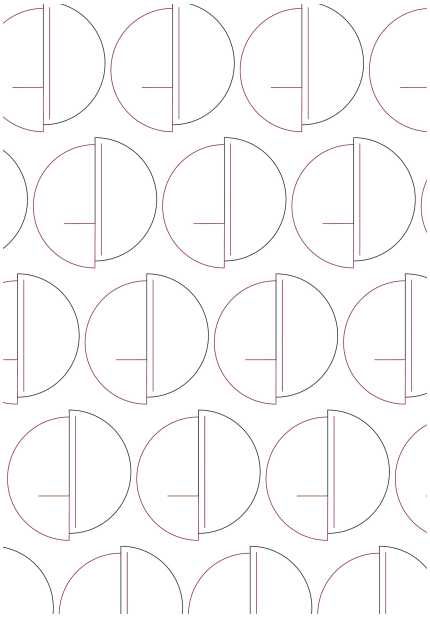
Materiali e documenti

Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2022 Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo



University Press

Sapienza Università Editrice

Collana Materiali e documenti 90

Annuario 2022
Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2022
Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo

SAPIENZA
UNIVERSITÀ EDITRICE
2022

Sapienza Università Editrice
Piazzale Aldo Moro 5 – 00185 Roma

www.editricesapienza.it
editrice.sapienza@uniroma1.it

Iscrizione Registro Operatori Comunicazione n. 11420
Registry of Communication Workers registration n. 11420

ISBN 978-88-9377-256-3

DOI 10.13133/9788893772563

Pubblicato nel mese di dicembre 2022 | *Published in December 2022*

Impaginazione a cura di | *Layout by*: Lucio Casalini e Enzo Maria Incutti

In copertina | *Cover image*: Michela Tenace, *Elaborazione grafica del logo OGID/JODI*, 2022, Archivio personale dell'a.

Indice

Presentazione

L'idea e la realizzazione del presente Annuario, alla seconda edizione, hanno trovato sviluppo nell'ambito delle attività seminariali, di confronto e di studio promosse nel corso del secondo semestre del 2021 e del primo semestre del 2022 dall'Osservatorio Giuridico sull'Innovazione Digitale (OGID), costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università Sapienza di Roma (https://web.uniroma1.it/deap/ogid).

L'Osservatorio promuove lo studio dell'impatto delle applicazioni delle tecnologie digitali sulle relazioni tra i privati, e delle connesse questioni di *governance*, attraverso una serie di attività, tra le quali l'organizzazione, la tenuta e la partecipazione a *webinars*, seminari e convegni, la cura di pubblicazioni e la partecipazione alle procedure di consultazione pubblica delle istituzioni della Unione europea sulle proposte normative aventi ad oggetto le tematiche dell'innovazione digitale.

OGID cura dal 2020 la rubrica di aggiornamento "Diritto e nuove tecnologie" della rivista trimestrale online in *open access* Persona e Mercato (rivista di fascia A)[1].

---

[1] **Numeri del 2022**: 1/2022- http://www.personaemercato.it/wp-content/uploads/2022/04/Osservatorio.pdf. **Numeri del 2021:** 1/2021 - http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio.pdf; 2/2021- http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf; 3/2021- http://www.personaemercato.it/wp-content/uploads/2021/08/Osservatorio.pdf; 4/2021 - http://www.personaemercato.it/wp-content/uploads/2021/12/Osservatorio-1.pdf . **Numeri del 2020**: 1/2020 - http://www.personaemercato.it/wp-content/uploads/2020/03/Osservatorio-1-2020.pdf; 2/2020 - http://www.personaemercato.it/wp-content/uploads/2020/05/Osservatorio.pdf; 3/2020 - http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-

I contributi pubblicati in questo Annuario hanno ad oggetto temi trattati dagli Autori nei *webinars* e seminari dell'Osservatorio (nei quali hanno preso parte come relatori) o nella Rubrica "Diritto e nuove tecnologie" sulla rivista Persona e Mercato.

Sono contributi che coprono una varietà di temi. Li presentiamo seguendo l'ordine alfabetico degli Autori.

Buona lettura!

I Curatori

Salvatore Orlando Giuseppina Capaldo

1. Financial Markets and AI: the Algo-trading Regulation

Attilio Altieri (Università di Foggia)

1.1. Introduction. AI and financial markets

Since the 1980s, new technologies, and in particular artificial intelligence (AI), have triggered a profound transformation of securities markets, and more generally of the entire financial services industry. The advent of Algorithmic Trading (AT) has transformed the face of trading systems, leading to the transition to electronic exchanges, and the very operations of intermediaries. For the latter, the transition from Automated Trading to High Frequency Trading (HFT) was a real quantum leap, thanks to the speed of collection, processing and transmission of functional data for investment strategies, as well as the speed of execution and cancellation of orders (within milliseconds)[1].

This paper was prepared within the context of the PRIN 2017 Programme – Progetto di ricerca di Rilevante Interesse Nazionale: "Artificial Intelligence and Legal Studies Perspectives. Are the Algorithmic decision-making and data driven predictions calling for a new legal framework? A focus on financial and labour markets highlighting protection of rights and wealth distribution", Prot. 2017L9HJ25_001, CUP I84I19001180008.

[1] T.C.W. LIN, *The New Investor*, in *UCLA Law Review*, 2013, 60, p. 678 ff.; W. MATTLI (edited by), *Global Algorithmic Capital Markets: High Frequency Trading, Dark Pools, and Regulatory Challenges,* Oxford, 2018, *passim* and specifically T. FOUCAULT, S. MOINAS, *Is Trading Fast Dangerous?*, p. 9 ff.; Y. YADAV, *Algorithmic Trading and Market Regulation*, p. 232 ff.; S. KERN, G. LOIACONO, *High Frequency Trading and Circuit Breakers in the EU. Recent Findings and Regulatory Activities*, p. 308 ff.

The undoubtedly "experimental" scope of AT is particularly interesting because of the "space" in which AI operates, i.e. through the creation of a new environment (by design)[2], conceived and constructed specifically by humans for AI to be able to work. Considering the coordinates in which AT works, the AI mechanisms are able to operate because there is a suitable environment for them to do so; as we know, the problem arises with regard to traders because, even if we wanted to differentiate the environments (one for fast traders and the other for slow traders), it would be difficult to separate them within the same financial world. In other words, the "fluttering of wings" of fast trader will affect (as it has historically already happened) slow traders to a certain extent[3].

---

[2] L. FLORIDI, *Pensare l'infosfera*. *La filosofia come design concettuale,* (trad. it.), Milano, 2020, *passim*.

[3] J. ADRIAN, *Informational Inequality: How High Frequency Traders Use Premier Access to Information to Prey on Institutional Investors*, in *Duke L. & Tech. Rev.*, 2016, 14, p. 256 ff.; D.W. ARNER, J. BARBERIS, R.P. BUCKLEY, *The Evolution of FinTech: A New Post-Crisis Paradigm?*, 2016, SSRN-id2676553; M. BALDAUF, J. MOLLNER, *High-Frequency Trading and Market Performance,* 2020, SSRN-id2674767; M. BARON, J. BROGAARD, B. HAGSTROEM, A. KIRILENKO, *Risk and Return in High-Frequency Trading*, in *Journal of Fin and Quant Anal*, 2019, 54, p. 993 ff.; B. BIAIS, T. FOUCAULT, S. MOINAS, *Equilibrium fast trading,* in *Journal of Financial Economics*, 2015, 116, p. 292 ff.; A. BOULATOV, M. DIERKER, *Pricing Prices,* 2007, SSRN-id967363; N.D. BROWN, *The Rise of High Frequency Trading: The Role Algorithms and the Lack of Regulations, Play in Today's Stock Market,* in *Appalachian J.L.*, 2012, 11, p. 209 ff.; V. CAIVANO, *The Impact of High Frequency Trading on Volatility. Evidence from the Italian market*, in *Quaderni di finanza CONSOB*, March 2015, n. 80; V. CAIVANO, S. CICCARELLI, G. DI STEFANO, M. FRATINI, G. GASPARRI, M. GILIBERTI, N. LINCIANO, I. TAROLA, *Il* trading *ad alta frequenza. Caratteristiche, effetti, questioni di* policy, in *Discussion Papers CONSOB*, December 2012, n. 5; J. CVITANIC , A.A. KIRILENKO, *High Frequency Traders and Asset Prices*, 2010, SSRN-id1569067; B. ENDE, T. UHLE, M.C. WEBER, *The Impact of a Millisecond: Measuring Latency Effects in Securities Trading,* in *Wirtschaftinformatik Proceedings*, 2011, Paper 116, p. 27 ff.; M.J. MCGOWAN, *The Rise of Computerized High Frequency Trading: Use and Controversy*, in *Duke Law & Technology Review*, 2010, n. 16, p. 1 ff.; S. MCNAMARA, *The Law and Ethics of High-Frequency Trading*, in *Minn. J.L. Sci. & Tech.*, 2016, 17, p. 71 ff.; M. O'HARA, *High-Frequency Trading and Its Impact on Markets*, in *Financial Analysts Journal Volume,* 2014, 70, p. 18 ff.; E. PAGNOTTA, T. PHILIPPON, *Competing on Speed*, in *Econometrica*, 2018, 86, p. 1067 ff.; A. PUORRO, *High Frequency Trading: una panoramica*, in *«Questioni di Economia e Finanza - Occasional Papers»*, Banca d'Italia, 2013, n. 198; Y. YADAV, *How Algorithmic Trading Undermines Efficiency in Capital Markets*, in *Vand. L. Rev.*, 2015, 68, p. 1607 ff.

However, this technology has been very successful as AT generates undeniable benefits, including improvements in liquidity, trading book depth and price discovery. Yet, at the same time, it is cause for concern. On the one hand, it weakens the position of the so-called slow traders and undermines confidence in the integrity of stock markets, threatening key principles of their proper functioning (e.g. equal access, fair treatment, market transparency). Moreover, it can undermine information efficiency and exacerbate the risks of excessive price volatility and manipulation[4].

In conditions of market turbulence, then, the marginalisation of the human element (which vanishes immediately after the creation of the algorithm, the latter operating independently of human intervention) accentuates the risk of systemic crises. Without appropriate supervision, the automatism generated by algorithmic trading means that intermediaries are no longer able to govern market strategies by assessing their impact in advance. Since Black Monday in 1987, AI-managed exchanges have been blamed both for causing numerous episodes of flash crashes marked by a relatively rapid recovery to normal market conditions, and for amplifying and dramatizing the impact of exogenous factors (such as the sub-prime meltdown, the sovereign debt crisis, or the pandemic global recession).

These concerns have led to a process of regulation, both in Europe (MiFID II) and in the US (Reg SCI and Reg AT) and many other countries, which in various ways combines different forms and sources (legislation, regulations and decisions by authorities, intervention by private enforcement, including the market operators themselves), in the knowledge that «the standard narrative is that securities regulation has three main goals: market efficiency (usually associated with low transaction costs, high liquidity, and market integrity), financial stability (mitigating systemic risk, the prime regulatory goal in recent years), and investor protection (against own mistakes and against others' misconduct, in response to information asymmetries and conflicts of interest)»[5].

---

[4] In the USA, see M.B. Fox, L.R. Glosten, G.V. Rauterberg, *The New Stock Market. Law, Economics and Policy*, New York, 2019, *passim*; P. Gomber, B. Arndt, M. Lutat, T. Uhle, *High-Frequency Trading*, 2011, SSRN-id1858626.

[5] A.M. Fleckner, *Regulating trading practices*, in N. Moloney, E. Ferran, J. Payne (edited by), *The Oxford Handbook of Financial Regulation*, Oxford, 2015, p. 599; a

1.2. Analysis of the system of (legal and regulatory) sources

From the collection, classification and analysis not only of primary (and secondary) EU[6] and US[7] legislation, but also of the stock exchange rules and regulations of the main trading venues[8], as well as of the reports of the supervisory authorities[9], it is possible to trace the evolutionary lines of the regulatory approaches in the systems under analysis: therefore, in a nutshell, it can be affirmed that, in the USA, AT is included in a set of rules based on audited self-regulation[10] while in the EU we can observe a phenomenon of co-regulation[11].

---

representative synopsis is offered, as known, by International Organization of Securities Commissions (IOSCO), Objectives and Principles of Securities Regulation (2010), 3 ("*protecting investors; ensuring that markets are fair, efficient and transparent; reducing systemic risk*"). In literature, *ex multiis*, J.C. COFFEE, H.A. SALE, M.T. HENDERSON, *Securities Regulation: Cases and Materials*[13], St. Paul, MN, 2015, p. 1 ff.; N. MOLONEY, *Financial Services and Markets*, in R. BALDWIN, M. CAVE, M. LODGE, (edited by), *The Oxford Handbook of Regulation*, Oxford, 2010, p. 437 ff.

[6] MiFID II, Commission delegated regulation (EU) 2017/589 of 19 July 2016, Reg. 2014/596/UE – *Market Abuse Regulation* "MAR".

[7] Regulation Systems Compliance and Integrity e Regulation Automated Trading.

[8] New York Stock Exchange; Chicago Board of Trading; Euronext; Borsa Italiana; Börse Frankfurt; London Stock Exchange.

[9] Staff Report on Algorithmic Trading in U.S. Capital Markets della SEC (August 2020) and MiFID II/MiFIR review report on Algorithmic Trading dell'ESMA (September 2021).

[10] This, as is well known, is inspired by the method of responsive regulation, since it leaves the definition of the rules and/or standards to the will of the private individual, also by delegation of the public authority which sets the *ubi consistam*, only subsequently acquiring the "chrisms" of lawfulness. Then, the discretion of the private party will fix the *an* and *quomodo* of the regulation (sometimes even only the latter). For all, see F. CAFAGGI, *Crisi della statualità, pluralismo e modelli di autoregolamentazione*, in *Pol. dir.*, 2001, 4, pp. 543 ff.; ID, *Un diritto privato europeo della regolazione? Coordinamento tra pubblico e privato nei nuovi modelli regolativi*, in *Pol. dir.*, 2004, 2, p. 205 ff.; ID, *La responsabilità dei regolatori privati. Tra mercati finanziari e servizi professionali*, in *Merc. conc. reg.*, 2006, 1, p. 9 ff.

[11] That is to say, the model that contemplates, in compliance with the principles of subsidiarity and proportionality, coexistence of public and private regulator in

Starting from the object of the regulatory activity of the public authority (similar in the two western systems), which in both cases is focused on competition and efficiency (of and) in the markets[12], although with significant differences in terms of scope, it can be seen that through Reg SCI and Reg AT, US regulators have focused on the technological infrastructure of the securities market surrounding AT, by acting at the operational level. SEC designed Reg SCI to create a structure of periodic tests and controls by which market participants can adequately prepare for and overcome systemic disruptions, from short-term flash crashes to longer-term crises such as the 2008 financial crisis. Meanwhile, Reg AT introduces stricter registration requirements for new traders. Compared to MiFID and MiFIR regulations, Reg SCI and Reg AT "only scrape the surface" by setting up measures aimed primarily at transparency. Although MiFID II also requires forms of transparency, the latter, as we know, dives deeper, requiring traders to limit their activity only to certain financial instruments and on particular regulated platforms and establishing strict organisational requirements for trading firms and trading venues. Moreover, the two regulatory approaches differ in the regime of "publicity" and "transparency" of algorithm source codes, since in the EU, even if ex post and in presence of certain conditions[13], they can be probed and controlled by the Supervisory Authority, whereas in the US, this is opposed by various reasons of intellectual property, considered by the legislator as not expendable unless crimes are committed[14].

---

determining standards or establishing contractual clauses. In a multilevel system, this regulatory model enables forms of coordination between public regulator and private regulator in connection, not by chance, with the regulatory thrusts of EU origin. Thus, co-regulation can develop both horizontally - in the form of cooperation in reciprocal relations between the public and private regulator - and vertically or hierarchically, emanating from the national or EU legislator. Therefore, the paradigm on which co-regulation is based is the principle of command - whereby private regulator is obliged to apply the rule within the limits set by public regulator, so as to increase the latter's accountability in defining standards.

