Iorio C, 'Legal issues concerning the circulation and processing of data in the digital age' (2022) 2 EJPLT, 153-168.
DOI: https://doi.org/10.57230/ejplt222CI

EJPLT
ISSN 2704-8012

Legal issues concerning the circulation and processing of data in the digital age.

CHIARA IORIO
Postdoctoral Research Fellow
Università degli Studi di Macerata

Abstract

This paper focuses on some of the most controversial issues concerning the circulation of personal data. The legal nature of personal data will be framed. Then, the liability regime pursuant to Article 82 GDPR will be examined, with particular reference to data breach committed by an Internet service provider and in the context of a Blockchain.

Il presente contributo si propone di esaminare alcune delle questioni più controverse e attuali in materia di circolazione dei dati personali. Prendendo le mosse dall'inquadramento della natura e delle modalità di circolazione dei dati, sarà indagato il regime di responsabilità di cui all'art. 82 GDPR, con particolare riguardo all'illecito commesso dall'internet service provider, o nell'ambito di una Blockchain.

Keywords: data processing; liability; internet service provider; blockchain; digital services act; digital market act.

Introduction[1].

In the digital age, the centrality of personal data is indisputable. Data have acquired a multifunctional dimension, where the boundary between the public and the private sphere is blurred.[2] Data are not only a personal attribute, but also a means for the State to control their respective owners thanks to the use of technology and, therefore, a tool for exercising power. Consequently, many authors are discussing the rise of a "datacracy",[3] as well as a "datification".[4]

This is the reason why a detailed regulation of the use and circulation of data at a European level has been considered necessary in the recent "Digital Services" package, for protecting online users and stimulating innovation.

This paper aims to examine some of the most controversial legal issues in this area with specific regard to the Italian system. The regime of liability as referred to in Art. 82 GDPR will be analyzed starting from the classification of the nature and the circulation of data with particular focus on the damage caused by an internet service provider, or within a Blockchain.

1. The nature of personal data between fundamental rights and economic asset.

The plurality of regulations which have recently been affecting personal data confirms the centrality that data have assumed in the current technological society and highlights multiple legal issues.

The need for a differentiated disciplinary approach to this matter derives from the ambivalent nature of the personal data, which can be considered an

[1] This article has been written within the "TRUST - digital TuRn in EUrope: Strengthening relational reliance through Technology" Project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101007820. This article reflects only the author's view and the REA is not responsible for any use that may be made of the information it contains.

[2] Some authors have long sustained the opportunity to overcome the dichotomy between public and private: see P Perlingieri, 'L'incidenza dell'interesse pubblico sulla negoziazione privata' [1986] Rass dir civ, 57.

[3] See D De Kerckove, 'Mobile Culture in Singapore: from Democrature to Datacracy', in A Serrano (ed.), Between the Public and the Private in Mobile Communication (Taylor & Francis, 2017) 25; S Ranchordas, 'Citizens as Consumers in the Data Economy' (2018) 14 EuCML, 154.

[4] See S Calzolaio, 'Protezione dei dati personali', Dig. disc. pubbl. (Utet giuridica, 2017) 594.

"asset" and as a "fundamental right" at the same time, depending on the chosen approach.

According to the first point of view (the "mercantilist" one), data can be considered an "asset" with an economic value capable of being exchanged contractually. This theory is based on the observation of the economic reality, in which digital content or digital services are often supplied in a way that the consumer does not pay a price but provides personal data to the trader.[5]

The second approach (the "personalistic" one) refuses to compare data to money, noting that the protection of personal data is included among the fundamental rights by Art. 8 of the EU Charter[6]. According to this perspective, data cannot circulate as wealth, but can be seen as an attribute of the person and the foundation of a new conception of the right to "privacy".[7] Privacy indeed can no longer be considered in the "negative" meaning of the "confidentiality" claimed by the individual concerning invasions of the private sphere (especially towards the press)[8] but is to be seen in the (positive) sense of the right of each person to exercise effective control over the data entered in the network.[9]

The tension between the two opposing views about the nature of the data emerges in the legislative process of Directive (EU) 770/2019 concerning contracts for the supply of digital content and digital services.[10] Indeed, in the text of the proposal[11], the conferral of access to personal data by the consumer was expressly qualified as "counter-performance other than money".

---

[5] V Ricciuto, 'Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali (2020) 3 Riv dir civ, 642; see also A De Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Esi, 2017) 10. With specific reference to access to social network by means of consent to data processing, see C Perlingieri, *Profili civilistici dei social networks* (Esi, 2014) 80. See also K E Davis & F Marotta-Wurgler, 'Contracting for Personal Data' (2019) 94 N.Y U. Law Rev, 662.S Spiekermann and others, 'The Challengesof Personal Data Markets and Privacy' (2015) 25 Electron Markets, 25.

[6] See G Gonzlez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) 55; J Dai, 'On the Right to the Protection of Personal Data as a Constitutional Right' (2021) 20 J. HUM. Rts., 851.

[7] On the evolution of the concept of privacy see V Cuffaro, 'Il diritto europeo sul trattamento dei dati personali', (2018) 3 Contr impr,1098; G Visintini, 'Dal diritto alla riservatezza alla protezione dei dati personali' [2019] Dir inf e informatica, 1.

[8] G Giampiccolo, 'La tutela giuridica della persona umana e il c.d. diritto alla riservatezza' [1958] Riv trim dir e proc civ, 458; G Pugliese, 'Il diritto alla riservatezza nel quadro dei diritti della personalità' [1963] Riv dir civ, 605; P Rescigno, 'Il diritto all'intimità della vita privata', in *Studi in onore di F. Santoro-Passarelli* (Jovene, 1972) 121.

