ensure the correct functioning of the search engine, website and social network platforms as the services amount to the consideration for the licence granted to the user.

b) Art 7.4 GDPR, by virtue of which,

> 'when assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract'.[18]

c) the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content,[19] which allows the consumer to choose how to fulfill his

[18] See Corte di Cassazione 2 July 2018 no 17278, *Guida al diritto*, 42, 75 (2018) which stated that the consent must be freely given, it must not be tied to any conditions, it must be informed, which requires exhaustive and appropriate information to be provided beforehand, it must be specific, meaning that it has to be given for one or more specific purposes, it must not be intended for any indiscriminate collection of personal data, it must be unambiguous, with regard to the processing of sensitive data and decisions based on automated processing, included profiling according to Arts 9 and 22 of the European Regulation EU 679/2016 GDPR it also needs to be explicit. Thus, an operator of a website, who provides a fungible service, which can be renounced by the user without greater difficulties (in this case, a newsletter service on issues related to finance, taxes, law and labour), may tie the provision of the service to the consent to the processing of personal data for advertising purposes under the condition that the consent is separately and unequivocally given with regard to this effect and that the product sectors or services the advertisement will be related to are listed. On this point F. Bravo, 'Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto' *Contratto e impresa*, 34 (2019).

[19] Cf, most recently, the European Parliament legislative resolution of 26 March 2019 on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and services [COM(2015)0634 – C8-0394/2015 – 2015/0287(COD)] and the Position of the European Parliament adopted at first reading on 26th March 2019 regarding the adoption of the directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply

obligation by paying the price[20] or by a non-pecuniary counter-performance in the form of personal data or any other data (Art 3). Under these terms it is possible to imagine the exclusion of enforcement of the GDPR because the data becomes a good and so it will be separated from the protection of the natural person following the act of waiver.

d) the Draft Common Frame of Reference (DCFR)[21] which applies to contracts conferring, in exchange of a price or gratuitously, rights to information or data, including software and databases (Book IV, Section A, Chapter 1, Art 101; Book IV, Section H, Chapter 1, Art 103).

e) The hypothesis regarding data transfer as an exchange and so the consent to contractual value, is also confirmed in the absence of necessary conditions to qualify consent as an authorization with regard these contracts between the operator of web and the user.

As underlined by Art 7 GDPR[22] and in consideration of the 'Territorial scope' of Art 3 GDPR, consent must be autonomous, informed, specific, unequivocal, and explicit when processing special categories and for decisions based solely on automated processing, including profiling (Arts 9 and 22 GDPR). These conditions for consent are absent when operators of search engines, websites and social networks collect personal data.

These operators condition the use of network services on the release of data; data is used for a different purpose than the one that justified its collection; the informative and the consensual profile is not separated, as is evident from the pages of the main search engines, websites and social networks when data and

of digital content and services (P8_TCI-COD(2015)0287), available at https://tinyurl.com/yhq84y5g (last visited 30 December 2019).

For some criticism see A. De Franceschi, 'Il «pagamento» mediante dati personali' n 10 above, 1410, according to whom the proposal only adresses certain aspects of the topic 'paying with data', providing for solutions which are not completely consistent with the existing law ('*per quanto concerne alcuni aspetti limitati ed, in relazione a quelli, non contiene soluzioni del tutto coerenti e soprattutto coordinate con il diritto vigente*').

[20] According to Art 7 para 2 of the Position of the European Parliament adopted at first reading on 26 March 2019 regarding the adoption of the directive (EU) 2019/770 of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content and services [P8_TCI-COD(2015)0287] 'price' means 'money or a digital representation of value that is due in exchange for the supply of digital content or a digital service'.

[21] Cf G. Magri, 'L'armonizzazione del diritto privato europeo attraverso il DCFR', in P. Gallo et al eds, *L'armonizzazione del diritto europeo: il ruolo delle corti* (Milano: Giuffrè, 2017), 87; G. Alpa and G. Iudica eds, *Draft Common Frame of Reference (DCFR), what For?* (Milano: Giuffrè, 2013), 1; M. Maugeri, 'Alcune perplessità in merito alla possibilità di adottare il Dcfr (*draft common frame of reference*) come strumento opzionale (o facoltativo)' *Nuova giurisprudenza civile commentata*, 253 (2011); U. Breccia, 'Principles, definitions e model rules nel 'comune quadro di riferimento europeo' (draft common frame of reference)' *Contratti*, 95 (2010); H.W. Micklitz and F. Cafaggi eds, *European Private Law After the Common Frame of Reference* (Cheltenham, Nothampton: Edward Elgar Publisher, 2010) 1.