[12] For all, see M. WOODWARD, *The Need for Speed: Regulatory Approaches to High Frequency Trading in the United States and the European Union*, in 50 *VAND. J. Transnat'l L.* 1359 (2017).

[13] See art. 17 and art. 28, MiFID II

[14] M. WOODWARD, *The Need for Speed*, cit., p. 1374 ff.; but also *United States of America v. Michael Coscia* ("Court of Appeal 7th Circuit), 886 F.3d 782 (2017); A. LUPOI, *La*

Another important aspect that comes to light, also from the analysis of practice, is the fact that regulation in this discipline reveals an increase in costs and a decrease in the use of related technology[15], as well as being an obstacle to "ESG" finance and long-term sustainable growth[16].

In consideration of a decades-long application of AT and always with a view to analysing the regulatory approach to the phenomenon, we have witnessed a sort of "*réorientation*"[17] by the North American regulator, where alternative ways of regulating the phenomenon of AT have been used as a starting point, among which we begin to glimpse strategies of procedural or delegated regulation, with timid compliance policies or in any case with the inclusion of algorithmic control systems (not only) *ex post*. This re-orientation is understandable in the light not only of complexity of market strategies and volume of daily-traded orders (which make a simple ex-post control extremely difficult and identify the nature of violations in an uncertain manner), but also of the limited resources available to the supervisory authorities, which must deploy suitable instruments to carry out monitoring and enforcement, with a view to audited self-regulation[18]. In a very short summary, it is possible to say that the AT has led to the unveiling of the state of deep crisis on which the ex post sanctioning system lies, so much so that it has led the SEC itself to admit that «continued vigilance in monitoring these advances in technology and trading, and updating of systems and expertise will be necessary in order to help ensure that our capital markets remain fair, deep, and liquid»[19].

---

negoziazione algoritmica ad alta frequenza e la struttura dei mercati: due casi negli Stati Uniti, in *Riv. dir. comm.*, 2019, II, p. 1 ff.

[15] K. O'CONNELL, (2019). *Has Regulation affected the High Frequency Trading Market*, in *27CathUJLTech145*, p. 165: «Intensified government regulation is a factor in decreased profitability».

[16] T. MYKLEBUST, *High-Frequency Trading as an Impediment to Long-Term and Sustainable Finance: Identifying a Regulatory Gap That Can Put the Goals of the European Action Plan on Financing Sustainable Growth at Risk*, in *7 Oslo L. REV.* 63 (2020).

[17] F. MARTY, T. KIRAT, H. BOUTHINON-DUMAS, A. REZAEE, *The Crisis of the Regulation by the Ex Post Sanction: New Avenues of Financial Regulation, from the Subprime Crisis to High Frequency Trading*, in 104 *DROIT eT Societe* 71 (2020).

[18] F. CAFAGGI, *La responsabilità dei regolatori privati*, cit., p. 30 ff.

[19] Staff of the U.S. Securities and Exchange Commission Report on Algorithmic Trading in U.S. Capital Markets, August 5, 2020, p. 83.

Instead, looking at the other side of the Atlantic, the EU regulatory framework is characterised by a series of measures aimed at prohibiting behaviours and strategies that are clearly market manipulative by Algorithmic Traders to the detriment of Slow Traders (i.e. conduct that generates operational market manipulation)[20] as well as by regulation addressed to both Algo-traders and trading venue operators where AT is allowed: in particular, with regard to the latter legal framework, the risk management approach (now also set out in the proposal for a regulation on AI) has been implemented through a census and assessment of the risks themselves, with the consequent imposition of certain organisational structures (adequately monitored), suitable to mitigate the distorting effects of AT[21].

The "co-regulatory style" of the EU lawmaker (and, consequently, of the national lawmaker) has, however, allowed degrees of flexibility and room for discretion on the part of the supervisory authority in the implementation of the relevant measure (as well as on the part of the judge in the judicial review of the administrative intervention): and it is possible to think of the implementation of formal requirements both in terms of organisational structures and in terms of the collection and provision of information imposed on the algorithmic trader and the related trading venues[22]; or, moreover, the degree of opacity of AT (i.e. the conceptual and other contrasts developed in the literature between intentional and intrinsic opacity)[23].

---

[20] This legal framework is contained in the Market Abuse Regulation, in part. §12 and §15.

[21] For an effective systematic reconstruction, cf. M. Bertani, *Trading algoritmico ad alta frequenza e tutela dello* «slow trader», in *AGE,* 2019, 1, p. 261 ff.; also F. Annunziata, *I processi di mercato automatizzati e il* trading *algoritmico*, in M. Cian, C. Sandei (edited by), *Diritto del Fintech*, Milano, 2020, p. 397 ff.

[22] See the prohibition under art. 48.9 MiFID II on modulating fees in such a way as not to incentivise strategies that leverage the systematic placement, modification or cancellation of large quantities of orders to disorderly trading conditions or market abuse; or the discretion of trading venues to exercise their powers of intervention in event of risk or emergence of serious market disturbances or abnormal trading conditions; also, the rules defining the powers of supervisors to request data and respectively the obligations of operators (including HFTs and ATs) to disclosure regarding the algorithmic systems used, which art. 17 MiFID and 67-ter para. 3 TUF leave partly undefined.

[23] C. Tabarrini, *Comprendre la "*Big Mind*": il GDPR sana il divario di intelligibilità uomo-macchina*, in *Dir. inf.*, 2019, 2, p. 580.

The doctrine has reacted in various ways in order to close this gap: a simplified algorithmic supervision that tracks orders and imposes *ex-post* sanctions has been proposed[24]; greater transparency for AT operators and the provision of licences for traders to monitor the phenomenon as well as ensuring a levelled playing field for scarce AT resources (i.e. proximity and co-location services) have been called for[25]; rules to determine a "price of prices" have been hypothesised, i.e. to consider the mechanisms for determining the prices of access to the different levels of depth of the trading book (pre-trade information) and the prices of access to post-trade information, so as to price such information appropriately according to its quality and close the gap with the HFT[26]; someone proposed to limit the negative effects of HFT on market efficiency by reducing the competitive advantage of algorithms through the exploitation of information and by reducing the costs of supplying market information to slow traders[27]; finally, the hypothesis of drawing up operational rules aimed at preserving competitive advantages that depend on significant investments, minimising organisational costs and proportioning formal requirements to substantive objectives was put forward[28].

1.3. Standards vs. rules; data vs. information

The US example (and to some extent the European one) shows how the market system has not contributed to the adoption of a better regulatory framework than the state one, not only in terms of market efficiency and financial stability, but above all with regard to investor protection. This is demonstrated by both the "failure" of ex post sanctioning and the repercussions on the protection of slow traders,

---

[24] P. LUCANTONI, *L'*«high frequency trading» *nel prisma della vigilanza algoritmica del mercato*, in *AGE*, 2019, 1, p. 297 ff.

[25] S. ALVARO, M. VENTORUZZO, «High-Frequency Trading»: *note per una discussione,* in *Banca impr. soc.*, 2016, 3, p. 417 ff.

[26] M. GARGANTINI, M. SIRI, *Il "prezzo dei prezzi". Una soluzione di mercato ai rischi dell'*high frequency trading, in *Riv. soc.*, 2019, 5, p. 1100 ff.

[27] G. BALP, G. STRAMPELLI, *Preserving Capital Markets Efficiency in the High-Frequency Trading Era,* in *Journal of Law, Technology & Policy*, 2018, p. 359 ff.

[28] M. BERTANI, *Trading algoritmico ad alta frequenza e tutela*, cit., p. 261 ff.

right up to the so-called "circuit breakers", which are able to temporarily suspend or limit trading[29].

For a different analysis of the problem it would be necessary to start from the assumption that A(*gere sine*) I(*ntelligere*) needs an adequate environment[30] – apart from the hypothesis that AI itself is an environment[31] – and, somewhat evocatively, this "eco-system" seems to have been offered by the markets, as mentioned in the introduction: it can be said that this fact would already be able to justify the "failure" of *ex post* protections and to set up (*rectius*, strengthen) the system in terms of "prevention" (with an *ex ante* approach), since one would be dealing with "spatial" coordinates and, consequently, with a problem of "organization" of that space; but in addition to that, there would be at least two other factors that could justify a different approach.

The first one is provided by the joint reading of MiFID II, of the regulations of the stock markets listed above and of the proposal for a regulation on AI[32]: from these sources it is possible to understand how the implementation of standards in terms of organisational structures and the collection and supply of information imposed on algorithmic traders and trading venues, in addition to affecting their organisational costs, trading strategies and interaction with slow traders, already gives the interpreter an anticipatory vision and a so-called risk-based approach at this historical stage.

The second factor can be found right between the folds of the organisational rules, which today, unfortunately, do not take into

---

[29] On the issue, see A. SUBRAHMANYAM, *Algorithmic trading, the Flash Crash, and coordinated circuit breakers*, in *Borsa Istanbul Review*, Volume 13, Issue 3, 2013, p. 4 ff.

[30] L. FLORIDI, F. CABITZA, *Intelligenza artificiale. L'uso delle nuove macchine. Martini Lecture*, Firenze-Milano, 2021, p. 139 ff. Moreover, the same paradigm can be constructed by comparing the problems surrounding so-called Autonomous Vehicles and Autonomous Shipping, where the former encounter greater difficulties than the latter precisely because of the different "space" in which they operate. About this issue, *ex multiis*, cf. E. GABRIELLI, U. RUFFOLO, *Intelligenza Artificiale e diritto*, in *Giur. it.*, 2019, 7, p. 1657 ff.; S. GUERRA, *Ready about, Here Comes AI: Potential Maritime Law Challenges for Autonomous Shipping*, in *University of San Francisco Maritime Law Journal*, 30, no. 2, 2017, p. 69 ff.

[31] M. BARBERIS, *Ecologia della rete. Come usare internet e vivere felici*, Milano-Udine, 2021, p. 40 ff., p. 161 ff.

[32] Together with the complex of proposals and acts already approved on (and for) the digital world: Data Governance Act, Digital Markets Act, Digital Services Act, the proposal for a regulation on machine products and GDPR.

account the fact that AI not only does not exploit capital and labour in an orthodox way, but in some cases it is a tool for business and the financial industry without using the same capital and labour: in fact, the inputs of the "new" production are not only something else, but do not represent a meagre resource at all (just think of data or, better, of Big data)[33]. If we combine this "architecture" with the exploitation of "financial microstructures", and therefore the use of the various exchange mechanisms that influence the price discovery[34], we perceive that the real core of intervention can only be that related (once again) to data (given the non-adherence of AT to models based on stocks, to those based on information and to behavioural finance) and, if we wanted to summarise the concept through an equation, it would be quite icastic to say that data is to AT as information is to the slow trader. As it is well known, data is a *species* of the *genus* information but, unlike the latter, as already mentioned, it is not a meagre resource and, in the financial markets (unlike information) it does not represent a competing resource[35].

1.4. Some (provisional) conclusions

The problem, at this point, shifts from a Law & Economics approach (which is nonetheless present, since there are tragic choices, but with a different meaning) to a "new" and possible liability, which takes into account not the quantity of data, but their quality, which "weighs" resources instead of "counting" them (*rectius*, computing

[33] Cf. P. SAMUELSON, *Privacy as Intellectual Property*, in *Stanford L. Rev.*, 2000, p. 1138; M.J. RADIN, *Property Evolving in Cyberspace*, in *J. L. & Com.*, 1996, p. 514 ff.

[34] M. O'HARA, *Market Microstructure Theory*, Cambridge MA, 1995, p. 1 ff.; P. PAIARDINI, *La microstruttura dei mercati finanziari. Teorie, applicazioni ed esperimenti*, Torino, 2021, *passim*.

[35] S. ORLANDO, *Le informazioni*, Padova, 2012, who distinguishes between information and reproduction and between information and representation; H. ZECH, *Information as Property*, in *JIPITEC*, 2015, p. 192 ff., who identifies three levels of talking about information: the semantic level of information (meaning), the syntactic level of information (signs and their relation with each other) and communication channel (on the physical level).

them), from the point of view not of cost allocation but of resource dislocation[36].

Therefore, a first step would be the identification of an "organisational" and "adequate" solution, imposed by law, which must take into account these parameters *ex ante*, i.e. before the operational release of AT: and this rule should be imposed by the (EU) lawmaker with regard to algo-traders (and therefore, in the Italian case, to Sim[37] and banks) and trading venues, implementing the already existing regulatory framework.

The second step is intertwined with the theme of algorithmic "transparency" and with the consequent right to an explanation[38], in the wake of Art. 22 GDPR and of the proposal for a regulation on AI: far from wishing to apply such a mechanism to markets (moreover, this would be a downstream problem involving the individual slow trader, which is beyond the scope of this paper), it seems interesting to grasp the systematic developments in order to integrate the "rule" that we are trying to construct in anticipation. In fact, considering AT as a "black box", or rather as a procedure where matrix calculations are performed without being able to be reconstructed in their logical path, the problem of fallacy of transparency is more evident[39]: then, in order to provide a compulsory market-centric "explanation"[40], it is precisely

---

[36] G. CALABRESI, *The Future of Law and Economics*, New Haven, 2016; G. CALABRESI, E. AL MUREDEN, Drivereless cars. *Intelligenza artificiale e future della mobilità,* Bologna, 2021.

[37] SIM stands for "Società di intermediazione mobiliare", namely Securities or investment firm.

[38] Cf. E. FALLETTI, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in *Dir. informazione e informatica,* 2020, 2, p. 169 ff.

[39] M. ANNANY, K. CRAWFORD, *Seeing Without knowing: limitations of the transparency ideal and its application to algorithmic accountability*, 20, *New Media & Society*, 3, p. 973 ff.; but it would be enough to apply the thinking of S. PAGLIANTINI, *Trasparenza contrattuale* (voce), in *Enc. Dir.,* Annali VI, 2012.

[40] Borrowing and paraphrasing the expression of "sensitivity-based" explanation used by L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16, *Duke Law & Technology Review*, 18, 2017, p. 39 ff.; see also C. TABARRINI, *Comprendre la "*Big Mind*"*, cit., p. 580, where she states «*affinché una spiegazione soggetto-centrica si possa configurare come significativa questa dovrebbe: (i) prendere in considerazione le specifiche circostanze del caso; (ii) focalizzarsi sullo scoprire il funzionamento interno del software utilizzato per la decisione; (iii) consentire ai soggetti interessati di avere un'idea chiara di tutte le variabili concretamente prese in considerazione e il peso che ciascuna ha esercitato sullo specifico esito*».

on the governance of data that one must affect, defining inputs[41] to obviate the Luddite shutdown of the AT circuit when one is no longer able to control the "euphoria and panic" of markets[42]. In other words, it would be the task of the European legislator, again with a view to co-regulation, to identify criteria on how to "organise" data, on how the flow of that data is generated, on how data, losing itself in the algorithm, becomes information itself; it would then be the task of managers of trading venues to ensure that there is adequate compliance with the *regula iuris* established upstream, by including this activity in the periodic due diligence communications to the supervisory authority.

De jure condendo, the third step would be to coordinate sentiment analysis[43] more effectively, i.e. opinion mining[44] that extracts information from a text to identify and classify subjective opinions[45]: the result would be achieved either through the prohibition of such

---

[41] Not by chance, F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge, 2015 (but also ID, *Law's Acceleration of Finance: Redefining the Problem of High-Frequency Trading*, 36 Cardozo L. Rev. 2015, p. 2085 ff.).

[42] This direction is partly taken by the proposal for a Directive contained in the Digital Finance Package [see recital no. 5 and Art. 6(3)], which amends MiFID II, pending MiFID III.