[9] S Rodotà, 'Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali' [1997] Riv crit dir priv, 583; G Finocchiaro, 'Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali', in G Finocchiaro (ed), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, (Zanichelli, 2019) 5.

[10] For a detailed analysis of the Directive, see C Camardi, 'Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali' [2019] Giust civ, 499; J M Carvalho, 'Sale of Goods and Supply of Digital Content and Digital Services - Overview of Directives 2019/770 and 2019/771' (2019) 5 EuCML, 194; K Sein, G Spindler, 'The new Directive on Contracts for the Supply of Digital Content and Digital Services - Scope of Application and Trader's Obligation to Supply' (2019) 15 ERCL, 257; B Gsell, R Araldi, 'Time Limits of Remedies for Hidden Defects under under Directive (EU) 2019/770 on Contracts for the Supply of Digital Content and Digital Services and Directive (EU) 2019/771 on Contracts for the Sale of Goods' (2020) 12 Cuadernos de Derecho Transnacional, 475; C Cauffman, 'New EU Rules on Business-to-Consumer and Platform-to-Business Relationships' (2019) 26 Maastricht J Eur & Comp L, 469.

[11] See G Spindler, 'Contracts For the Supply of Digital Content - Scope of Application and Basic Approach - Proposal of the Commission for a Directive on Contracts for the Supply of Digital Content', (2016) 12 ERCL, 183; F Zoll, 'The remedies in the Proposals of the Only Sales Directive and the Directive on the Supply of Digital Content' (2016) 5 J Eur Consumer & Mkt L, 250.

The final version of the Directive rejects the equivalence between personal data and goods. In compliance with the comments given by the European Data Protection Supervisor[12], the Directive formally excludes that access to digital content through the transfer of personal data can be qualified as a bilateral contract.[13] Art. 3 distinguishes between case (a) where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price; and case (b) where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader.

Although the Directive shall apply to both cases, hypothesis (a) is expressly qualified as a "contract", while hypothesis (b) is generally referred to as a case "where" the supply takes place.

And yet, despite the wording of the provision, the two hypotheses are not differently regulated, from a substantial point of view. The directive extends, indeed, the application of remedies for non-conformity also to case (b).

In the same sense, should be seen also Directive (EU) 2161/2019[14], whose recital No. 31 highlights the "similarities" and the "interchangeability" of paid digital services and digital services provided in exchange for personal data, and therefore states that they should be subject to the same rules under that Directive.

In this regard, it is also worth mentioning the Art. 3-bis, Dir. (EU) 2011/83[15], which provides for the application of the Directive also to cases where the trader supplies digital services and the consumer gives access to its data.

These regulatory solutions comply with the legal theory and are consistent with the effective dynamics of the traffics in the net.

It is certainly undeniable that the protection of personal data is a component of the rights of the individual. However, it cannot be excluded that the consent to their processing as a condition for the use of digital services gives rise to a negotiation involving consideration.

More specifically, as observed by some authors, in such cases the processing of data becomes an element of a complex contractual situation, in which there is a dual expression of consent: consent to the use of the digital service in the absence of payment of a price in money, on the one hand, and consent to access to data, on the other.

---

[12] EDPS, Opinion 4/2017, in www. edps.europa.eu stated that '[F]undamental rights, such as the right to the protection of personal data, cannot be reduced to mere consumer interests and personal data cannot be considered a mere commodity'.

[13] According to recital n. 24 '[T]he protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity'.

[14] European Parliament and Council Directive 2019/2161/EU of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L 328/7.

[15] European Parliament and Council Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJL 304/64.

The two acts of "consent" [16] cannot be studied independently, being functionally connected. In other words, the consumer's consent to processing is justified precisely in relation to the supply of the service by the trader. In this way, consent to data processing can be seen as the consideration of the negotiation. [17] Therefore, a bilateral contract is configured in the case examined.[18] It should be clarified that this contract cannot be qualified as a "purchase" agreement.[19] Given the peculiarity of personal data (which pertains to a fundamental right), they cannot be definitively ceded to other parties. In this direction, we should remind that Art. 7, par. 3, GDPR states that the data subject has at "any time" the right to withdraw his consent.

We could conclude that the consumer cannot cede the data, but he can transfer the right of economic exploitation of the data, through a negotiation scheme that, according to some authors, could be qualified in terms of a "license".[20]

Moreover, it should be noted that the recognition of the commercial nature of data entails more effective protection for the data subject.

Let us think of the applicable remedies.

The personalist approach should lead to the application of the sole remedies provided for the rights of the personality and in the GDPR, while the discipline regarding patrimonial phenomena (such as the remedies provided for in the matter of unfair commercial practices) could not be applicable.

---

[16] Legal nature of 'consent' is highly debated by the scholars: some authors consider it as a negotial consenus: V Cuffaro, 'A proposito del ruolo del consenso', in V Cuffaro and others (eds), *Trattamento dei dati e tutela della persona* (Giuffré, 1999) 121; G Oppo, '«Trattamento» dei dati personali e consenso dell'interessato", in G Oppo, *Scritti giuridici*, VI, *Principi e problemi del diritto privato* (CEDAM, 2000)113. Other scholars consider it as a legal act in the strict sense: S Patti, 'Il consenso dell'interessato al trattamento dei dati personali' [1999] Riv Dir Civ, 455 qualifies ita as a form of "justification". F Bravo, 'Lo «scambio di dati personali» nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto' [2019] Contr impr, 34 qualifies it as merely authorizing act; R Messinetti, 'Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali' [1998] Riv crit Dir priv, 35, has the same opinion. See also C. Solinas, 'Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette' [2021] Giur it, 320.