[22] Cf eg F. Caggia, 'Libertà ed espressione del consenso', in V. Cuffaro et al eds, n 4 above, 257-267; F. Bravo, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro ed, n 4 above, 157-161.

cookies policies are published. In these cases they simply inform the user regarding the processes by which such companies 'collect, use, and share data' and 'use cookies or similar technologies' and require users to confirm 'having read the data and cookies policies'. By contrast a user can decline certain uses of his or her data, by changing the privacy defaults, an option that was only recently included by the main social networks in order to comply with the GDPR (Art 25).

B) Contracts with data brokers that collect information online from public sources (for example, Land Registries, Income Revenue Authorities, Public Automobile Registries, Registries of Companies and so on) are particularly interesting. The data brokers select, analyze, evaluate, organize and give licence to third parties to use this information within the data market. This contract concluded between the data broker and the customer, who is a user of the result who does not have a direct relationship with the subjects of the data, should not give rise to problems in terms of the GDPR because the personal data processed is public; it is made public by public administrations to meet transparency obligations.

However, the fact that such data is easily accessible does not mean that it is also freely reusable by anyone and for any purpose. The enforcement of the principle of purpose (Art 5.1.b GDPR) does not allow the reuse of data if it is incompatible with the original purposes for which the data is public: examples of uses that might be barred include the reuse of contact details of state employees for marketing or campaign purposes or the repurposing of personal data from the Public Automobile Register, and others.

Moreover, the data broker cannot lawfully justify the processing based on the legitimate interests of the entity in control of the data (Art 6.1.f GDPR). In order for such a justification to be possible, the interest of the entity in control of the data, even if legitimate, would have to prevail over the fundamental interests, rights and freedom of the subjects of the data. In this regard Opinion 06/2014 of Working Party 29 on the notion of legitimate interests of the data controller under Art 7 of European Parliament and Council Directive 95/46/EC[23] is confirmed. The legitimate interest of the controller to be aware of the preferences of his customers in order to create targeted advertising and personalized offers, does not involve monitoring their online and offline activities and creating complex personality profiles with the collaboration of data brokers.

In the age of Big Data it is complicated to provide adequate information to the subject of the data on the purposes of processing that are unknown when the data is collected. Therefore, if the data is personal and public, the process of data collection must take place within the limits of the purpose for which it has been made accessible to the public; if the data is personal and non-public without the conditions of lawful processing – including consent and legitimate interest – massive personal data processing can happen only through the enforcement of

[23] See https://tinyurl.com/y999oddq (last visited 30 December 2019).

two rules of GDPR: 1) Art 6.4, which permits the processing, for a purpose other than that for which the personal data has been collected without the subject's consent, if the controller considers: a) any link between the purposes for which the personal data has been collected and the purposes of the intended further processing; b) the context in which the personal data has been collected, in particular regarding the relationship between the subjects of the data and the controller; c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Art 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Art 10; d) the possible consequences of the intended further processing for subjects of the data; e) the existence of appropriate safeguards, which may include encryption or pseudonymisation; and 2) Art 89, which permits the renunciation of measures of pseudonymisation if these are incompatible with the purpose of archiving in the public interest, statistics and scientific or historical research for which it is sufficient that the data is only minimized.

Massive processing of personal data, therefore, must be carried out in respect of accountability, privacy by design and privacy by default and must be subject to a Data Protection Impact Assessment. In this regard the GDPR introduces a legal regime strongly characterized by the need to ensure the free flow of data while balancing its protection and security by offering rules to tackle the new problems generated by Big Data. Consequently, I cannot agree with the recent assertion by Italian academics that

> 'the GDPR remains imprisoned in the individual perspective that since the beginning has characterized the legal regime governing the processing of personal data but which is inadequate in the face of the superpersonal dimension of Big Data'.[24]

Otherwise, if the data processed by the data brokers are non personal, their treatment is regulated, as discussed above, by the legal regime of scientific or trade secrets.

VIII. Concluding Remarks

In conclusion, the sharing of a case method of analysis has allowed the analysis of the different contractual models inherent to data and that have stemmed from the use of new technologies. When the good, object of the contract, has been identified, it can be stated that only contracts for the movement

[24] See A. Iuliani, 'Note minime in tema di trattamento di dati personali' *Europa e Diritto Privato*, 298 (2018). The following authors share this approach F. Piraino, 'Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' *Le nuove leggi civili commentate*, 378 (2017); A. Mantelero, 'Responsabilità e rischio nel Reg. UE 2016/679' *Le nuove leggi civili commentate*, 144 (2017).

of data, personal or non, when data acquires a value not in its singularity but aggregated, confirm the now famous phrase '*personal data is the new oil of the internet and the new currency of the digital world*'[25] in the knowledge that the automated processing of personal data is still a human treatment by automated means and as such a source of liability.

[25] M. Kuneva, *Keynote Speech. Roundtable on Online Data Collection, Targeting and Profiling*, Brussels, 31 March 2009. See also European Commission, *Building a European Data Economy*, 2, COM (2017) 9 final of the 10 January 2017: '(d)ata has become an essential resource for economic growth, job creation, and societal progress'.