[43] As partly suggested by D. SHAH, H. ISAH, F. ZULKERNINE, *Predicting the Effects of News Sentiments on the Stock Market*, in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, p. 4705 ff. Cf. also E. IPPOLITI, *Un filosofo a Wall Sreet. Speculazioni sulla finanza da Aristotele ai bitocoin*, Milano, 2020, p. 157 ff.

[44] And thus the analysis of opinions, moods or attitudes. But on this point, see S.L. HESTON, N.R. SINHA, *News Versus Sentiment: Predicting Stock Returns from News Stories* (June, 2016), in *FEDS Working Paper* No. 2016-48, available at SSRN: https://ssrn.com/abstract=2792559.

[45] X. ZHANG, H. FUEHRES, P.A. GLOOR, *Predicting Stock Market Indicators Through Twitter "I hope it is not as bad as I fear"*, in *Procedia - Social and Behavioral Sciences*, Volume 26, 2011, p. 55 ff., who tried to predict market indicators such as Dow Jones, NASDAQ and S&P 500 through the analysis of Twitter posts and, by collecting their feeds for six months and measuring their collective hope and fear each day, they analysed the correlation between these indices and market indicators. The research concludes with the statement that «when the emotions on twitter fly high, that is when people express a lot of hope, fear, and worry, the Dow goes down the next day. When people have less hope, fear, and worry, the Dow goes up. It therefore seems that just checking on twitter for emotional outbursts of any kind gives a predictor of how the stock market will be doing the next day».

conducts or through the regulation and/or disclosure of this "method", in order to avoid the recurrence of emblematic events that have also made the headlines, such as the "GameStop" case, where a very high number of posts on Reddit heavily influenced the activity not only of the slow trader but also (and above all) of the algo-trader[46]. All this should lead to a more efficient view of the market, maintaining financial stability, also with a view to protecting (non-algorithmic) investors[47], not by leveraging price, but by persuading algo-traders to act in certain ways.

In short, we return to the well-known crossroads between data, information and knowledge[48], where, as it is widely known, although the last of these represents the major input in the production process, more than raw materials and capital itself, and one of the fundamental variables in the path of expansion of any enterprise[49], it is precisely knowledge, as meta-information[50], which cannot be confused with *datum*[51] and, more significantly, cannot be a preventive source of learning about the factors that determine the behaviour of either market players or the results of their interactions, otherwise competition will be debased as a discovery process[52]. And the regulation of a phenomenon of this magnitude cannot be left to the definition of standards or included in some ethical code, otherwise we would progressively abandon that Popper's intuition "open society", with the serious risk

---

[46] Cf. A. BETZER, J.PH. HARRIES, *How Online Comments affect Stock Trading - The Case of Gamestop* (May 10, 2021). Forthcoming, in *Financial Markets and Portfolio Management*, Available at SSRN: https://ssrn.com/abstract=3844378; but also C. LONG, B.M. LUCEY, L. YAROVAYA, *'I Just Like the Stock' versus 'Fear and Loathing on Main Street' : The Role of Reddit Sentiment in the GameStop Short Squeeze* (April 8, 2021). available at SSRN: https://ssrn.com/abstract=3822315.

[47] I. ROSU, *Fast and slow informed trading*, in *Journal of Financial Markets*, 2019, 43, p. 1 ff.

[48] O.H. DOMBALAGIAN, *Chasign the tape: Information Law and Policy in Capital Markets*, Cambridge MA, 2015

[49] V. ZENO-ZENCOVICH, G.B. SANDICCHI, *L'economia della conoscenza ed i suoi riflessi giuridici*, in *Dir. inf.*, 2002, p. 972.

[50] K.E. BOULDING, *The Economics of Knowledge and the Knowledge of Economics*, in *The American Economic Review*, 1966, Vol. 56, p. 1 ff.

[51] Overcoming the "incontinence of emptiness" that cybernetics seeks to suppress: for some interesting ideas, see S. ŽIŽEK, *L'incontinenza del vuoto. Pennacchi economico-filosofici* (trad. it.), Milano, 2019.

[52] F.A. VON HAYEK, *La concorrenza come procedimento di scoperta*, in ID, *Competizione e conoscenza*, (trad. it.), Soveria Mannelli, 2017, p. 91 ff.

of closing processes of knowledge (not only of the market) within a memory rethought and organised by cybernetics on the model of the black box[53].

[53] And see the conclusions of T. NUMERICO, *Big data e algoritmi. Prospettive critiche*, Roma, 2021, p. 251 ff.

2. *Privacy Enhancing Technologies*, trasparenza e tutela della persona nell'ambiente digitale

Alessandro Bernes (Università Ca' Foscari Venezia)

2.1. Le funzioni della tecnologia nell'era digitale

In seguito alla "rivoluzione" condotta dalle nuove tecnologie, per un verso, è reso a molti più semplice e immediato l'accesso ad *Internet* e, in generale, prender parte alla società dell'informazione; per altro verso, con riferimento alla navigazione sul *web*, alla sottoscrizione di servizi digitali, al *download* di contenuti digitali, e via dicendo, gli utenti hanno una scarsa percezione dei rischi legati a dette attività, mentre, al contrario, basano quasi esclusivamente le proprie scelte sulla fiducia, piena e incondizionata, circa la diffusione tra i consociati di quanto loro offerto. Di qui, il problema del c.d. *privacy paradox*, per il quale ciascun individuo tiene molto ad evitare intrusioni non autorizzate nella propria sfera privata, ma al tempo stesso presta poca attenzione alla quantità e alle categorie di dati ad esso riconducibili, raccolti nel momento in cui ci si interfaccia con l'ambiente digitale, soprattutto quando il servizio è fornito "gratuitamente"[1].

[1] Stando a S. BARTH, M. D.T. DE JONG, *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*, in *Telematics and Informatics*, 2017(34), p. 1039, «*while many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behavior, this rarely translates into actual protective behaviour* (…) *Although users are aware of privacy risks on the internet, they tend to share private information in exchange for retail value and personalized services*». L'AGCM ha pubblicato, nel 2018, i risultati dell'"Analisi della propensione degli utenti online a consentire l'uso dei propri dati a fronte dell'erogazione di servizi", reperibile *online* all'indirizzo https://www.agcm.it/dotcmsDOC/allegati-news/IC53%20-%20Survey%20primi%20risultati.pdf. In particolare, dal sondaggio, condotto su un campione di utenti di servizi *online*, è emerso che circa 6 utenti su

In realtà, gli individui non sembrano in grado di potere valutare, nella pratica, le conseguenze (future) delle loro scelte in merito all'immissione in Rete di dati personali e, quindi, esercitare un vero e proprio controllo sul loro flusso[2] – anche perché i fornitori di servizi della società dell'informazione dettano unilateralmente la disciplina dei termini e delle condizioni cui gli utenti devono necessariamente adeguarsi, qualora intendano fruire di quanto loro offerto. In questo senso, l'alternativa tra il fornire o no i propri dati per l'utilizzo dei servizi *online* costituisce, invero, una falsa opzione, posto che il mancato accesso a *quel* servizio degenera in una auto-esclusione sociale, nella perdita di benefici ovvero nell'emersione di costi di transazione; ciò che determina un effetto di tipo *lock-in*[3].

Tra le molte ragioni che hanno portato al fenomeno del *privacy paradox*, vi è da chiedersi quale ruolo assuma il *gap* di natura tecnologica, piuttosto che regolamentare in senso stretto[4]. In altre parole, è forse la mancanza di strumenti tecnologici, i quali consentano, in maniera trasparente, la visualizzazione dei dati raccolti, nel tempo, dai servizi della società dell'informazione, ovvero con chi i dati vengono condivisi, ciò che impedisce alle persone di comprendere – ma prima ancora

10 non solo sono consapevoli di generare, con le loro attività *online*, dati utilizzabili per attività di profilazione, ma anche che essi appaiono informati dell'elevato grado di pervasività dei sistemi di raccolta (es. geolocalizzazione, accesso a funzionalità come la rubrica, il microfono e la videocamera) e della possibilità di sfruttamento dei dati da parte delle imprese. Nel complesso è risultato che 4 utenti su 10 sono consapevoli della stretta relazione esistente tra la concessione del consenso e la gratuità del servizio. Per l'apparente gratuità delle c.d. *non-monetary transactions*, dove i fornitori di un servizio digitale gratuito vanno a sfruttare commercialmente i dati (personali) resi o generati dagli utenti, si veda C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, p. 61 ss.

2 Sul diritto alla protezione dei dati personali inteso nel senso di controllo da parte del singolo circa le informazioni che lo riguardano, vedi già le precorritrici affermazioni di S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; per l'elaborazione successiva, ID., *Il diritto di avere diritti*, Roma-Bari, 2012. Per una efficace sintesi di una bibliografia oramai sterminata, V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 3 ss.

3 Per tutti, D. J. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, in *Harvard Law Review*, 126(7), 2013, p. 1880 ss.

4 Desta perplessità, soprattutto nell'epoca della *Big data analytics*, la possibilità che gli strumenti del diritto possano far fronte, da soli, alla tutela dei dati personali: così A. C. NAZZARO, *L'utilizzo dei* Big data *e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, p. 1239.

di conoscere[5] – i meccanismi di "mercato"[6] dei dati personali o, per meglio dire, la (libera) circolazione delle informazioni nell'ambiente digitale[7]?

Ci si deve domandare, in sostanza, se le tecnologie che permettono il trattamento di dati personali possono venire in supporto anche alla stessa tutela della persona, in modo da riequilibrare, per tale via, l'asimmetria conoscitiva esistente tra chi rende i servizi digitali e coloro che li utilizzano quotidianamente[8]; squilibrio, questo, sia pur esacerbato dal nuovo contesto della Rete, comunque riconducibile a quello, da tempo noto, intercorrente fra professionista e consumatore[9].

Il presente scritto si propone allora di indagare come ci si possa servire della "scelta tecnica" in funzione della protezione dei dati

---

[5] Sulla rilevanza, nell'ordinamento giuridico, della *conoscibilità* piuttosto che della *conoscenza*, vedasi S. PUGLIATTI, *Conoscenza*, in *Enc. dir.*, IX, 1961, p. 45 ss., ove si richiama, peraltro, la postulata correlazione funzionale della volontà (impulso) alla conoscenza e della conoscenza (guida) alla volontà. Più di recente, S. ORLANDO, *Le informazioni*, Padova, 2013, p. 67 ss.

[6] V. ZENO-ZENCOVICH, *Do "Data Markets" exist?*, in *MediaLaws – Rivista di diritto dei media*, 2019, 2, p. 22 ss.

[7] La raccolta di dati personali ma soprattutto la loro analisi e l'estrazione di informazioni inferenziali costituiscono oggi un'operazione confacente a molteplici modelli di *data-driven economy* e di valorizzazione del potere informativo, soprattutto al fine di costruire un profilo utente e giungere sino a predirne i comportamenti. Sul fenomeno della patrimonializzazione dei dati personali, si vedano, per tutti, V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, p. 642 ss., nonché R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2020, p. 760 ss. In giurisprudenza, in merito al noto caso *Facebook vs*. AGCM, si è pronunciato, da ultimo, CONS. STATO, sez. VI, 29 marzo 2021, n. 2631, in *Foro it*, 2021, III, c. 325 ss., con nota di R. PARDOLESI, A. D'AVOLA, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i 'dark pattern') parallele convergenti?*

[8] ENISA, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, 2015, p. 5, ove ci si interroga se i problemi generati dalla tecnologia che rende possibile il trattamento dei dati personali, in particolare per i *digital providers*, possano trovare, oggi, una risposta anche nella stessa tecnologia. Il tema dell'intersezione fra la tecnica giuridica e la tecnica informatica, e dell'apporto fornito dall'una e dall'altra, è una costante della riflessione in tema di *data protection*: sul punto, U. PAGALLO, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Torino, 2014, p. 285 ss.

[9] L'accostamento della disciplina della protezione dei dati personali alla normativa in tema di tutela del consumatore è stato da tempo evidenziato in dottrina; sul punto, di recente, D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, pp. 2786-2787; F. PIRAINO, *I ''diritti dell'interessato'' nel Regolamento generale sulla protezione dei dati personali*, *ivi*, p. 2789.

personali, al fine di tutelare i diritti fondamentali della persona che si interfaccia con l'ambiente digitale[10]. In particolare, l'attenzione sarà rivolta alle *modalità* attraverso le quali implementare le norme applicabili al trattamento di dati personali, per il tramite di strumenti informatici volti a garantire una maggiore trasparenza delle operazioni e rendere di queste più consapevoli gli individui; allo stesso tempo, attraverso la predisposizione di certune tecnologie da parte dei titolari del trattamento, sembra rafforzarsi l'*effettività* della tutela stessa dei diritti dell'interessato. Ciò dovrebbe determinare, in ultima istanza, un ripensamento, da un lato, quanto ai meccanismi di produzione di norme, almeno in senso formale, diversamente ragionando sui rapporti tra tecnica e diritto[11]; dall'altro lato, guardare al ruolo assunto oggigiorno dai soggetti privati che pongono in essere operazioni con dati personali, quali veri e propri attori della regolazione dei mercati digitali[12].

Il tema indagato si interseca con il noto fenomeno per il quale le principali società tecnologiche – e non solo gli *Internet Service Provider* – hanno assunto oggi, grazie alle economie di scale e agli effetti di rete, il ruolo di *gatekeeper* per l'utilizzo dei servizi offerti dal *Web*: esse esercitano, autolegittimandosi di fatto (d)all'interno del mercato[13], un

[10] Quanto al diritto alla protezione dei dati personali inteso come precondizione al pieno godimento di altri diritti fondamentali dell'uomo, e in ultima istanza della dignità della persona, magistralmente, S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa. Il nuovo codice della privacy*, in *Eur. dir. priv*., 2004, p. 1 ss.

[11] In argomento, G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Dir. inf*., 2012, p. 831, secondo la quale «oggi l'informazione senza la tecnologia non meriterebbe un discorso a sé, e probabilmente non avrebbe senso (…)». Più in generale, in un dibattito a più voci, N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, 2001; L. MENGONI, *Diritto e tecnica*, in *Riv. trim. dir. proc. civ*., 2001, p. 1 ss.; N. IRTI, *Un incompiuto dialogo con Luigi Mengoni*, in *Eur. dir. priv*., 2012, p. 197 ss.

[12] Sul diritto privato in funzione regolativa, di recente, A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020, p. 201 ss.; ma cfr. anche V. DE LUCA, *Autonomia privata e mercato telematico nel sistema delle fonti*, Milano, 2004, p. 58, dove si affianca, nell'epoca della globalizzazione, ad una nuova *lex mercatoria* anche una *lex informatica*; in termini simili, G. TEUBNER, *Regimi privati globali. Nuovo diritto spontaneo e costituzione duale nelle sfere autonome della società globale*, in ID., *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, trad. it. a cura di R. Prandini, Roma, 2005, p. 59 ss.

[13] Sui poteri privati che superano la tradizionale parità dei soggetti, fondamentali sono gli studi di C. M. BIANCA, *Le autorità private*, Napoli, 1977; ID., *Ex facto oritur ius*, in *Riv. dir. civ*., 1995, I, p. 787 ss., ove si elaborava una categoria che comunque metteva già in discussione la tradizionale separazione tra pubblico e privato; ma cfr. già W. CESARINI SFORZA, *Il diritto dei privati*, Milano, 1963, *passim*. Di recente declinato, con riferimento al nuovo assetto economico-sociale della realtà odierna, si veda il volume di P. SIRENA,

controllo pressoché totale dell'informazione da processare, attraverso meccanismi (per lo più *software*) che consistono nel selezionare, analizzare, riprodurre, estrarre e cancellare l'informazione stessa[14]. Inoltre, le *Big Tech* mostrano di detenere il monopolio delle tecnologie non solo per la raccolta dei dati personali – da riutilizzare poi a fini commerciali – ma sembrano essere addirittura gli unici soggetti in grado di tutelare i diritti dell'interessato, come evidenziato nelle sentenze della Corte di Giustizia dell'Unione Europea in materia di "oblio": qui è stato esplicitamente riconosciuto a *Google* il potere di bilanciare finanche diritti fondamentali[15], da attuarsi, peraltro, mediante il ricorso a strumenti tecnici, quali la de-indicizzazione dei *link* verso le pagine *web* dall'elenco dei risultati mostrati dai motori di ricerca[16].