[17] See V Ricciuto, 'Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali', (2020), 652: "[T]he economic function, in short, is to realize, concretely and beyond the schemes used, an exchange, even where the contractual scheme is apparently free". Differently, for C Camardi, 'Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali' [2019], 550, the contractual operation can be seen as a supply of digital goods/services with a 'free structure', which is linked to an act of transfer of personal data by the consumer for non-commercial purposes that cannot be considered as consideration.
In case law, see the decision of the Italian Consiglio di Stato of 29 March 2021, n. 2631, GiustizaCivile.com, with comment by V Ricciuto and C Solinas, 'Supply of digital services and provision of personal data: firm points and ambiguities on the equivalence of the contract'. The decision rules that the services of the social network Facebook are '[P]romised as free, but, evidently, are not free, ending up representing the «consideration» of the provision of personal data of the individual user for commercial purposes'.

[18] See also C Perlingieri, *Profili civilistici dei social networks* (Esi, 2014), 88. The author states that "[T]he disposition of privacy and personal data is in function of the use of the platform, so that by virtue of the synallagma, the user has both the right to use the platform - and the social is obliged to allow its use - as the social can collect and exploit personal data. Also A De Franceschi, *La circolazione dei dati personali tra privacy e contratto* (Esi, 2017), 75 affirms the nature of a contract for consideration.

[19] But Tar Lazio of 10 January 2020, n. 260, Giur it, 2021, 320, qualified it as a purchase agreement.

[20] V Zeno-Zencovich, 'Do "Data Markets" Exist?' [2019], 26. See also on this matter V Ricciuto, 'Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali' (2020), 656: '[T]he rights which are transmitted or acquired by the data controller may be of different types, non-exclusive enjoyment, economic exploitation, transformation in order to create additional data through, for example, profiling, etc'.

Otherwise, the full application of the consumer discipline cannot be excluded when we assume that personal data can circulate for commercial purposes.

Thus, in the (very frequent) cases where the trader does not inform the consumer of the profiling of his data for commercial purposes, an unfair commercial practice (according to Articles 20, 21, and 22 of the Italian Consumer Code) or an aggressive practice (according to Article 20, 24 and 25 of the Italian Consumer Code) could be configured.

In this way, there is the overcoming of the logic of the "watertight compartments" of protection. At the same time, a new conception of "multi-level protection"[21] is embraced, which is able to ensure effective protection of the rights of an individual, in the event that a very personal right is exploited for commercial purposes, even independently of the will of the interested party.

2. Data processing liability.

Another controversial issue concerns the reconstruction of the liability regime deriving from the processing of data, currently regulated by Art. 82 GDPR.

As well known, this subject was previously regulated in Italy by Art. 15 of the Legislative Decree 196/2003 (the so-called "Privacy Code"), which stated that "Any person causing harm to others as a result of treatment of personal data is liable to compensation under Article 2050 of the Civil Code".

The reference to Art. 2050 has been variously interpreted by scholars.

According to most authors, it was a classic hypothesis of non-contractual liability, according to the general regime as provided for in Article 2043 of the Civil Code.[22] Other lawyers qualified it as a special form of tortious liability.[23] According to the minority of the scholars, Article 15 provided for a hypothesis of contractual liability, since the reference to Art. 2050 had to be interpreted as referring only to the probative rule established therein.[24]

---

[21] Consiglio di Stato of 29 March 2021, n. 2631 speaks about a "multi-level protection" and rejects the argument that the only GDPR legislation should be considered applicable - because of its alleged specialty - with the effect of excluding the applicability of any other legal framework. Without prejudice to the centrality of the GDPR, the Consiglio di Stato excludes the possibility that, in this matter, "protective watertight compartments" may be identified. It follows that '[W]hen the processing involves conduct and situations governed by other legal sources to protect other values and interests (as important as the protection of data relating to the natural person), the legal system cannot allow any disapplication of other sector disciplines (...) to reduce the safeguards granted to natural person'.

[22] According to this interpretation, in particular, the source of liability would still be unfair damage (where the meritorious subjective situation of the injured person would have to be assessed on a case-by-case basis) caused by intentional or negligent conduct. See F Caringella, 'La tutela aquiliana della privacy nel codice per la protezione dei dati personali (d. lgs. n. 196/2003)' in *Studi di diritto civile. III. Obbligazioni e responsabilità* (Giuffré, 2005) 715.

[23] V Roppo, 'La responsabilità civile per trattamento di dati personali' [1997] Danno resp, 663.

[24] F D Busnelli, 'Itinerari europei nella «terra di nessuno tra contratto e fatto illecito»: la responsabilità da informazioni inesatte' [1991] Contr impr, 539; C Castronovo, 'Situazioni soggettive e tutela nella legge sul trattamento dei dati personali' [1998] Eur dir priv, 656; C Scognamiglio, 'Buona fede e responsabilità civile' [2001] Eur dir priv, 357; E Pellecchia, 'La responsabilità civile per trattamento dei dati personali' [2006] Resp civ prev, 221.

The question arises again in light of the text of the GDPR, which is the result of the mediation between the different legal cultures of the Member States.[25] Article 82 of GDPR establishes that "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"[26].

Although the wording of the provision may call to mind Art. 2043 of our Civil Code, a more careful analysis reveals the inadequacy of a unitary reconstruction of the provided liability.[27]

First of all, we can distinguish between the regime of liability of the controller and that of the processor. According to the second paragraph of Art. 82, indeed, any controller involved in processing shall be liable "for the damage caused by processing which infringes this Regulation". The processor shall be liable for the damage caused by processing (a) where "it has not complied with obligations of this Regulation specifically directed to processors" or (b) where "it has acted outside or contrary to lawful instructions of the controller".

We can assume that the liability of the data controller can be qualified as having a contractual nature, while the liability of the data processor has a contractual nature only in case (a).