Eppure, l'emersione di autorità private, e delle soluzioni da esse dettate, è rappresentativa di un fenomeno economico-sociale che non può prescindere dal rispetto delle regole giuridiche, alle quali spetta comunque dare legittimazione ai poteri degli operatori, in funzione non soltanto della regolazione dei mercati, ma soprattutto della tutela dei diritti fondamentali della persona[17]. A tal fine, come si avrà modo

---

A. ZOPPINI (a cura di), *I poteri privati e il diritto della regolazione. A quarant'anni da «Le autorità private» di C.M. Bianca*, Roma, 2018.

[14] Per una panoramica generale, A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Firenze, 2020.

[15] A partire dalla sentenza CGUE, 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, nonché di recente CGUE, 24 settembre 2019, causa C-136/17, *GC e a. contro Commission nationale de l'informatique et des libertés (CNIL)*, confermato anche dall'EDPB, *Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca*, 7 luglio 2020, reperibili *online* all'indirizzo https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_it.pdf. Sui rapporti tra diritto all'informazione e diritto all'oblio, per tutti, G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio dopo la sentenza Google Spain*, Roma, 2015.

[16] Di recente, Cass., sez. I, 8 febbraio 2022, n. 3952, in *OneLegale*, ove si rammenta che «attraverso la deindicizzazione l'informazione non viene eliminata dalla rete, ma può essere attinta raggiungendo il sito che la ospita (il cosiddetto sito sorgente) o attraverso altre metodologie di ricerca, come l'uso di parole-chiave diverse»; ma cfr. anche Trib. Milano, 5 settembre 2018, in *Danno e resp.*, 2019, p. 122 ss., con nota di S. BONAVITA, *Deindicizzazione: tecnologie abilitanti ed evoluzione del rapporto tecnologia e diritto*, per il quale il *de-listing* sembra assumere i contorni di una tecnologia applicabile alla tutela di diritti anche diversi dall'oblio.

[17] Nel primo senso, proprio al fine di "responsabilizzare" lo strapotere assunto dai *gatekeeper*, si inserisce, da ultimo, il Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale (meglio noto come *Digital Markets Act*); nel secondo, ovviamente, il

di vedere, pare opportuno aggiungere alla norma di fonte eteronoma, l'elaborazione di linee guida, raccomandazioni, *best practices*, certificazioni, codici di condotta, misure di sicurezza e finanche prodotti tecnologici a tutela dei dati personali, che incidano direttamente sui rapporti tra i titolari del trattamento e gli interessati, conformandoli[18]. In ogni caso, al riconoscimento esplicito della libertà di scelta dettata dall'autoregolamentazione interna – declinazione del principio di sussidiarietà orizzontale[19] – è pur sempre necessaria una verifica esterna delle misure tecniche ed organizzative costitutive del trattamento di dati personali (*accountability*[20]), specialmente ad opera delle autorità di controllo[21], favorita dal legislatore in un contesto regolatorio e procedimentalizzato dei mercati digitali[22].

2.2. Le *Privacy Enhancing Technologies*

Nel contesto sopra brevemente illustrato, vengono continuamente ad intrecciarsi la normazione e l'automazione, sicché diritto e tecnologia si trovano legati in un connubio *funzionale*, regolamentare, da un lato, e operativo, dall'altro[23].

Il riferimento va subito ristretto alle c.d. *Privacy Enhancing Technologies* (*PETs*)[24], che già dagli anni '90 del secolo scorso sono state

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, conosciuto anche con l'acronimo GDPR.

[18] G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, p. 234.

[19] P. LAGHI, *Cyberspazio e sussidiarietà*, Napoli, 2015, *passim*.

[20] Per tutti, G. FINOCCHIARO, *Il principio di* accountability, in *Giur. it.*, 2019, p. 2778 ss.

[21] Sul punto, F. PIZZETTI, *Le Autorità garanti per la protezione dei dati personali e la sentenza della Corte di Giustizia sul caso Google Spain: è tempo di far cadere il "velo di maya"*, in *Dir. inf.*, 2014, p. 805 ss.

[22] Cfr. P. PERLINGIERI, Privacy *digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, p. 482.

[23] A. PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy: privacy by design *e* privacy by default settings, in *Contr. impr./Europa*, 2015, p. 198.

[24] H. VAN ROSSUM, H. GARDENIERS, J.J. BORKING, A. CAVOUKIAN, J. BRANS, N. MUTTUPULLE, N. MAGISTRALE, *Privacy-Enhancing Technologies: The Path to Anonymity*, The Hague, 1995; S. FISCHER-HUBNER, S. BERTHOLD, *Privacy-Enhancing Technologies*, in J. R. VACCA (edited by), *Computer and Information Security Handbook*, 3th ed., Amsterdam, 2017, pp. 759-778.

invocate per realizzare un nuovo approccio alla protezione dei dati personali, noto come *privacy by design*[25] e meglio definibile oggi nella *data protection by design*[26]. Si tratta di un principio che è stato fatto proprio dal Regolamento 2016/679/UE (in avanti, GDPR), posto che, sulla base di una analisi *ex ante* dei rischi e delle circostanze concrete attinenti al trattamento di dati personali, è necessaria non solo la configurazione dei sistemi computazionali idonei a garantirne la legittimità, bensì la predisposizione, sin dal principio, di misure tecniche e organizzative rispondenti alla protezione dei dati personali e ai principi che la governano (art. 25, par. 1, GDPR)[27].

Possono essere considerate *PETs*, in generale, «*systems encompassing technical processes, methods, or knowledge to achieve specific privacy or data protection functionality or to protect against risks to privacy of an individual or a group of natural persons*»[28]. Seguendo la definizione riportata, il concetto è davvero vastissimo e le sue concrete applicazioni innumerevoli. Qui non si intendono sondare le varie tecniche di anonimizzazione (k-*anonimity*, *differential privacy*, etc.) o di elaborazione computazionale distribuite, né indagare sofisticate misure di sicurezza (*homomorphic encryption*)[29]; diversamente, lo sguardo è rivolto verso quelle tecnologie che permettono al titolare del trattamento di implementare, in pratica, il principio generale della *trasparenza* (art. 5, par. 1, lett. *a*, GDPR), nonché garantire un *empowerment* dell'interessato attraverso un effettivo esercizio del potere di controllo dei dati personali, riconducibile al più ampio diritto fondamentale alla loro protezione[30].

---

[25] Per tutti, A. CAVOUKIAN, *Privacy by Design – The 7 Foundational Principles*, August 2009 (revised January 2011), reperibile *online* all'indirizzo https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[26] Come si sottolinea in M. VEALE, R. BINNS, J. AUSLOOS, *When data protection by design and data subject rights clash*, in *Int. Data Privacy Law Rev.*, 2018, p. 2, la mutata espressione non è solo ideologica, dal momento che lo scopo principale del GDPR è la protezione dei dati personali; *amplius*, L. A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in *Oslo Law Review*, 4(2), 2017, p. 105 ss.

[27] Per un primo commento, R. D'ORAZIO, *Protezione dei dati* by default *e* by design, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, p. 79 ss.

[28] ENISA, *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan*, 2015, p. 9.

[29] Per una analisi completa, si rinvia a G. D'ACQUISTO, M. NALDI, Big data *e* privacy by design. *Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017.

[30] Sulla differenza tra strategie di *front-end* rispetto a quelle di *back-end*, vedasi A. PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy, cit., p. 200, dove si afferma: «Infatti, nel momento *back-end*, il *design* riguarda i modi di conservazione e trattamento dei dati

Tutto ciò rappresenta un momento essenziale per incrementare altresì la *fiducia* nei mercati digitali, onde evitare reazioni meramente inibitorie da parte degli utenti della Rete, come il rifuggire dal *Web*, in chiara ottica oppositiva[31]. Il compito svolto dalle *PETs* improntate ad una maggiore trasparenza assume, quindi, una posizione di prim'ordine; tant'è che la Commissione europea, di recente, ne ha sottolineato la complementarità rispetto all'attuale quadro normativo, già in vigore o in preparazione, deputato alla regolazione dei traffici nell'era dei *Big Data*[32].

Due precisazioni appaiono necessarie, discorrendo di *PETs*.

La prima, avente carattere preliminare, è che deve essere abbandonata una logica meramente difensiva delle situazioni giuridiche ascrivibili all'interessato. La protezione dei dati personali non si pone, infatti, in posizione conflittuale rispetto all'uso delle tecnologie dell'informazione e della comunicazione e ai loro derivati; al contrario, i diritti del singolo, tra i quali la riservatezza e l'identità personale, vengono costantemente attraversati da altri e diversi interessi, privati o pubblici, che rendono legittime le varie operazioni eseguite con i dati di qualcuno, o perché volontariamente questi si è così determinato, o perché si fa riferimento ad attività necessarie alla stregua di particolari finalità, ritenute meritevoli di tutela, e nel caso specifico prevalenti, perseguite da un soggetto diverso dall'interessato[33].

già acquisiti, e deve assicurare il rispetto di quanto previsto a livello legislativo e contrattuale, assicurando una corretta fruizione dei dati sia a livello di chi tratta i dati sia di parti terze. Il momento *front-end* invece guarda a quanto avviene nel momento in cui l'utente si interfaccia con il servizio fornitogli, a come si acquisiscono i dati personali del soggetto. In quest'ultimo caso, lo scopo deve essere quello di fornire all'utente le necessarie informazioni sui dati che verranno acquisiti e di accrescere il controllo dello stesso su esse».

[31] Si pensi alla ritrosia verso gli *advertising cookies*, con il ricorso a strumenti di *ad-blocking*, operanti come una sorta di "autodifesa" del soggetto dinanzi alla tecnologia adoperata dai servizi digitali, così S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 26.

[32] COMM. EU, *Una strategia europea per i dati*, 19.2.2020 COM(2020) 66 final, p. 22, ove sono definite le "coordinate" fondamentali per le prossime fasi dell'economia dei dati.

[33] Sulla natura relazionale del diritto alla protezione dei dati personali, si veda il *considerando* § 4 del GDPR. In argomento, diffusamente, A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2017, p. 591 ss., ma già F. D. BUSNELLI, *Dalla legge al «codice»: un dilemma, una sfida, un consolidamento normativo, una (imperfetta) razionalizzazione delle tutele*, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, 2007, p. XXXIX.

Con l'evolversi della *data-driven economy* e dell'attitudine dell'informazione a fungere da elemento redditizio a molteplici modelli di *business* – ma anche semplicemente considerando la crescente digitalizzazione della vita quotidiana su svariati fronti – non si può pensare che la tutela dei dati personali possa essere lasciata unicamente al singolo, almeno nel senso di pretesa azionabile dinanzi all'autorità, giudiziaria o amministrativa che sia: o perché l'interessato è strutturalmente debole dinanzi all'irresistibile processo di innovazione che fagocita sempre più dati[34]; o semplicemente per la sua scarsa propensione ad agire, dovuta alla mancata comprensione circa l'immissione delle informazioni in Rete, in forza del già ricordato *privacy paradox*. Così, al fine di riempire di contenuto il diritto alla protezione dei dati personali, la disciplina europea prescrive che il titolare del trattamento sia tenuto a certi obblighi di informazione e ad adottare precise misure tecniche ed organizzative per la tutela degli interessati[35]: la (libera) circolazione delle informazioni riferibili ad una persona fisica è garantita in quanto il trattamento di dati personali sia rivolto a finalità considerate legittime e soprattutto accompagnato da *modalità* che si mostrino, in concreto, rispondenti alla protezione dei diritti della persona[36].

L'altra considerazione cui si accennava ha essenzialmente carattere sistematico. In riferimento alla *data protection by design*, il ruolo del diritto sembra essere quello di orientare, in concreto, la scelta della

---

[34] La debolezza dello strumento della responsabilità aquiliana, per esempio, dinanzi a danni «per definizione seriali e massivi», è sottolineata da C. CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus Civile*, 3, 2020, p. 810.

[35] Il cambio di paradigma del GDPR rispetto alla precedente Direttiva 1995/46/CE è rinvenibile proprio nella gestione del rischio del trattamento dei dati personali, il quale impone l'adozione di una serie di obblighi in capo ai soggetti attivi del trattamento. In questa prospettiva, A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 144 ss. Nell'estendere l'istituto degli "obblighi di protezione" alle misure tecniche ed organizzative cui è tenuto ad adottare il titolare (ed il responsabile) del trattamento, l'impostazione seguita da F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 775 ss., spec. p. 787. Per lo sforzo di combinare ordinamento interno e legislazione comunitaria, riconducendoli a razionalità, si rinvia a A. GENTILI, *Il diritto come discorso*, in *Trattato di diritto privato*, diretto da G. Iudica e P. Zatti, Milano, 2013, p. 227 ss.

[36] Sul punto, cfr. F. G. VITERBO, *The 'User-Centric' and 'Tailor-Made' Approach of the GDPR Through the Principles It Lays down*, in *The Italian Law Journal*, 5(2), 2019, p. 637, secondo il quale «[t]*he problem is establishing whether and how personal data may be processed in each specific concrete online or offline context. That is to say, whether and how the data subject's fundamental rights may be preserved*».

tecnologia più rispondente all'attuazione delle norme che regolano la protezione dei dati personali[37]. Compito del giurista, in particolare, è quello di fornire chiare indicazioni per l'implementazione, pratica ed effettiva, della disciplina applicabile alla protezione dei dati a tutti coloro che si trovano non solo a dover ideare, programmare o sviluppare sistemi informatici, ma anche a *scegliere* quali tra le più diverse tecnologie preposte al trattamento utilizzare[38].

La regola giuridica deve essere, pertanto, letta di concerto alla tecnica, allo scopo di darne effettività[39]. Si può parlare quindi di un *technological enforcement* della protezione dei dati personali, in modo da garantire non solo il corretto funzionamento dei mercati digitali, ma anche e soprattutto la tutela della persona dell'utente[40], alla stregua di quanto è stato definito un vero e proprio "*New Deal*" per il diritto dei consumatori[41].

---

[37] Cfr. B.J. KOOPS – R. LEENES, *Privacy Regulation Cannot Be Hardcoded. A critical comment on the 'privacy by design' provision in data protection law*, in *Int. Rev. Law, Computers & Technology*, 2014(28), p. 168, ove si afferma che la *privacy by design* «*should not be read as a procedural requirement to embed data protection rules as much as possible in system design, but instead as a substantive requirement calling upon data controllers to consistently keep privacy at the front of their minds when defining system requirements*». Ancora, S. RODOTÀ, *Libertà, opportunità, democrazia, informazione*, relazione introduttiva al Convegno intitolato "*Internet e privacy - Quali regole?*", Roma, 8 maggio 1998, reperibile *online* all'indirizzo *https://www.privacy.it/archivio/garanterelrod.html*: «Le *privacy enhancing technologies* richiedono questo tipo di riflessione; il riferimento alle norme giuridiche richiede altrettanta riflessione critica. Che tipo di norme giuridiche? Norme giuridiche di tipo stringente o norme giuridiche elastiche, capaci di autoadattarsi alle situazioni che cambiano? Questa è una domanda alla quale dobbiamo rispondere».

[38] Cfr. *considerando* § 78: «(…) In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati».