In order to understand this assumption, it is essential to clarify the radical change of structure of the GDPR, if compared to the "old" Directive (CE) 95/46.[28]

The most recent regulation, indeed, provides for a series of detailed obligations in respect of data controller and data processor[29], aimed at ensuring the lawfulness of the processing and, therefore, at protecting the rights of the data subject (according to art. 5 GDPR). In this way, the principle of "accountability" is implemented, which pursues an "ex-ante" approach, in order to prevent the risk of damage to the data subject.[30]

---

[25] F Bravo, 'Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali', in N Zorzi Galgano (ed) *Persona e mercato dei dati. Riflessioni sul GDPR* (Wolters Kluver, 2019) 393, stresses that, in the force of existing regulations, domestic legal categories must give way to European ones, in the dynamics of 'droit pluriel'.

[26] On the nature of the liability provided for in Art. 82 GDPR see: A B Menezes Cordeiro, 'Civil liability for processing of personal data in GDPR' [2019] Eur. Data prot. Law Review, 492. About liability for data breach, see also J P Kesan & C M Hayes, 'Liability for Data Injuries' (2019) 1 U Ill L Rev, 295; K Nekit, D Kolodin & V Fedorov, 'Personal Data Protection and Liability for Damage in the Field of the Internet of Things' (2020) 10 Juridical Trib, 80.

[27] Among the first interpretations of art. 82 GDPR, it is widespread, however, the qualification of liability arising from data processing as non-contractual. *Ex multis*, see M Gambini, *Principio di responsabilità e tutela aquiliana dei dati personali* (Esi, 2018) 124; E Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale* (Giuffré, 2019) 49.

[28] On the directive, see C M Bianca and F D Busnelli (eds) *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, (Cedam, 2009); V Cuffaro and others (eds), *Il Codice del trattamento dei dati personali* (Giappichelli, 2007); See also S Sica and P Stanzione (eds), *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196* (Zanichelli, 2005).

[29] Consider, *ex multis*, the obligations relating to the adoption of security measures, referred to in art. 24, 25 and 32; to the obligations deriving from the application of the rights of the interested party, referred to in art. 12-22; the provisions relating to informed consent, referred to in art. 6, par. 1 lett. a) and 9, par. 1, lett. b).

[30] See M Renna, 'Sicurezza e gestione del rischio nel trattamento dei dati personali' [2020] Resp civ prev, 1343.

Since the data controller and processor are burdened with heavy obligations to fulfill, we can conclude that a contractual relationship between them and the data subject arises.[31]

It follows that, where, as a result of the infringement of the Regulation (Art. 82), the data subject suffers damage, a contractual liability according to Art. 1218 C.C. will be configured.

Such a solution seems easy to be argued if the subjects are already part of a contractual relationship where the treatment is necessary "for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (Art. 6, paragraph 1, lett. b).

We could reach the same conclusion in cases where the data subject gives specific consent to the processing of data, or in other cases where Art. 6 acknowledges the existence of a "legitimate legal basis" for processing. In fact, the set of information (Art. 12, 13, 14) and security (Art. 32) obligations that are imposed on the data controller (and, in some cases, also on the data processor) exclude that the data controller could be considered just as a "passer-by"[32], i.e. a "quivis de populo" which is only burdened with a generic duty of "neminem laedere".

The applicability of Art. 2043 c.c., indeed, requires that the relationship between the damaging party and the damaged one is created when the damage occurs. Differently, in the case of data processing, we can notice the existence of obligations for the data controller, which are pre-existing with respect to the damage.

We can conclude that GDPR codifies "ex lege" obligations to be included in the "variae causarum figurae" referred to in Art. 1173 c.c.. It means that, in case of their infringement, a classic hypothesis of liability deriving from a breach of an existing obligation is configured.

Therefore, a non-contractual liability could be configured just in two residual cases: a) where the processor "has acted outside or contrary to lawful instructions of the controller", as , in such a case, there is no legal relationship between the data processor and the data subject;[33] b) where the processing is carried out by a person who cannot be qualified as data controller or processor,[34] or outside the existence of a legitimate basis, according to Art. 6 GDPR.

On a disciplinary level, Art. 82 exempts the controller and the processor from liability if it proves "that it is not in any way responsible for the event giving rise to the damage".

---

[31] Cfr. F Piraino, 'Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' [2017] Nuove leggi civ comm, 369; Similar is the opinion of F Zecchin, ' Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali' [2022] Eur dir priv, 517.

[32] The theorizing of non-contractual liability as the liability of the "passerby" is due to Carlo Castronovo. See C Castronovo, *Responsabilità civile* (Giuffré, 2018), 551.

[33] The data processor indeed, is subject to liability (pursuant to the second paragraph of art. 82 GDPR) in the event that "it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. See R Bravo, 'Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali' (Wolters Kluver, 2019), 383.

[34] This qualification, in fact, triggers the set of obligations of conduct that leads to the affirmation of the existence of a mandatory relationship.

This provision recalls the wording of Art. 1218 Civil Code and implies a presumption of the existence of the causal link. Once the existence of the damage has been demonstrated and the breach has been alleged, a reversal of the burden of proof is triggered.

Finally, it should be pointed out that the abovementioned obligations of conduct laid down in the Regulation are purely procedural in nature[35] and do not, therefore, confer immediate utility on the data subject. It follows that the award of damages presupposes, in any event, the proof of a "material or non-material" damage suffered by the damaged party.

In the case, however, in which a non-contractual liability is configurable, compensation is subject to proof of the injustice of the damage, given that, under the general theory of tortious liability, we have to exclude the hypothesis of "in re ipsa" injustice.[36]

3. The internet service provider's liability for data processing.

When unlawful processing of data takes place in the context of the supply of an information society service even more issues arise.

The GDPR (Art. 2, paragraph 4) expressly does not affect the application of Directive 2000/31/EC, with particular regard to the liability rules of intermediary service providers in Articles 12 to 15 of that Directive. Therefore, there is a need for coordination between the two disciplines.

As well known, the so-called "e-commerce" Directive set a special regime of liability for internet providers, intending to encourage the expansion of the digital market.[37]

As a result, a set of exemptions of liability has been laid down, depending on the activity carried out by the provider.[38] Moreover, there are not obligations of active conduct for the provider.[39]

---

[35] See F Piraino, 'Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato' [2017] 390.

[36] Under the old Privacy Code, the case law frequently sated the '[T]he non-pecuniary damage [...] does not escape verification of the 'severity of the injury' and the 'seriousness of the damage'. Cass. 8th February 2017 n. 3311, in *DeJure*; Cass. 5th September 2014 n. 18812; Cass. 15th July 2014 n. 16133.

[37] It should be clarified that the very recent Digital Services Act [European Parliament and Council Regulation 2022/2065/EU of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC [2022] OJL 277/1], which will apply from 17 February 2024, regulates the liability of providers in a way which is substantially similar to the old e-commerce Directive. DSA maintains the prevision of the causes of exemption of liability, distinguishing between service providers of 'mere conduit' (art. 4), 'caching' (art. 5) and 'hosting' (art. 6). Substantial innovations consist in the introduction (Art 6) of a cause of exclusion of the benefit of the exemption of responsibility; in the forecast (Art 7) of the 'good samaritan' clause; in the introduction of specific obligations of action for the provider in the case of illicit content (Art 9 and 10).

[38] Intermediaries who are limited to an activity of 'mere conduit' (Art. 12 dir; Art. 14 D. Lgs. 70/2003) and 'caching' are exempt from liability, provided that they do not modify the information transmitted and, if informed of an irregularity on the platform, act promptly to remove the stored information, or to disable access (Art 13; Art 15 D. lgs 70/2003). Even permanent storage ('hosting') does not entail the liability of the operator, provided that the latter is not actually aware that the activity or information is illegal and that, as soon as he is aware of such facts, act immediately to remove the information or to disable access (art. 14 Directive; art. 16 D. Lgs. 70/2003).

[39] Subjection of providers to obligations of monitoring the information transmitted is also excluded; also active search of facts or circumstances indicative of illegal conduct is excluded (Art. 15 Directive; Art. 17 D.lgs. 70/03513). Only where the provider becomes aware of alleged unlawful activities an obligation to inform without delay the judicial or administrative authority acting as a vigilance (Art. 17, paragraph 2, lett

However, this regime turned out to be inadequate in the face of the massive development of digital relations.[40]

This is why the Italian Court of Cassation has tended to bring the provider's liability into line with the ordinary system. A distinction between "passive" and "active" providers has been drafted by the case law.[41]

"Passive" provider benefits from the integral application of the exemption clauses, while the "active" is liable according to the general regime according to Art. 2043 Civil Code.[42]

This distinction corresponds to that of illegal conduct which, as is well known, "may consist of an action or an omission, in the latter case by tort or omission in the proper sense, in the absence of the event, or, where an event results, in an improper sense; where the event is the unlawful act of another person, the offense of commission is constituted by omission in competition with the principal author".[43]

The figure of the active provider must, then, generally be traced back to the case of the illegal active conduct of the competition.

---

a) arises. The third paragraph of that Article states that 'The provider shall be legally responsible for the content of such services if, at the request of the supervisory judicial or administrative authority, he has not acted promptly to prevent access to that content, or if, having become aware of the unlawful or harmful character of a third of the content of a service to which it provides access, it has not informed the competent authority'.

[40] F Bocchini, 'Responsabilità dell'hosting provider, la responsabilità di Facebook per la mancata rimozione di contenuti illeciti' [2017] Giur it, 629 defines Dir. 2000/31/EC as '[T]he directive of irresponsibility'.

[41] Judgment of 23 March 2017, Google vs Louis Vuitton, C-236/08, ECLI:EU:C:2010:159 ruled that the special regime pursuant to Art. 14 dir. Is only applicable where the role played by the operator is 'neutral'. To this end, it is required that the conduct is purely technical, automatic and passive, which implies lack of knowledge or control of the stored content. See also Judgment of 12nd July 2011, L'Oreal c. e-Bay, C-324/09, EU:C:2010:159

The distinction between 'passive' and 'active' hosting providers has been immediately transposed by Italian jurisprudence, which applies just to the 'passive provider the exemption regime referred to in Art. 16, while submitting to the ordinary judgment of Art. 2043 the 'active' provider who 'carries out an activity that is outside a service of purely technical, automatic and passive order, and instead puts in place an active conduct, competing with others in the commission of the offence'. See Cass of 19March 2019, n. 7708, in *Foro it.*, 2019, I, c. 2045.

See F Di Ciommo, 'Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea' (2019) I Foro it., 2078; G Cassano, 'La Cassazione civile si pronuncia sulla responsabilità dell'internet service provider' [2019] Dir ind, 35; F Bocchini, 'La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP' [2019] Giur it, 2604; M L Gambini, 'La responsabilità dell'internet service provider approda in Cassazione' [2020] Corr giur, 177.

The case-law has identified a number of symptomatic factors which may indicate the 'active' nature of the service provider. Consider, by way of example, activities of 'filter, selection, indexing, organization, cataloguing, aggregation, evaluation, use, modification, extraction or promotion of content, carried out through an entrepreneurial management of the service, as well as the adoption of a technique of behavioural evaluation of users to increase their loyalty: conduct that have, in essence, the effect of completing and enriching in a non-passive way the enjoyment of the contents by indeterminate users'. In such cases, therefore, the affirmation of the liability of the intermediary is subject to the assessment of the constitutive elements of the non-contractual liability referred to in Art. 2043 c.c. See Trib. Roma of 2 October 2019, DeJure.