[39] In una siffatta impostazione, dove l'efficacia giuridica è determinata da regole tecniche non tradotte in regole di fonte legislativa o contrattuale, C. PERLINGIERI, *Profili civilistici dei* social networks, Napoli, 2014, p. 20, nonché P. FEMIA, *Una finestra sul cortile. Internet e il diritto all'esperienza metastrutturale*, in C. PERLINGIERI, L. RUGGERI, *Internet e Diritto civile*, Napoli, 2015, p. 38.

[40] Sulla duplicità di propositi che animano la disciplina europea dei dati personali, N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in Id. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano-Padova, 2019, p. 35 ss.

[41] COMM. EU, *Un "New Deal" per i consumatori*, 11.4.2018, COM(2018) 183 final, p. 4, ove si legge: «Il "*New Deal per i consumatori*" prende le mosse dal quadro esistente della

2.3. Il problema degli strumenti della conoscenza

Non c'è da stupirsi oggi della compiuta perdita di controllo sul flusso di dati personali da parte dell'individuo, da tempo ormai fatta palese[42]. Passando in rassegna le varie "versioni" del *Web*[43], oggi si parla di "vita iper-connessa" – un cambiamento che reca con sé alcuni neologismi, quali il termine *onlife*, che ben esprime la non più netta cesura fra reale e virtuale[44] – la quale si esplica non soltanto nei mercati digitali, ma anche nei rapporti con le pubbliche amministrazioni e, in generale, fra gli stessi consociati (paradigmatico è il caso dei *social network*). Un "ecosistema", questo, dove le attività quotidiane su scala globale ruotano attorno all'utilizzo di dati e le operazioni sono effettuate utilizzando tecnologie *hardware* e soprattutto *software* sempre più sofisticate e, per ampi tratti, riconducibili alle applicazioni dell'Intelligenza Artificiale[45].

Posto che la circolazione di (nuovi) dati personali è incessante e proviene dall'intera comunità digitale – come la pandemia da Covid-19 ha di recente mostrato – altrettanto proporzionalmente decresce però la consapevolezza che ciascuno ha in relazione al trattamento di dati personali. Problemi questi acuiti dall'utilizzo massiccio di assistenti vocali, *wearables*, dall'*Internet of Things*, ove l'utente è tendenzialmente ignaro circa la raccolta di dati personali, per l'assenza o a causa

politica dei consumatori e compie un passo in avanti proponendo norme moderne e adeguate ai mutevoli mercati e prassi commerciali di oggi, strumenti giuridici più efficaci a livello pubblico e privato e migliori possibilità di ricorso». Nella prospettiva tecnologica qui approcciata, v. altresì lo studio intitolato *New aspects and challenges in consumer protection. Digital services and artificial intelligence*, commissionato dallo *European Parliament's committee on the Internal Market and Consumer Protection*, reperibile *online* all'indirizzo https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648790/IPOL_STU(2020)648790_EN.pdf, spec. p. 26 s.

[42] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 82 ss.

[43] K. C. A. Khanzode, R. D. Sarode, *Evolution of the World Wide Web: from Web 1.0 to 6.0*, in *Int. Journal of Digital Library Services,* 6(2), 2016, p. 1 ss.

[44] Interessante ricordare il neologismo "*onlife*", utilizzato da Luciano Floridi, per indicare l'assenza di confini tra la vita *online* e *offline* e, quindi l'assenza di distinzione, dalla prospettiva dell'utente, tra virtuale e reale. V. L. Floridi (ed. by), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, 2015.

[45] Per una panoramica, U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

delle ridotte dimensioni dell'interfaccia grafica del servizio che gli viene reso.

Andando a fondo sul punto, il tema non è tanto legato alla mancanza di trasparenza circa le finalità o i propositi delle operazioni compiute con i dati personali; il problema sembra rinvenirsi piuttosto nella rappresentazione, in concreto, di quali dati personali vengono raccolti, conservati, diffusi, e così via: questi processi – quand'anche fossero comprensibili – rimangono per lo più inaccessibili, nella pratica, per l'interessato, alimentando il *privacy paradox*[46].

Facendo un esempio: coloro che utilizzano intensivamente lo *smartphone* non sono in grado di visualizzare, sia pur in maniera approssimativa, quanti dati sono stati raccolti, nel tempo, effettuando acquisti *online*, utilizzando piattaforme di *car sharing* o *food delivery*, e così via. Ciò si traduce, al di là della mancata percezione delle insidie circa i dati messi in circolo, molto spesso in subdole profilazioni[47], fino a sfociare in limitazioni ovvero discriminazioni, tanto da potersi affermare un nuovo tipo di capitalismo, detto "della sorveglianza"[48].

Tutto ciò è il derivato di un modello di tutela oltremodo inefficiente.

Anzitutto, vi è il diffuso approccio "*notice and consent*", consistente nell'approvazione, da parte dell'interessato, di lunghe, spesso vaghe o, all'opposto, particolarmente dettagliate "informative sul trattamento" – scritte, peraltro, in un linguaggio poco intellegibile ai più[49]: nonostante l'obbligo di fornire all'interessato le informazioni circa il trattamento dei dati personali, l'utente si trova fisiologicamente a

---

[46] Il rapporto tra informazione e trasparenza, dopotutto, è di mezzo a fine, così R. SENIGAGLIA, *Accesso alle informazioni e trasparenza. Profili della conoscenza nel diritto dei contratti*, Padova, 2007, p. 113.

[47] Sui rapporti tra profilazione e il fenomeno della "*filter bubble*", frutto di un uso automatizzato dei dati attraverso algoritmi che crea un effetto di isolamento, in quanto il soggetto è chiuso nel suo profilo, M. BIANCA, *La* filter bubble *e il problema dell'identità digitale*, in *MediaLaws – Rivista di diritto dei media*, 2019, 2, p. 1 ss.

[48] Celebre è il volume di S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (trad. it.), Roma, 2019.

[49] H. NISSENBAUM, *A Contextual Approach to Privacy Online*, in *Daedalus*, 140(4), 2011, p. 32 ss.; A. MANTELERO, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law and Security Rev.*, 30, 2014, p. 643 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, p. 339 ss. Più di recente, IDD., *Privacy and Consent. A Legal and UX&HMI Approach*, Napoli, 2021.

dover accettare i termini di servizio pure con riguardo all'utilizzo dei dati, sulla base della condizione (implicita) "*take it or leave it*".

Ancora, poco importa che il GDPR abbia (ri-)affermato una serie di diritti dell'interessato, quali l'accesso ai dati personali, la revoca del consenso, la cancellazione, ecc., se poi l'assolvimento delle richieste presentate da parte del titolare del trattamento rimane ancora lento e macchinoso: non sempre l'interessato si convince ad agire, dal momento che, per la rapidità in cui si muove la realtà virtuale, anche solo spedire una *e-mail* sembra (paradossalmente) essere troppo dispendioso.

Analoghe considerazioni valgono nell'ipotesi di *data breach* [50]: quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve informare l'interessato della natura della violazione, descrivendo «ove possibile (…) le categorie e il numero approssimativo di registrazioni dei dati personali in questione» (art. 33, par. 3, lett. *a*, GDPR). Difficilmente però l'utente è in grado di capire la serietà e la gravità della violazione, se non altro perché non risulta pienamente consapevole della quantità e della qualità di dati personali precedentemente collezionati.

La sfida che qui si delinea – evidenziata anche nella Strategia Europea per i dati[51] – interroga l'ordinamento giuridico sul *come* coinvolgere gli interessati all'interno delle operazioni costituenti trattamento di dati personali, al fine rendere effettivo l'esercizio dei diritti loro riconosciuti[52]. Un compito che sembra essere stato lasciato dal legislatore eurounitario agli stessi titolari del trattamento, mediante un approccio valutativo *ex ante* e basato sul rischio di pregiudizio concreto che l'uso dei dati personali possa determinare in capo ai diritti e alle libertà fondamentali della persona. Ne discende, infatti, l'obbligo per chi utilizza i dati personali di mettere in atto (ed essere in grado di dimostrare l'adozione di) misure organizzative ma soprattutto

[50] Art. 4, par. 1, n. 12, GDPR: «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

[51] COMM. EU, *Una strategia europea per i dati*, cit., p. 23: «È opportuno sostenere ulteriormente le persone nell'esercizio dei loro diritti per quanto riguarda l'utilizzo dei dati che generano, dando loro la possibilità di controllare i propri dati attraverso strumenti e mezzi per poter decidere di volta in volta in dettaglio ciò che può essere fatto con essi».

[52] Quanto all'attuazione del principio di effettività e, alle sue applicazioni concrete, di recente, G. VETTORI, *Effettività fra legge e diritto*, Milano, 2020, p. 63 ss.

tecniche che siano adeguate allo scopo rappresentato e in funzione dei presunti rischi, aventi probabilità e gravità diverse a seconda del trattamento da effettuarsi (art. 24 GDPR)[53].

Individuando un *continuum* sotto il profilo gestionale[54], l'espressa enunciazione del principio della *data protection by design* (art. 25 GDPR) richiama proprio il dovere per il titolare di predisporre misure tecniche e organizzative che siano *adeguate* al trattamento dei dati personali. Ciò non è privo di conseguenze sotto il profilo giuridico, finendo per legittimare la costruzione "fattuale" (*recte* para-normativa) delle regole concernenti i rapporti tra soggetti nell'ambito del trattamento dei dati personali[55]: ancorché i controlli esterni, si avrà modo di vedere, non vengano comunque meno, la legislazione sembra qui arrestarsi, demandando alle forme dell'autoregolamentazione privata, in quanto più vicina agli interessi da disciplinare, il compito di stabilire il complessivo assetto di dettaglio[56].

Operando un mutamento di prospettiva, la questione della trasparenza del trattamento, in particolare, va affrontata allora non tanto sul piano dell'*an*, posto che ricevere certe informazioni è atto dovuto, quanto sul terreno del *quomodo*, cioè con riguardo alle modalità attraverso cui l'interessato può ricevere una rappresentazione chiara e trasparente delle operazioni eseguite con i dati personali. Del resto, quello che ad oggi manca non è tanto l'ideazione, quanto l'implementazione, pratica ed effettiva, di infrastrutture, processi e soluzioni informatiche, quali le *Privacy Enhancing Technologies*, che permettano all'interessato di acquisire, con semplicità e immediatezza, e in

---

[53] Ancora, *considerando* § 74: «È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche».

[54] Cfr. S. CALZOLAIO, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *federalismi.it*, 20 dicembre 2017, p. 14.

[55] In questo senso, F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 801, p. 817, ove si richiama la tesi elaborata da M. MAGGIOLO, *Il contratto predisposto*, Padova, 1996, p. 196 ss., secondo il quale con riguardo ai rapporti giuridici (anche diversi da quelli contrattuali) può aversi un allestimento di un assetto rilevante nella sua materialità, che diviene oggetto di un potere di gestione pur sempre riconducibile all'autonomia privata.

[56] Così P. LAGHI, *Cyberspazio e sussidiarietà*, cit., p. 213.

sicurezza, una migliore comprensione circa la raccolta, l'uso e la circolazione dei dati personali nell'ambito dei servizi della società dell'informazione.

2.4. L'inclusione dell'interessato nella gestione dei dati personali: i *Personal Information Management Systems*

La soluzione proposta con le specifiche *PETs* volte a rafforzare la trasparenza del trattamento – denominate, per questi motivi, *Transparency Enhancing Tools*[57] – è senza dubbio di segno opposto rispetto alle derive espansionistiche della «società della sorveglianza»[58].

L'interessato viene qui coinvolto, in prima persona, nella gestione dei dati, in modo tale che sia accresciuta la sua consapevolezza del trattamento, almeno nell'accezione "minima" di controllo (ad esempio, con chi condivido i dati, per quanto tempo, per quali finalità, etc.). Tuttavia, non basta soltanto fornire la visualizzazione in tempo reale dei dati personali raccolti dal titolare del trattamento, bensì tali meccanismi tecnici devono agevolare altresì il concreto e pratico esercizio dei diritti riconosciuti all'interessato, come la cancellazione, la rettifica, la revoca del consenso, la portabilità dei dati personali, e così via.

Nella prospettiva delineata, particolare rilievo assumono i c.d. *Personal Information Management System* – che forse sarebbe più opportuno rinominare, alla luce del GDPR, *Data Protection Management Tools*[59]. Si tratta di una "architettura" di trattamento dei dati personali consistente per lo più in sistemi *software* mediante i quali l'utente interviene direttamente nel processo di raccolta, conservazione e diffusione dei dati, venendosi a creare, programmaticamente, una nuova realtà «in

---

[57] D. Spagnuelo, A. Ferreira, G. Lenzini, *Transparency Enhancing Tools and the GDPR: Do They Match?*, in P. Mori, S. Furnell, O. Camp (edited by), *Information Systems Security and Privacy*, Cham, 2020, p 162 ss.; C. Zimmermann, A *Categorization of Transparency-Enhancing Technologies*, in *arXiv*, 2015, https://arxiv.org/ftp/arxiv/papers/1507/1507.04914.pdf.

[58] D. Lyon, Z. Bauman, *Sesto potere. La sorveglianza nella modernità liquida*, Roma-Bari, 2014.

[59] Per una prima analisi, EDPS, *Opinion 9/2016 on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data*, 20.10.2016, reperibile *online* all'indirizzo https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf, nonché, da ultimo, EDPS, *Opinion 3/2020 on the European startegy for data*, 16.6.2020, reperibile *online* all'indirizzo https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf.

cui le persone gestiscono e controllano la propria identità *online*»[60]. Ciò è reso possibile attraverso il coinvolgimento *diretto* degli interessati, i quali possono interagire con i propri dati, per esempio, scegliendo i destinatari con cui condividerli ovvero le categorie di informazioni oggetto di trattamento ulteriore per finalità diverse da quelle iniziali, o ancora eliminando particolari contenuti informativi, considerati non più rilevanti. Sicché l'obiettivo di garantire una più *accessibile* gestione dei dati personali – dal ricevere le informazioni in merito al trattamento in essere sino all'effettivo esercizio del diritto alla cancellazione – trova una risposta attraverso l'implementazione di semplici e immediate soluzioni interattive di tipo "*point and click*"[61].

Potenzialmente, un sistema del genere permette di riequilibrare, per un certo verso, l'asimmetria (informativa) per la quale l'interessato manca, di fatto, degli strumenti tecnici per controllare adeguatamente il trattamento di dati personali. Così, l'approccio statico, ancora largamente diffuso tra i titolari del trattamento, dovrebbe dirigersi verso un'inclusione *dinamica* dell'interessato all'interno della gestione dei dati personali. In questo modo, sembra mutare anche il ruolo assunto della persona fisica, da soggetto passivo, inerte, a parte attiva dell'economia digitale, rafforzandosi l'autodeterminazione informativa del singolo.

È bene notare come una maggiore trasparenza non deve assolutamente condurre all'esito opposto di *information overload*, nell'ipotesi di troppe informazioni specifiche che non beneficiano affatto l'utente (e neanche il fornitore del servizio digitale): i criteri da seguire, e che limitano la discrezionalità di chi adotta, in pratica, le diverse tecnologie, sono quelli della necessità, della proporzionalità e della

---

[60] Testualmente «*[t]he PIMS concept offers a new approach by which individuals are the holders of their own personal information*»: così EDPS, Opinion 9/2016, cit., p. 5.

[61] H. JANSSEN, J. COBBE, J. SINGH, *Personal information management systems: a user-centric privacy utopia?*, in *Internet Policy Review*, 9(4), 2020, p. 1 ss.; A. CRABTREE, T. LODGE, J. COLLEY, C. GREENHALGH, K. GLOVER, H. HADDADI, Y. AMAR, R. MORTIER, Q. LI, J. MOORE, L. WANG, P. YADAV, J. ZHAO, A. BROWN, L. URQUHART, D. MCAULEY, *Building accountability into the Internet of Things: the IoT Databox model*, in *Journal of Reliable Intelligent Environments*, 4(1), 2018, p. 39 ss.; A. POIKOLA, K. KUIKKANIEMI, H. HONKO, *MyData – A Nordic Model for human-centered personal data management and processing*, 2015, [white paper], reperibile *online* all'indirizzo https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf.

ragionevolezza di ciò che dev'essere visualizzato[62]. In questo senso, è opportuno sia attribuita una attenzione particolare alle preferenze di coloro che usufruiscono dei diversi servizi della società dell'informazione[63]: l'accettabilità e l'usabilità degli utenti sono elementi fondamentali dei quali tenere conto nelle scelte delle misure tecniche da adottare in concreto[64].

Ancora una volta, sono facilmente comprensibili i limiti che incontra la regolazione, se intesa soltanto come normazione pubblica eteronoma, in ragione della rapida obsolescenza delle regole di dettaglio dinanzi all'innovazione tecnologica[65]; o ciò che è lo stesso, pare impossibile prescindere, in questi casi, dal potere normativo dei soggetti privati nella protezione dei dati personali. Più precisamente, al fine di rafforzare la tutela della persona nell'ambiente digitale, non può non considerarsi il ruolo assunto dai titolari del trattamento, ai quali è affidato l'obbligo di garantire che i mezzi mediante i quali si realizza il trattamento di dati personali siano rispondenti ai principi generali applicabili alla protezione dei dati personali; ciò nell'ottica di quella *accountability* sopra ricordata, per la quale si rende necessaria l'adozione di misure tecniche e organizzative – sistemi, processi, protocolli, tecnologie[66] – *adeguate* al tipo di trattamento da espletarsi, tenuto conto «dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i

---

[62] Per una completa analisi del principio di ragionevolezza e di proporzionalità nel diritto civile, G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015.

[63] A. Mantelero, Digital privacy*: tecnologie "conformate" e regole giuridiche*, in F. Bergadano, A. Mantelero, G. Ruffo, G. Sartor (a cura di), Privacy *digitale. Giuristi e informatici a confronto*, Torino, 2005, p. 19 ss.

[64] Seppur in ambito parzialmente diverso, pare opportuno richiamare quanto affermato da Art. 29 WP, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, reperibili *online* all'indirizzo https://ec.europa.eu/newsroom/article29/items/612053: al titolare del trattamento è imposto di fornire informazioni sulla logica utilizzata nei processi decisionali automatizzati, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati. Le informazioni fornite dovrebbero comunque essere sufficientemente complete affinché l'interessato possa comprendere i motivi posti alla base della decisione.

[65] D. Di Sabato, *Diritto e* new economy, Napoli, 2020, p. 27.

[66] Cfr. F. Romeo, *Il governo giuridico delle tecniche dell'informazione e della comunicazione*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 1261: «Il diritto deve essere costruito dentro alla tecnica stessa, per evitare l'attuale stato di ineffettività di tante statuizioni ed inapplicabilità di tante interpretazioni».

diritti e le libertà delle persone fisiche costituiti dal trattamento» (art. 25, par. 1, GDPR), coniugando di quest'ultimo l'aspetto strutturale con la funzione che la protezione dei dati personali intende garantire nei confronti dell'interessato[67].

2.5. Il principio di *data protection by design* come criterio di selezione

Si è visto, discorrendo di *data protection by design*, che l'elemento strutturale relativo alla predisposizione delle tecnologie del trattamento si salda con l'aspetto funzionale cui esse sono rivolte, allo scopo di garantire, per un verso, la legittimità del trattamento, la trasparenza, la minimizzazione dei dati, etc., nonché la tutela dell'interessato, rendendo finanche possibile l'esercizio pratico dei diritti a quest'ultimo riconosciuti dal GDPR[68].

Non è corretto però ritenere che le *Privacy Enhancing Technologies* debbano intervenire soltanto *a posteriori*, per rinforzare, alla stregua di particolari misure di sicurezza, i principi e le regole relative al trattamento su sistemi non pensati *ex ante* per integrare nella loro struttura la protezione dei dati personali[69]. Diversamente, la strategia portata avanti con le *PETs* richiede la scelta ponderata di tecnologie adeguate alla normativa sulla protezione dei dati personali già in fase di programmazione delle operazioni da svolgersi, secondo un *prius* logico

[67] Per R. D'ORAZIO, *Protezione dei* dati by default *e* by design, cit., p. 83, l'operare dell'art. 25 GDPR si esplica in un quadro variabile, in relazione sia alla gravosità dell'impegno, sia in base ai costi da sostenere.

[68] Ciò trova conferma in una lettura teleologicamente orientata dell'art. 25, par. 1, GDPR, laddove «(…) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (…) volte ad attuare in modo efficace i principi di protezione dei dati (…) e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».

[69] Cfr. S. CALZOLAIO, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, cit., p. 16. Come osserva R. D'ORAZIO, *Protezione dei* dati by default *e* by design, cit., p. 103, le *PETs* sono frutto di un approccio "ingegneristico" alla tecnologia volto a ricavarne dispostivi più "virtuosi" di tutela dei dati personali, mentre le "misure" di cui all'art. 25 GDPR riflettono una concezione più ampia, la quale unisce l'elemento tecnologico con le regole giuridiche che condizionano il trattamento dei dati personali.

rispetto al successivo trattamento[70]. Infatti, l'adozione di talune soluzioni, tra quelle messe a disposizione del titolare, non incide soltanto sul momento ideativo del trattamento, in modo statico[71]; al contrario, le misure predisposte sono pensate, in quanto congegnate già in fase di programmazione delle attività come indirizzate alla protezione dei dati personali, per coprire l'intero "ciclo vitale" del trattamento, e come tali richiedono un costante aggiornamento, in maniera dinamica[72].

Ora, è pacifico che il GDPR abbia recepito il principio di *digital neutrality*, secondo il quale la norma giuridica non consiglia l'adozione di una o l'altra tecnologia[73]. Eppure, la scelta di una certa tecnologia è influenzata dalla regola giuridica da applicare, la quale, sia pur nella complessità dell'ordinamento, seleziona gli interessi meritevoli di protezione nel caso concreto e li colloca entro una scala assiologica[74]; così accade anche per le norme poste a presidio del trattamento dei dati personali, le quali, nel contesto applicativo, pure quando si relazionano con gli apparati tecnologici, rispondono comunque agli scopi di tutela tracciati dal diritto[75].

---

[70] Cfr. EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, v. 2.0, 20.10.2020, reperibili *online* all'indirizzo https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, p. 10, ove si afferma che «(…) *from a cost-benefit perspective, it is also in controllers' interest to take DPbDD into account sooner rather than later, as it could be challenging and costly to make later changes to plansthat have already been made and processing operations that have already been designed*».

[71] Se non per i c.d. *system level requirements* come osservano B.J. KOOPS, R. LEENES, *Privacy Regulation Cannot Be Hardcoded*, cit., p. 162.

[72] F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 790.

[73] Cfr. *considerando* § 15: «Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate». Sul punto, D. FARACE, Privacy by design *e* privacy by default, in E. TOSI (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 499.

[74] Lo sottolinea C. PERLINGIERI, *La tutela dei minori di età nei* social networks, in *Rass. dir. civ.*, 2016, p. 1331, in quanto le regole tecniche, se sono di per sé neutrali, perdono il carattere della neutralità quando divengono struttura logica di interconnessioni soggettive e devono essere valutate sotto il profilo della legittimità.

[75] Così anche S. RODOTÀ, *Libertà, opportunità, democrazia, informazione*, cit., secondo il quale «[n]on siamo di fronte a tecnologie neutre, neutrali; siamo di fronte a tecnologie in cui si manifesta al massimo grado la forza di modello sociale della rete e quindi esigono una seria discussione sul quadro istituzionale, all'interno del quale noi possiamo muoverci e dobbiamo muoverci». Del resto, il GDPR intende porsi come uno *standard* globale di tutela dei dati personali, come affermato da G. BUTTARELLI, *The EU*

Del resto, come il diritto può vietare il ricorso a certi strumenti tecnologici, viceversa, la tecnica può determinare l'inefficacia della norma giuridica[76]: la questione allora non è tanto quali regole o quali tecniche adottare, in astratto; il nodo cruciale sta nell'individuare una connessione *teleologica* tra le finalità perseguite (e gli interessi coinvolti) nel trattamento di dati personali e i mezzi con i quali esso si esplica, in concreto, avuto riguardo alla *scelta* della tecnologia da adottare, alla luce della tutela della persona. In questo senso, la prerogativa di stabilire ciò che è lecito o meno nell'uso di una certa tecnologia spetta al diritto, il quale determina così una funzionalizzazione degli interessi (*recte* conformazione) anche con riferimento alla tecnica.

Facendo un esempio: la quantità e la qualità di informazioni rese all'interessato in merito al trattamento possono essere rappresentate in varie forme, ma alcune modalità – e le conseguenti misure da adottare – rimangono più adeguate di altre per accrescere la trasparenza e l'accesso alle informazioni da parte dell'utente, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

a) Una efficace rappresentazione sia dei dati personali, sia del trattamento, trascorre necessariamente per l'interfaccia-utente e quindi per la grafica[77]. Così, una semplice "lista" dei dati raccolti si mostrerebbe come una soluzione inefficiente; sembra preferibile, invece, l'adozione di un sistema dove i dati personali siano raggruppati per

GDPR as a clarion call for a new global digital gold standard, in *Int. Data Privacy Law*, 2016, p. 77.

[76] O potenzialmente essere migliore della norma giuridica nel plasmare i comportamenti dei consociati. Per il dibattito sviluppatosi circa *lex informatica*, L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999, per il quale una certa architettura della Rete (il *code*), dal punto di vista eminentemente tecnico, è in grado di condizionare talune (o altre) condotte degli utenti, permettendole o inibendole in via automatica; su una posizione diversa, S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2002. Sul tema specifico indagato anche J. D. REIDENBERG, Lex informatica*: The Formulation of Information Privacy Rules Through Technology*, in *Texas Law Review*, 76(3), 1998, p. 553 ss.

[77] Per il maggiore adeguamento ai principi della *user experience* delle interfacce *web* in relazione alla *data protection*, vedi P. COSTA, User experience design *e dati personali: come (ri)progettare la privacy*, in B. PASA (a cura di), *Design e innovazione digitale. Dialogo interdisciplinare per un ripensamento delle tutele*, Napoli, 2021, p. 142 ss.; ancora, H. HAAPIO, M. HAGAN, M. PALMIRANI, A. ROSSI, *Legal Design Patterns for Privacy*, in E. SCHWEIGHOFER ET AL. (edited by), *Data Protection / LegalTech*, *Proceedings of the 21th International Legal Informatics Symposium 2018*, Berna, 2018, pp. 445–450.

diverse categorie semantiche, usando vari colori, diagrammi, o ancora icone standardizzate, elementi percentuali o intervalli di tempo.

b) Assai utile, per l'implementazione effettiva della trasparenza, è la costruzione di un sistema multilivello, dove le informazioni più rilevanti siano poste visivamente in primo piano. Ciò dovrebbe essere reso possibile, in particolare, per coloro che non abbiano una sufficiente educazione quanto alle insidie del mondo digitale, in particolare minori e anziani[78]. Inoltre, molti utenti potrebbero non ritenersi soddisfatti del contenuto minimo informativo così presentato dal *digital provider*; pertanto, è più spendibile una tecnologia che preveda l'integrazione di diverse finestre (o *pop-up*) man mano contenenti maggiori informazioni, dove quelle essenziali vengono indicate con "enfasi" maggiore.

c) Un sistema di notifiche, ancora, permette di definire in maniera chiara e semplice le operazioni successive alla raccolta, con particolare riferimento alla comunicazione e diffusione di dati personali. Inoltre, un *alert* potrebbe avvisare l'interessato nell'ipotesi di un *data breach*, descrivendo meglio i dati oggetto di divulgazione non autorizzata, come anche, in generale, rendere edotto l'utente circa le minacce rilevate, specie in caso di sovraesposizione a causa di una eccessiva raccolta di dati personali e, di conseguenza, suggerire l'azione successiva da intraprendere.

d) Un ulteriore aspetto da valutare è quello di prevedere una sorta di pannello intuitivo di controllo che costituisca un'interfaccia altamente personalizzabile e attrattiva, mediante la quale comunicare in tempo reale con il titolare del trattamento (ad esempio, una particolare *dashboard* dedicata, quale *feature* specifica della *app*), come se fosse una sorta di *customer service* dedicato ai dati personali. Tutto ciò renderebbe altresì molto più semplice esercitare concretamente i diritti dell'interessato.

In buona sostanza, la *data protection by design* richiede che i requisiti legali relativi al trattamento di dati personali non siano tradotti in termini algoritmici, come si suole affermare[79], bensì implementati nella *scelta* di misure tecniche e operative adeguate, ragionevoli e proporzionate alla situazione specifica, garantendo, per questa via,

---

[78] In argomento, G. Malgieri, J. Niklas, *Vulnerable data subjects*, in *Computer Law and Security Review*, 37, 2020, p. 1 ss.

[79] Con una critica efficace, v. B.J. Koops, R. Leenes, *Privacy Regulation Cannot Be Hardcoded*, cit., p. 166.

l'effettività della disciplina che governa la protezione dei dati personali. In ogni caso, si tratta di criteri dinamici, flessibili ed empirici, il cui contenuto è da valutarsi nella situazione specifica, o di una serie omogenea di casi, a seconda degli interessi di volta in volta richiamati. Vieppiù che tali criteri muovono dall'essere metro di misura dell'adozione di tecnologia a «tecnica argomentativa»[80] per attuare il principio di *accountability* e, in ultimo, essere parametro di giudizio per la congruità delle misure adottate per la tutela dei dati personali.

D'altro canto, «una buona regolamentazione, se pur essenziale, non è sufficiente»[81]; semmai la norma giuridica deve orientare la realizzazione degli algoritmi, coordinandosi, da un lato, con le altre scienze e, dall'altro, guidando gli operatori pratici nelle decisioni relative all'implementazione dei principi e delle regole attraverso le tecnologie; verificando, in seguito, se l'effettività delle tutele sia raggiunta, soprattutto in ragione delle alternative tecniche, della complessità e dei repentini mutamenti dell'era digitale[82].

In questa prospettiva, i codici di condotta[83], i meccanismi di certificazione[84], ma anche i *privacy design patterns*[85], i quali rappresentano varie combinazioni prefissate di misure tecniche e organizzative di possibile adozione, costituiscono tutti strumenti fondamentali attraverso i quali definire l'architettura del trattamento, specialmente nella fase di predisposizione dei sistemi informatici, nonché di una loro successiva modifica o revisione. A ciò si aggiungono, naturalmente, le previsioni fornite dalle autorità di controllo, nazionali ed europee, in funzione propulsiva, autorizzativa o partecipativa con riguardo a siffatte nuove espressioni della giuridicità – specie per i menzionati codici di

---

[80] Così R. D'ORAZIO, *Protezione dei* dati by default *e* by design, cit., p. 95 ss.

[81] EDPS, *Opinion 9/2016*, cit., p. 14 («*Good regulation, while crucial, is not sufficient in itself*»), ove si sottolinea come il contributo offerto dalla tecnologia appare essenziale nell'affermazione dei *PIMS*.

[82] Effettività più volte ricordata anche dall'EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, cit. (per ben 51 volte!).

[83] D. POLETTI, M. C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. TOSI, Privacy *digitale*, cit., p. 369 ss.

[84] Ad es., si potrebbe pensare allo *standard* già esistente ISO/IEC 27701 sui *Privacy Information Management System* (PIMS), inteso come una estensione della ISO/IEC 27001 e ISO/IEC 27002 su *privacy management*.

[85] In argomento, J. LENHARD, L. FRITSCH, S. HEROLD, *A Literature Study on Privacy Patterns Research*, 2017, 43rd *Euromicro Conference on Software Engineering and Advanced Applications*, reperibile *online* all'indirizzo https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8051348, pp. 194 ss.

condotta e meccanismi di certificazione[86] –, ben diverse dalla regola intesa in senso formale: il che si traduce in una strategia di normazione integrata, che si delinea, appunto, come un'autonomia (privata) "controllata"[87].