[42] The system of immunity therefore ceases to apply in cases where the provider plays an active role, giving it knowledge or control of the said contents. It is therefore essential that the 'unlawful nature of the activity or information should result from an actual knowledge or be manifest, that is to say that it must be concretely demonstrated or easily identifiable' (Judgment of 22 June 2021, *Cyando*, C-682/18 Press and Information YouTube, C-683/18 Youtube and Cyando, C-682/18 - C-683/18, EU:C:2021:50.

[43] Cass., 19th March 2019, n. 77008.

When the damage derives from the processing of data, the internet provider could be generally considered as the data controller, or as the data processor.[44] As far as the liability regime is concerned, we must make a distinction. The "passive" provider can go exempt from liability (according to Article 14 et seq.), while the "active" provider will be subject to the application of the common rules according to Art. 1218 or Art. 2043 c.c. (depending on the relevant liability regime, as already noted in the previous paragraph).

Once the liability of the service provider has been established, special attention should be paid to the quantification of damages.

The identification of the parameters for the liquidation requires the interpreter to take note of the now acclaimed "polyfunctionality" of civil liability, which, in order to guarantee effective protection to the injured party, pursues not only a compensatory function but also a sanctioning and deterrent purpose.

To this end, it is essential to consider the specificity of the offense committed via the Internet.

The absence of spatial boundaries of the net,[45] on the one hand, and the speed of propagation of the offense, on the other, determine the opportunity to set effective remedies, able to ensure full protection for the damaged interests, and, at the same time, to act as a deterrent in a general-preventive perspective.

On this point, it should be remembered that, under the "old" Privacy Code, the case law tended to award compensation for the unlawful processing of data based on a presumptive mechanism which reconnected the existence of damage to the particular wrongfulness of the conduct, or to the type of interest affected.

We can consider the (widely known) case[46] where the violation of the privacy of a famous footballer was compensated with a large number of damages (two million by the Tribunal, reduced to 70,000 Euros by the Court of Appeal).[47] This case is relevant because, even though there was no proof of actual damage, the compensation was assessed by the Court on the basis that the conduct was "particularly reprehensible for their sneaky and unfair character" and aimed "at the distorted use of the telephone for the achievement of illicit purposes".

---

[44] The investigation about the qualification of the provider must necessarily be carried out on a case-by-case basis. For example, the provider of the 'web hosting' service is 'responsible for processing' on behalf of the website operator, which is 'data controller'. The 'cloud provider' - according to a recent opinion of the Slovenian Data Protection Authority (IP - 0612-23/2019/19) - qualifies as joint data controller together with the customer, and not as a mere processor. As for social networks, the EDPB has issued guidelines (n. 8/2020), in which it is noted that the advertiser and the social media provider operate jointly in the case of targeted display advertising and must, consequently, qualify as joint processors. With regard to the relationship between social networks and the operator of a page administered by a different entity, the Court of Justice (Judgment of 5 June 2018, C-210/16, EU:C:2018:388) ruled that the administrators of 'Fanpage' on Facebook should be considered 'joint controllers' together with Facebook itself, in relation to the processing carried out through the use of such social pages.

[45] See N Irti, *Norma e luoghi. Problemi di geo-diritto* (Ed. Laterza, 2006) 5; N Irti, *L'ordine giuridico del mercato* (Ed. Laterza, 2009) 150.

[46] Trib Milano of 3 September 2012, n. 9749, Danno resp (2013), 51.

[47] App Milano of 22 July 2015, *Danno resp* (2015), 1047 states that "there is no doubt that the conduct of which the companies are responsible for appears to be particularly reprehensible because of their sneaky and unfair nature'.

Similarly, the Italian Court of Cassation considered awarding non-pecuniary damage as a result of the mere "violation of the rules of correctness and lawfulness, which are aimed at balancing the freedom of those who process data with the preservation of the sphere of the damaged party".[48]

As a result, damages are aimed to sanction the damaging party. In fact, the constitutional status of the interests damaged in the case of the processing of personal data justifies the assessment of damages even "in the absence of any evidence of a concrete alteration of the domestic customs" of the injured party, in order "to ensure the punitive value which is also proper to the compensation of the non-pecuniary damage from injury to fundamental rights".[49]

Moreover, in certain rulings on the liability of active providers, case law has assessed damages based on the degree of the wrongfulness of the operator's conduct. We can consider a case concerning the infringement of copyright on the internet. The Court of Rome decided to quantify the amount of compensation based on the "conduct held by the counterfeiter, the more or less sudden reaction in the removal of the materials illicitly transmitted and therefore the gravity and duration of the omissive conduct perpetrated to the detriment of the damaged party".[50]

The degree of the wrongfulness of the conduct and the peculiarity of the injured interest (eligible to be compensated "in re ipsa") are, hence, the parameters of the liquidation.

Therefore we can conclude that this field constitutes a further emergence point of the "polyfunctionality"[51] of non-contractual liability, which can provide adequate protection for the personality rights of network users and can act as an impulse for the accountability of internet providers.

4. Data processing and Blockchain.

Even denser are the questions that arise when unlawful data processing takes place within a Blockchain.

---

[48] Cass of 4 June 2016, Giur it (2019), 41, with reference to an unlawful data processing carried out by the Customs Agency, responsible for having communicated sensitive data relating to the judicial affairs of an employee through an ordinary protocol open to all. It ruled that Art 15 raised the presumption that the non-pecuniary damage is to be considered 'in re ipsa' unless the person causing damage proves that no loss have been suffered.

[49] Trib. Catania of 31 January 2018, n. 466 about the infringement of the constitutionally guaranteed right to the protection of one's domicile.