Tutto ciò rende, in definitiva, l'algoritmo e soprattutto la tecnologia stessa "testabile" e "contestabile"[88], non solo da parte dell'utente, ma anche dagli altri soggetti che partecipano attivamente nei mercati digitali, come i titolari (e i responsabili) del trattamento, le autorità di controllo e, non da ultimo, i legislatori[89].

2.6. L'esempio dei *Personal Data Stores*: un modello vincente?

Dotare gli utenti dei servizi digitali di strumenti tecnologici per meglio interfacciarsi con il trattamento dei dati personali è senz'altro funzionale ad accrescere la loro consapevolezza in merito all'utilizzo che viene fatto delle informazioni ad essi riconducibili, come anche a rafforzare la loro autonomia nell'alveo del capitalismo dell'informazione.

In questo frangente, si inserisce una particolare tipologia di *PIMS*, noto come *Personal Data Store*[90]. In sostanza, si tratta di un'alternativa al classico sistema di memorizzazione dei dati personali all'interno dei *server* centralizzati (*silos*) sotto il controllo diretto dei *digital providers*[91]:

---

[86] Per fare un esempio: l'art. 57, GDPR, individuando i compiti delle autorità di controllo, indica espressamente quello di incoraggiare l'elaborazione di codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma del procedimento indicato nell'art. 40 GDPR. Analogo discorso può farsi con i meccanismi di certificazione di cui all'art. 42 GDPR.

[87] Cfr. S. RODOTÀ, *Tecnologie e diritti*, cit., p. 51 ss.; più di recente, P. LAGHI, *Cyberspazio e sussidiarietà*, cit., p. 110 ss.

[88] M. HILDEBRANDT, *Saved by Design? The Case of Legal Protection by Design*, in *Nanoethics*, 2017, p. 309.

[89] Vedi sul punto P. LAGHI, *Cyberspazio e sussidiarietà*, cit., p. 115, ove si riconosce la maggiore idoneità regolativa dell'autonomia privata organizzata (c.d. *co-regulation*) nel soddisfacimento degli interessi coinvolti, mantenendosi però un ruolo di direzione e di orientamento del potere pubblico che consente di supplire ad essa allorché si dimostri incapace di realizzare un assetto equilibrato.

[90] H. JANSSEN, J. COBBE, C. NORVAL, J. SINGH, *Decentralised Data Processing: Personal Data Stores and the GDPR*, in *Int. Data Privacy Law*, 9, 2020, p. 356 ss. e ivi ampi riferimenti bibliografici.

[91] T. LEHTINIEMI, *Personal Data Spaces: An Interventation in Surveillance Capitalism*, in *Surveillance & Society*, 15(5), p. 631.

il modello proposto è di stampo decentralizzato, dal momento che i dati personali di ciascun utente vengono memorizzati solo in locale sui singoli *device* in possesso dell'individuo, ovvero su un *cloud*, fornito, di solito, da un soggetto terzo; sicché i diversi fornitori di servizi digitali possono solo accedere al *PDS* in maniera selettiva, a seconda delle preferenze accordate dall'utente, caso per caso, o in una serie omogenea di casi, senza la possibilità di "replicare" i dati oppure di svolgere la analisi al di fuori del "luogo virtuale" prescelto[92].

Oltre ad essere in grado di percepire meglio quali dati personali vengono utilizzati da altri soggetti, gli utenti sono messi in condizione di esercitare in maniera più agevole i diritti loro spettanti, come la rettifica e la cancellazione dei dati, il diritto di opposizione o la revoca del consenso al trattamento, o ancora il diritto alla portabilità dei dati, posto che l'esistenza di *standard* compatibili e di formato, con riguardo all'esistenza di un singolo spazio virtuale, rendono più semplice il trasferimento di dati. Anzi, a maggior ragione, i *PDS* possono fungere da vero e proprio collettore di dati relativi a molteplici servizi della società dell'informazione e, per certi versi, ricostruire l'identità personale, sempre più frammentata nella "data-sfera"[93].

È auspicabile, dunque, l'utilizzo dei *PDS*, i quali permettono all'individuo decisioni più consapevoli in merito al trattamento dei dati personali e un controllo effettivo e concreto delle informazioni riguardanti la persona, laddove quest'ultima è davvero posta al centro della scena, mediante un approccio inclusivo e non alienante, nell'incessante processo di "datificazione" della sfera privata. E come un circolo virtuoso, l'adozione di tali strumenti, che senz'altro rinforzano la trasparenza del trattamento, dovrebbe permettere all'interessato di acquisire maggiore fiducia e affidabilità nei servizi offerti nella società dell'informazione, in quanto resi con modalità più accessibili e comprensibili[94].

---

[92] Cfr. EDPS, *Opinion 9/2016*, cit., p. 6. Per un modello opposto a quello del *PDS*, laddove l'intermediario è delegato dall'interessato ad ottenere i dati personali presso i diversi titolari del trattamento, allo scopo di riunirli in un'unica banca dati per "monetizzarne" l'uso, F. BRAVO, *Il commercio elettronico dei dati personali*, in T. PASQUINO, A. RIZZO, M. TESCARO, *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, p. 93 ss.

[93] Sul significato di tale espressione, V. ZENO-ZENCOVICH, *La "Datasfera". Regole giuridiche per il mondo digitale*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, 99 ss.

[94] In questo senso, v. anche EDPS, *Opinion 9/2016*, cit., p. 8. Si rafforza così il coordinamento tra disciplina posta a presidio della circolazione dei dati personali, la tutela dei consumatori e la concorrenza nel Mercato Unico Digitale.

Quanto appena affermato, letto alla luce del principio della *data protection by design*, implica una rottura del paradigma *company-centric* tuttora diffuso, indirizzando le misure tecniche e organizzative, delle quali si serve il titolare del trattamento, verso un approccio maggiormente *user-oriented*. Così, i *PDS* possono essere visti come strumenti tecnologici che forniscono all'individuo uno "sguardo all'interno" del trattamento, considerando, tra l'altro, come la raccolta dei dati spesso avvenga al primo contatto con l'interessato, mentre difficilmente in seguito si vanno a modificare le scelte accordate. Inoltre, i *PDS* rappresentano una occasione d'intervento nel capitalismo di sorveglianza, andando ad attribuire agli interessati un ruolo operativo nelle dinamiche relative alla circolazione dei dati personali, fronteggiando apertamente i pericoli di un trattamento "oscuro" non tanto per le finalità, ma soprattutto per i mezzi impiegati, specie quando vi sia un uso intensivo di prodotti dell'Intelligenza Artificiale e delle tecniche di *machine learning*.

Nondimeno, la soluzione dei *PDS* solleva alcune questioni sotto l'ambito di applicazione del GDPR[95]. Tra le tante, non è affatto semplice individuare il ruolo (e le relative responsabilità) dei gestori del *PDS*, potendo agire, di fatto, quali titolari del trattamento, responsabili, o ancora come titolari "autonomi" (*recte* "terzi"[96]). Posto che gli utenti non possono essere considerati come "titolari" (del trattamento) quanto alle informazioni ad essi riconducibili, una possibile soluzione potrebbe essere vista nella contitolarità del trattamento, laddove i vari soggetti che operano con i dati personali, accedendo ai *PDS*, regolano preventivamente e attraverso lo strumento contrattuale rispettivi obblighi e responsabilità, sia nei confronti dell'interessato, sia tra di loro[97].

---

[95] Cfr. H. JANSSEN, J. COBBE, C. NORVAL, J. SINGH, *Decentralised Data Processing: Personal Data Stores and the GDPR*, cit.

[96] Art. 4, n. 10, GDPR: «"terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile».

[97] Interessanti sono le indicazioni fornite dall'EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, v. 1.0, 2.9.2020, spec. p. 40 sul concetto di *joint controllership* di cui all'art. 26, GDPR, laddove si richiama la pronuncia CGUE, 5 giugno 2018, causa C-210/6, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH* (pubblicata in *Foro it*., 2018, IV, c. 361, con nota di richiami di R. PARDOLESI e S. BONAVITA), dove i giudici hanno ritenuto l'amministratore di una *fan page* ospitata su *Facebook* e il noto *social network* come

L'esplosione di un mercato di servizi *PDS* è ancora più complicato[98]. L'implementazione pratica di un siffatto modello deve fare i conti con l'idea di *business* ancora basata sul capitalismo predominante dell'impresa, e non sulla persona dell'utente. Ciò è dovuto, principalmente, alla presenza di pochi monopolisti (soprattutto i *Tech Giants*), i quali hanno accresciuto la quantità di utenti (e di dati) in loro possesso, anche grazie agli effetti di rete di accaparramento della clientela, determinando, di fatto, delle forti barriere all'ingresso di nuovi *competitor* nei mercati digitali[99]. L'assenza di vantaggi competitivi per tali categorie di soggetti non può che tradursi in una carenza di interesse quanto alla diffusione di strumenti informatici più incentrati sulla persona.

Ora, se per le attività nelle quali il *core business* non è rappresentato dall'accumulo di dati personali l'adozione dei *PDS* vedrebbe facilmente ridotti i costi di *compliance* e i rischi inerenti a possibili violazioni di sicurezza, mediante l'affidamento della loro gestione a un terzo "fiduciario", cambiare l'attuale assetto della *Big Data economy* appare ancora molto distante, con pochi soggetti che godono ancora di una "rendita da posizione". Qui forse solo la trasparenza potrebbe giocare un ruolo chiave di incentivo: si passerebbe, in tal senso, da un modello di mercato basato sulla *data rentention* ad uno in cui la qualità del servizio offerto costituisce la chiave per assicurarsi un maggior numero di clienti; di conseguenza, gli utenti sarebbero propensi a fornire dati sempre più precisi e aggiornati, in quanto interessati a ricevere servizi costruiti in base alle loro *attuali* preferenze – il che porterebbe, peraltro, ad una migliore profilazione della clientela. Ulteriori stimoli potrebbero rinvenirsi, poi, nella semplificazione delle attività condotte dal

contitolari del trattamento rispetto agli utenti della pagina; più di recente, CGUE, 29 luglio 2019, causa C-40/17, *Fashion Id Gmbh & Co. Verbraucherzentrale Nrw Ev, Facebook Ireland Ltd Landesbeauftragte Fu¨R Datenschutz Und Informationsfreiheit Nordrhein-Westfalen*, in *Dir. inf.*, 2019, p. 1253 ss., con nota di G. GIANNONE CODIGLIONE, *Trattamenti multipli di dati personali e parcellizzazione degli obblighi di condotta*.

[98] Per l'analisi di alcune soluzioni di mercato, I. BOLYCHEVSKY, S. WORTHINGTON, *Are Personal Data Stores about to become the NEXT BIG THING?*, https://medium.com/@shevski/are-personal-data-stores-about-to-become-the-next-big-thing-b767295ed842; T. BERNERS-LEE, *We Need to Change How We Share Our Personal Data Online in the Age of COVID-19*, in *Time*, 15 luglio 2020, reperibile all'indirizzo https://time.com/5867314/we-need-to-change-how-we-share-our-personal-data-online-in-the-age-of-covid-19/.

[99] Sul punto, diffusamente, T. LEHTINIEMI, *Personal Data Spaces*, cit., p. 626 ss.

titolare, nonché, da ultimo, in una migliore immagine guadagnata dall'impresa[100].

2.7. La trasparenza quale presupposto per la scelta "democratica" della tecnologia

La trasparenza costituisce un elemento cruciale dell'intero sistema di scelta della tecnologia nel trattamento di dati personali in funzione della persona, dal momento che funge non solo da connettore delle diverse operazioni in cui esso si esplica, ma garantisce anche, coordinando le finalità e i mezzi del medesimo, l'effettività dei diritti che il GDPR ha riconosciuto all'interessato e, per questa via, rafforza pure la tutela dei diritti e delle libertà fondamentali dell'individuo.

Si è già visto come le tecnologie volte ad implementare il principio della trasparenza nel trattamento dei dati personali possano essere utilizzate per bilanciare l'asimmetria informativa esistente tra i *digital service provider* e i loro fruitori, accrescendo il potere di controllo degli interessati quanto alle informazioni ad essi riconducibili. Infatti, le soluzioni offerte da *PIMS* e *PDS* sembrano fornire una maggiore conoscenza della circolazione dei dati personali nell'ambiente digitale, connettendo la prospettiva *ex ante* (ottenere dal titolare le informazioni obbligatorie circa il trattamento effettuato) con quella *ex post* (relativamente all'esercizio dei diritti riconosciuti all'interessato), non più tenute distinte, ma saldate in un circolo virtuoso fra il titolare e l'interessato.

Sotto un diverso profilo, gli strumenti sopra ricordati potrebbero risolvere alcuni problemi derivanti dall'universo *IoT*, dove il più delle volte risulta difficile rendere le informazioni chiare e comprensibili quanto al trattamento, stante la ridotta dimensione o addirittura l'assenza di un *display* con il quale visualizzare i dati, continuamente collezionati attraverso il servizio digitale; cosicché l'esistenza di un *PDS* dedicato, che consenta di gestire i dati personali dell'interessato, condurrebbe non solo al rafforzamento del ruolo dell'utente, ma anche a

[100] Per un'approfondita analisi di mercato, *Study commisioned to Cambridge Judge Business School* intitolato *Personal Data Stores* [Report], Cambridge University, 2015, reperibile *online* all'indirizzo https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school.

rendere più chiaro l'operato del fornitore del servizio legato all'"oggetto connesso".

Quello che ancora manca per il concreto funzionamento delle *PETs* è l'educazione digitale degli utenti della Rete, senz'altro carente in merito ai rischi e ai pericoli che l'ambiente *online* porta con sé, come dimostrato dal *privacy paradox*[101]. In questo senso, soccorrerebbe, ancora, la *data protection by design*, in funzione "formativa" della persona: se l'architettura del sistema di gestione dei dati personali viene davvero predisposta dal titolare del trattamento in maniera più trasparente e a misura d'utente, tenuto conto dei rischi e del contesto situazionale, non solo il pieno rispetto del GDPR, ma anche il reciproco rapporto tra fornitore di servizio digitale e il cliente non può che uscirne migliorato; il tutto nella prospettiva di una tutela effettiva degli individui, sia pure risultato di una compartecipazione fra regola tecnica e norma giuridica, autoregolamentazione e controllo esterno, mercato e persona.

La *data protection by design* non è, dunque, un concetto rigido o statico, dal momento che al titolare del trattamento si richiede una attenta e continua valutazione non solo dei rischi per i diritti e le libertà fondamentali dell'interessato, ma anche del contesto e soprattutto degli interessi in forza dei quali si compiono le operazioni con i dati personali. Sicché l'effettività della protezione dei dati personali non può essere lasciata alla sola tecnica, men che meno al solo diritto[102]. Al contrario, il *test* di adeguatezza, proporzionalità e ragionevolezza dell'adozione di una certa tecnologia utilizzata nel trattamento deve necessariamente prendere in considerazione, tre le presenti (e future) alternative, la tutela degli interessi giuridicamente meritevoli di

[101] Nel senso che tecnologie di *data control by design* permettono all'utente non solo una gestione modulare dei dati personali con il vantaggio di formare in esso un "migliore" consenso al trattamento, ma anche una maggiore educazione sui rischi e sugli usi cui sono esposte le informazioni che lo riguardano, v. altresì A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019, p. 213, nota 109. In una più ampia prospettiva, M. D'AMBROSIO, *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Napoli, 2017, p. 112 ss. Nondimeno, pure il settore dell'*eGovernment* potrebbe essere considerato come un settore promettente, specie quello sanitario: COMM. EU, *An emerging offer of "personal information management services". Current state of service offers and challenges*, 2015, reperibile *online* all'indirizzo https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118, p. 13.