[50] Trib. Roma of 10 January 2019, *Dir internet* (2019), 140.

[51] C Salvi, 'La responsabilità civile', in G Iudica and P Zatti (eds) *Tratt. dir. privato* Iudica-Zatti (Giuffré, 2019) 11; G Alpa, *La responsabilità civile. Parte generale* (Utet giuridica, 2010) 159; P Trimarchi, *La responsabilità civile: atti illeciti, rischio, danno* (Giuffré, 2019) 283; A Di Majo, 'Principio di legalità e di proporzionalità nel risarcimento con funzione punitiva' [2017] Corr giur, 1042; P G Monateri, 'Le Sezioni Unite e le funzioni della responsabilità civile' [2017] Danno resp, 419; G Ponzanelli, 'Polifunzionalità della responsabilità civile tra diritto internazionale privato e diritto privato' [2017] Danno resp, 435; C Scognamiglio, 'Le Sezioni Unite ed i danni punitivi tra legge e giudizio' [2017] Resp civ prev, 1109; P Perlingieri, 'Le funzioni della responsabilità civile' [2004] Rass dir civ, 115; P Perlingieri, 'La responsabilità civile tra indennizzo e risarcimento' [2004] Rass dir civ, 1063; P Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, IV, *Attività e responsabilità* (Esi, 2020) 406.

In this case, indeed, the issues concern the compliance between the discipline referred to in Reg. 679/2016 and the architecture of the distributed Ledger.[52]

It should be noted that, despite the intent of its creators, the Blockchain does not constitute a system independent of the application of the rules established by the legal system.[53]

Therefore, the Blockchain needs to be framed and regulated according to the traditional legal categories.

In this context, the GDPR is abstractly applicable concerning the processing of data recorded in the ledger. Despite being encrypted, the information on the blockchain is not technically anonymous,[54] but it is pseudonym.[55]

However, it is hard to reconcile the decentralized system of the Distributed Ledger with the centralized structure of GDPR.

5. Principles of minimization and data processing by design.

The structure of the Blockchain seems hardly consistent with some of the cornerstones on which the implementation of the principle of accountability in Reg. 679/2016 is based, and which are essential for ensuring the safety of data processing.

First of all, we can consider the principle of "minimisation", according to Art. 5, paragraph 1, lett. c), which requires data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

This requirement contrasts with the distributed nature of the Blockchain, where data are replicated on each server. The same issue can be found concerning the right to restriction of processing (Art. 18).

We can think, again, about some of the fundamental rights of the data subject, such as the right to rectification (Art. 16) and to the erasure of data (Art. 17), which appear difficult to be exercised in the context of the Blockchain, where the recorded information is characterized by immutability.

Therefore, the existence of technical solutions for ensuring the implementation of the GDPR provisions must be checked.

---

[52] *Ex multis*, M Berberich-Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?' [2016] European Data Protection Law Review, 422; A Palladino, 'L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance' [2019] MediaLaws, 150; G Frezza, 'Blockchain, autenticazione e arte contemporanea' [2020] Dir fam pers, 489; F Rampone, 'I dati personali in ambiente blockchain tra anonimato e pseudonimato' [2018] Ciberspazio e dir, 459; A Mirchandani, 'The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR' (2019) 29 Fordham Intell Prop Media & Ent LJ, 1201.

[53] C Iorio, 'Blockchain e diritto dei contratti: criticità e prospettive' [2021] Actualidad juridica iberoamericana, 656.

[54] The GDPR is not applicable in the case of anonymous data, namely 'information that does not relate to an identified or identifiable natural person or to personal data rendered sufficiently anonymous to prevent or no longer allow the identification of the data subject' (recital 26 GDPR).

[55] There is always, in fact, the possibility, through special techniques, of re-identification. See F Faini, 'Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection' [2020] Resp civ prev, 297; A Gambino and C Bomprezzi, 'Blockchain e protezione dei dati personali' [2019] 619.

Concerning the principles of minimization and limitation of processing, some authors have suggested solutions which may prove useful for this purpose. They go from the addition of "noise" to the data, to making it more difficult to associate a private key and the data entered.[56] Also, the use of c.d. "disposable addresses"[57] that allow for the creation of a new address and a new one-time password for each transaction could grant compliance with GDPR.

More complex is the attempt to reconcile the Blockchain with the exercise of the right to erasure and rectification of data.[58] In fact, there is the technical possibility of acting on the blocks and modifying the recorded information. However, such an intervention undermines the users' trust in the Blockchain, whose use is justified precisely because the ledger guarantees the certainty and unchangeability of the information recorded on the chain.

Therefore, we can agree with the authors who propose to interpret the right to "erasure" in the generic meaning of making data "inaccessible" for the users. In case the "right to be forgotten" is exercised by the data subject, the information could be made unreachable by means of the destruction of the private key.[59] Another solution is the storing of personal data on an "off-chain" database, which would be linked to the Blockchain (and, therefore, not recorded on the blocks) through a hash.

Thus, the personal data could be deleted, or corrected, without altering the algorithmic function, which would remain unchanged in the digital ledger.[60]

6. The identification of data controller and data processor.

Therefore, there are technical solutions capable of ensuring compliance between the Blockchain and the principles of privacy by design and by default.

Critical issues remain concerning the difficult identification of data processors and data controller within a Blockchain, given the absence of a central authority with supervisory powers in the Ledger.

Several solutions have been suggested by scholars concerning the permissionless Blockchain.

---

[56] The proposed solutions, in detail, include the use of: a) 'Zero-knowledge proofs', a technique that allows a given subject to acquire evidence of a given statement, without guaranteeing access to the underlying data; b) adding 'noise' to data, consisting in grouping a given number of transactions together, so that it is impossible to discern the identity of part of the same; c) 'ring signature', that is, a special type of digital signature that, given a group of users equipped with public and private keys, allows to associate the transaction to the group in a generic way, without detecting the identity of the signing user. M Finck, 'Blockchains and Data Protection in the European Union' [2018] *European Data Protection Law Review*, 15. This opinion is followed by A Gambino and C Bomprezzi, 'Blockchain e protezione dei dati personali' [2019] 622.

[57] M Finck, 'Blockchains and Data Protection in the European Union' [2018] *European Data Protection Law Review*, 15.

[58] There are several technical solutions that can make recorded data editable: ranging from the function of 'chamelon hashes', to the technique of 'pruning' (which allows to delete a data, when the same is no longer necessary), or that of 'fork', leading to the redefinition of chain rules, with the creation of a new Ledger. See M Finck, 'Blockchains and Data Protection in the European Union' [2018] 15.

[59] This solution was suggested by the French CNIL: Solutions for a responsible use of the blockchain in the context of personal data", in https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

[60] This solution could be achieved by using the IPFS protocol ('interplanetary file system'), which includes 'on chain' only the link to the data, in addition to a time stamp and a hash of the outsourced data. M Finck, 'Blockchains and Data Protection in the European Union' [2018] 15.

As for the data controller, there is a tendency to exclude that this role can be played by the software developers, since they do not have the power to decide the purposes or means of processing, or by miners, who only participate in the process of validation of transactions and, therefore, of formation of the chain, without affecting the determination of the purposes of the processing.[61]

Some authors state that data controllers are all the nodes involved in the transaction, provided that the user's choice to make use of that specific Blockchain to carry out a very precise economic operation integrates the determination - respectively - of the means and purposes of data processing.[62]

At the same time, all the nodes that do not participate in the transaction and maintain a copy of the data qualify as data processor.

The identification of the data processor seems less problematic. This role can be easily attributed to the developers of smart contracts or to the "miners": the former are called to process data on behalf of users, while the latter validate the transactions containing personal data, so both of them clearly "process data on behalf of the data controller".[63]

And yet, although we can abstractly proceed to the attribution of the relevant qualifications for the purposes of the GDPR, it is a fact that the features of the permissionless Blockchain make it extremely difficult to fulfill the penetrating obligations provided by the GDPR.

On the one hand, the nature of the register makes it difficult for the data controller to monitor the totality of transactions added to the blocks; but, above all, the pseudonym of the identities prevents users from identifying the controllers, and the latter from identifying the recipient of specific obligations of conduct.

At present, therefore, it would seem that the only technology fully compatible with the legal framework is that of private permissioned Blockchain.

In this case, indeed, since there is an entity that determines the rules of access to the system, roles under the GDPR are easily identifiable: the title of data controller should be assumed by the central authority responsible for determining the criteria for selecting nodes, the system updates, and the rules of transparency.

Conclusions.

The purpose of this paper is to examine some of the critical issues related to the circulation and data processing in the digital age.

As outlined, the disciplinary framework is far from being considered defined.

---

[61] V Bellomia, 'Il contratto intelligente: questioni di diritto civile', in www.judicium.it

[62] M Finck, 'Blockchains and Data Protection in the European Union' [2018] 17; see also French CNIL, 'Solutions for a responsible use of the blockchain in the contex of personal data'; *contra* V Bellomia, 'Il contratto intelligente: questioni di diritto civile', www.judicium.it, 12, who states that this thesis - resulting in a 'widespread responsibility', would involve for any intervention on the treatment (such as the correction of a data) the necessary consent of the majority of nodes, as all co-controllers of each treatment, with the effect of paralyzing the system.

[63] This is the opinion of CNIL, 'Solutions for a responsible use of the blockchain in the context of personal data'.

There are still uncertainties about the legal nature of personal data, as well as about the identification of contractual schemes for their circulations, and the available remedy in case of infringement.

In order to guarantee more extended protection to interested parties, we must welcome the innovations introduced by the two recent EU Regulations of the "Digital Services Act"[64] and the "Digital Market Act".[65]

In order to face the opacity of the algorithmic choices also in relation to the use of data, the first Act provides specific obligations for platforms in terms of information and transparency. In particular, it requires that users are made aware of the rules on the operation of moderation and content recommendation systems, as well as on online advertising. Significantly, there are bans on the use of deceptive practices to manipulate users' choices, and targeted advertising aimed at minors or based on sensitive user data. Also, an obligation for the platforms to enable users to block "recommendations" based on profiling is introduced.

The Digital Market Act completes the set of protections for the consumer, looking at the possible use of data, by the "gatekeeper", for purposes that distort competition in the market.[66] For this reason, the Act establishes new prohibitions on restricting or refusing data portability or data reuse, in order to discourage or prevent the user from leaving the platform; it also provides for the prohibition of combining personal data of the user, derived from the platform services, with other personal data obtained from other services, including third parties, without the user's express permission. In addition, it states the obligation to provide commercial users with effective, continuous, and real-time access to aggregated and non-aggregated data provided or generated in the context of the use of the relevant basic platform services (always with the user's consent).

These Regulations, read in conjunction with the GDPR, are a further piece of the design of that "multi-level protection" of the digital user that, as we have pointed out, is essential to fully implement the effectiveness of the protection of fundamental rights in the technological society.

[64] European Parliament and Council Regulation 2022/2065/EU of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC [2022] OJ L 277/1.

[65] European Parliament and Council Regulation 2022/1925/EU of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJL265/1.

[66] "Gatekeepers" are the subjective categories of platforms subject to the application of the Digital Market Act. The designation as gatekeeper takes place on the basis of qualitative and subjective criteria, as well as in reference to the types of services offered (the so-called "Core Platform Services"), according to the thresholds established by Art. 3.