[102] F. ROMEO, *Il governo giuridico delle tecniche dell'informazione e della comunicazione*, cit., p. 1270, secondo il quale il governo della tecnica presuppone la conoscenza delle sue regole, dal momento che il diritto deve essere in grado di interagire con essa al fine di orientare i risultati verso gli scopi posti dalla norma giuridica.

protezione, nelle specifiche circostanze del caso. In fondo, la norma giuridica non può certo perdere la sua funzione di valutare gli strumenti migliori per tutelare gli interessi protetti.

Posto che la definizione degli algoritmi e delle tecnologie non assicura la medesima partecipazione democratica presente a livello della regolamentazione legislativa, è proprio attraverso il sindacato di legittimità circa l'autonomia della scelta – quand'anche relativa alle misure, in concreto, da adottare – e specialmente degli obblighi gravanti sui titolari del trattamento, sin dal momento di determinare i mezzi dello stesso, che si coniugano la tecnologia in termini democratici e la sua rispondenza ai valori costituzionali riferibili alla persona.

Nell'era digitale, la tutela dell'individuo, per considerarsi davvero effettiva, deve essere perciò supportata dalle medesime tecnologie che rendono possibile il trattamento di dati personali per i fornitori di servizi nella società dell'informazione. Come ben sottolineato dal *considerando* § 4 del GDPR, laddove si afferma che «[i]l trattamento dei dati personali dovrebbe essere al servizio dell'uomo», vero fruitore ultimo dei benefici tecnologici, anche la scelta di una tecnologia piuttosto che un'altra non è mai neutrale, bensì è sviluppata e adottata, da chi se ne serve, entro la cifra assiologica della dignità della persona[103]. In questa prospettiva, la soluzione va ricercata quindi nella scelta "democratica" della tecnologia più trasparente da utilizzare, in modo da fugare i pericoli della «dittatura dell'algoritmo»[104].

[103] Cfr. R. SENIGAGLIA, *Il dovere di educare i figli nell'era digitale*, in *Persona e mercato*, 3, 2021, p. 525, per il quale «(…) la necessità di definire il rapporto tra l'uomo e la tecnica digitale all'insegna della conformazione di quest'ultima direttamente ad opera di chi la pone: attraverso (i) regole che la rendano compatibile con la dignità dell'uomo, (ii) meccanismi tecnici di controllo (mediante il ricorso agli stessi algoritmi), (iii) mezzi idonei a renderla controllabile e sanzionabile da tutti gli utenti».

[104] S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 402, dove «scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili».

3. Dati e identità personale. Note sparse a partire da una recente pronuncia del Consiglio di Stato

Lucio Casalini (Università di Camerino)

3.1. Premessa. L'«io diviso» in rete, tra *otium* e *negotium*

I nostri padri costituenti hanno costruito il concetto di persona attorno a tre istituti chiave del nostro ordinamento: la capacità giuridica, la cittadinanza e il nome. L'art. 22 Cost. prevede, infatti, che «[n]essuno può essere privato, per motivi politici, della capacità giuridica, della cittadinanza, del nome». Attraverso questa costruzione giuridica scolpita in Costituzione si è inteso plasmare il diritto all'identità personale, che forma un uno inscindibile e costituzionalmente inviolabile. Tuttavia, con il rapido sviluppo della tecnologia, oggi la questione si ripropone prepotentemente in contesti del tutto assenti a metà Novecento. Il riferimento corre, ovviamente, a Internet e, più di recente, al cd. metaverso[1]. Non è un caso se attorno a questi temi si sono intrecciate, non solo in Italia, sentenze fondamentali della Corte Costituzionale e della Corte di Cassazione, da una parte, e della Corte di Giustizia Europea e della Corte Europea dei Diritti dell'Uomo, dall'altra[2].

[1] Termine coniato da Neal Stephenson nel romanzo cyberpunk Snow crash (1992) per indicare uno spazio tridimensionale all'interno del quale persone fisiche possono muoversi, condividere e interagire attraverso avatar personalizzati. Il metaverso viene descritto come un enorme sistema operativo, regolato da demoni che lavorano in background, al quale gli individui si connettono trasformandosi a loro volta in software che interagisce con altro software e con la possibilità di condurre una vita elettronica autonoma. Il metaverso è regolato da norme specifiche e differenti dalla vita reale e il prestigio delle persone deriva dalla precisione e dall'originalità del rispettivo avatar. Si è parlato di metaverso per definire le chat tridimensionali e i giochi di ruolo multiplayer online (cfr. www.treccani.it/enciclopedia/metaverso).

[2] Un diritto all'identità personale che la Consulta ha consacrato in questi termini: «un diritto ad essere se stessi, inteso come rispetto dell'immagine di partecipe alla vita associata, con le idee e le

Il tratto precipuo dell'analisi, che il diritto accoglie come assioma di fondo è quello secondo cui l'identità non è un concetto statico, bensì dinamico. Se si cala questo stesso concetto nel mondo digitale, il dinamismo diviene "liquidità" – riprendendo la fortunata espressione di Zygmunt Bauman – e il diritto faticosamente riesce a connettersi ad esso, difficilmente ad anticiparlo e, nell'ipotesi migliore, a regolarlo *ex post*. Ciò perché la realtà si presenta fluttuante e, per certi versi, inafferrabile. Una tale difficoltà è esacerbata dal mutamento di prospettiva attraverso cui l'identità personale viene ricostruita, anche rispetto alla ricostruzione costituzionale richiamata: non già a partire da sé, bensì a partire dai dati che di sé la persona dissemina navigando nel web.

Invero, il problema si pone già da un punto di vista semantico. Il sostantivo "identità" non muta di significato al plurale, ma in internet diviene necessariamente plurale, poiché qui si frantuma e genera un caleidoscopio di identità digitali. Si è parlato, al riguardo, di «io diviso»: l'identità che supera la dimensione statica, istantanea e tendenzialmente immutabile, per divenire un processo dinamico, potenzialmente infinito e mutevole[3]. Per altro verso, se ci si immerge nelle dinamiche negoziali, questi ultimi rilievi evidenziano come, per la realizzazione del diritto attribuito a ciascuna persona alla "autodeterminazione informativa", sia insufficiente il gioco delle volontà in un

esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano e al tempo stesso qualificano l'individuo», v. Corte cost., 3 febbraio 1994, n. 13, in Foro it., 1994, I, 1668; v. anche Cass., sez. I, 2 luglio 2018, n. 17278, in *DeJure* e in *Foro it.* Si viene così catapultati nel cuore delle grandi tematiche afferenti alla *privacy*, ma anche delle origini biologiche (con riguardo alla conoscenza della madre nel caso di parto anonimo, di adozione o di procreazione artificiale; *ex multis*, cfr., ad esempio, Cass. 21 luglio 2016, n. 15024; Corte cost., n. 28 del 2013; Cass. 9 novembre 2016, n. 22838. Sul fronte della dottrina, cfr. almeno A. DE CUPIS, *Il diritto all'identità personale*, Milano, 1949; G.B. FERRI, *Privacy e identità personale*, in *Riv. dir. com.*, 1981, II, p. 379 ss.; F. MACIOCE, *Tutela civile della persona e identità personale*, Padova, 1984; V. ZENO-ZENCOVICH, voce *Identità personale*, in *Dig. disc. priv.*, Sez. civ., IX, p. 294 ss.; L. VALLE, *Il diritto all'identità personale*, in M. Sesta e V. Cuffaro (a cura di), *Persona, famiglia e successioni nella giurisprudenza costituzionale*, Napoli, 2006, p. 77 ss.; P. ZATTI, *Dimensioni ed aspetti della identità nel diritto privato attuale*, in *L'identità nell'orizzonte del diritto privato*, supplemento a *Nuov. giur. civ. comm.*, 4, 2007, p. 1 ss.; G. FINOCCHIARO, voce *Identità personale (diritto alla)*, in *Dig. disc. Priv.* sez. civ., Torino, 2010. Sul rapporto tra identità personale e dati, cfr. C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021.

[3] Mutuando il titolo del saggio di Ronald David Laing e riadattando l'idea della costruzione (e della perdita) delle identità nel contesto digitale, R.D. LAING, *L'io diviso. Studio di psichiatria esistenziale*, Einaudi, Torino 1969, ripreso da A. SORO, *Persone in rete. I dati tra poteri e diritti*, Fazi, Roma, 2018, p. 28. «L'unità della persona viene spezzata. Al suo posto non troviamo un unico "clone elettronico", bensì tante "persone elettroniche", tante persone create dal mercato quanti sono gli interessi diversificati che spingono alla raccolta delle informazioni. Siamo di fronte ad un individuo "moltiplicato"», così già si esprimeva S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Rivista critica di diritto privato*, 4, 1997, p. 585 ss.

mercato non regolamentato. Infatti, questa impostazione, da una parte, non tiene conto dell'antico argomento delle disparità di potere negoziale, dell'esistenza di contraenti deboli, che la pura logica di mercato potrebbe esporre persino al sacrificio della dignità; dall'altra, ignora proprio il delicatissimo bilanciamento di interessi che la disciplina dei dati personali porta con sé e che non può essere affidato soltanto alle dinamiche di mercato, poiché sono in gioco valori come il rispetto della dignità individuale e sociale, nonché la libertà d'informazione[4].

Nell'immaginario digitale, inoltre, è frequente l'accostamento del cd. *social networks* ad una piazza virtuale, dove, come in quella reale, ci si reca abitualmente per praticare l'*otium*. Difatti, nell'antichità, l'*otium* veniva considerato in contrapposizione al *negotium*. Quest'ultimo indicava letteralmente gli affari commerciali e le varie occupazioni che ogni cittadino svolgeva per il bene della sua città. Per ozio, invece, si intendeva tutto ciò che era lontano dall'attività pubblica e commerciale: l'*otium* era la cura di sé, che passava per la contemplazione e lo studio[5].

A ben vedere, tuttavia, le differenze tra reale e virtuale appaiono notevoli e i profili di criticità che segnano profondamente i rapporti giuridici tra i peculiari soggetti della rete non sono di poco momento[6].

La pronuncia del Consiglio di Stato da cui origina il presente contributo si colloca in questo solco ideale e dimostra come il processo in atto di assottigliamento tra *otium* e *negotium* sulle piattaforme di social network sia giunto ormai a completo compimento. Difatti, in questi contesti virtuali, la raccolta e il successivo riutilizzo a fini commerciali dei dati degli utenti contribuisce a corroborare le tesi secondo cui i tempi siano ormai maturi per parlare di un vero e proprio mercato dei dati digitali[7].

---

[4] *Ibidem*, p. 597 ss.

[5] Cfr., per tutti, SENECA, *De brevitate vitae*, 1, XIV, *«Soli omnium otiosi sunt qui sapientiae vacant, soli vivunt.»* (Soli fra tutti sono gli oziosi quelli che dedicano il tempo alla saggezza, solo essi vivono).

[6] Qui il riferimento va non solo - e non tanto - alle pratiche commerciali scorrette o alle condotte anticoncorrenziali poste in essere dai soggetti del mercato, ma a quei comportamenti tenuti dagli stessi utenti che, spesso, dietro le possibilità offerte dall'anonimato, indulgono in pratiche come *stalking, revenge porn*, *hate speech*, su cui cfr. O. POLLICINO, G. DE GREGORIO, *Hate speech: una prospettiva di diritto comparato*, in *Giornale di diritto amministrativo*, 4/2019, p. 423 ss.

[7] Cfr. S. TOBANI, *op. cit.,* p. 131 ss. Tale sovrapposizione, inoltre, è ancora più chiara per i servizi di *marketplace*, ora offerti anche dalla piattaforma Facebook, ove l'utente iscritto al social network può porre in essere negozi giuridici di natura commerciale.

Per queste ragioni, alla luce delle proporzioni assunte dal fenomeno, si fa largo nel dibattito (non soltanto giuridico) anche l'ulteriore questione inerente alla qualificazione di queste piattaforme, che qui occorre almeno lambire in premessa. Segnatamente, sono due i poli attorno cui si snoda l'analisi: soggetto privato o soggetto pubblico? Cioè a dire, è più utile il mantenimento di una soggettività privata per lo sviluppo del mercato digitale o, all'opposto, è ormai necessario riconoscere formalmente queste piattaforme come soggetti pubblici (cd. *public utilities*)[8]. Quest'ultima tesi appare oggi assai suggestiva e alcuni assertori si sono spinti al punto da ritenere ad esempio Facebook persino fondamentale per l'esistenza stessa degli individui in società. La presenza su Internet sarebbe «un requisito nel ventunesimo secolo per partecipare come cittadino, come consumatore, come persona informata e come essere sociale»[9].

Ciò imporrebbe una regolamentazione *ad hoc,* in grado di superare l'attuale *laissez-faire approach*, ormai inadeguato, dal momento che le tradizionali forme di regolazione (incluse le leggi antitrust) sembrano inidonee per la regolazione di tali imprese, spesso fondamentali anche per la democrazia stessa di ciascun Paese[10].

Fatta questa breve premessa di più ampio respiro pubblicistico, qui s'intende lumeggiare i profili di maggior interesse civilistico cui è pervenuto il supremo organo di giustizia amministrativa nelle

---

[8] Cfr. M. BASSINI, *Libertà di espressione e social network, tra nuovi "spazi pubblici" e "poteri privati". Spunti di comparazione*, in *MediaLaws*, 2, 2021, p. 67, dove l'Autore propone una panoramica di diritto comparato sulla più recente giurisprudenza statunitense ed europea relativa alla qualificazione giuridica dei social network, alla vigilia di importanti riforme che riguarderanno la disciplina dei servizi digitali a livello dell'Unione europea. L'obiettivo del contributo è mettere in evidenza come la frequente assimilazione di tali soggetti e dei relativi servizi ai caratteri di pubblicità possa comportare conseguenze non necessariamente favorevoli sul piano della tutela della libertà di espressione.

[9] Cfr. Z. TUFEKCI, *Google Buzz: The Corporatization of Social Commons*, in *Commcns.org*, 2010; ID., *Facebook: The Privatization of Our Privates and Life in the Company Town*, in *Commcns.org*, 2010. In questo senso, giova ricordare che secondo la Dichiarazione dei Diritti di Internet (elaborata dalla Commissione per i diritti e i doveri relativi ad Internet a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015) «L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale».

[10] Tuttavia, per quanto riguarda l'inquadramento di Facebook come servizio pubblico siamo ancora nel campo delle ipotesi, anche se i pericoli di una regolamentazione troppo scarsa sono già chiari. *Ex multis*, Cfr. T. WU, *The Master Switch: The Rise and Fall of Information Empires*, in *Commcns.org,* p. 303-304; S. PIVA, *Facebook è un servizio pubblico? La controversia su CasaPound risolleva la quaestio dell'inquadramento giuridico dei social network*, in *www.dirittifondamentali.it*, 2/2020, p. 1214. L'Autrice analizza un'interessante sentenza del Tribunale capitolino che s'inquadra nel dibattito, di rovente attualità, attorno alle piattaforme di social network (*Twitter* e *Facebook* in testa) e la libertà di espressione e di manifestazione del pensiero (Trib. Roma, sez. XVII, ordinanze del 19 dicembre 2019 e del 29 aprile 2020).

conclusioni della sentenza, con particolare riferimento al fenomeno della patrimonializzazione dei dati personali, che parrebbe spostare sempre più i termini del dibattito nell'orbita del *diritto del consumo*[11], alla luce dell'apparato rimediale che lo stesso è in grado di garantire all'utente/consumatore[12].

3.2. Il caso

Breviter, pare opportuno ripercorrere i fatti di causa. L'AGCM contestava alle società Facebook Inc. e Facebook Ireland Limited due distinte pratiche commerciali scorrette, in violazione degli artt. 20, 21, 22, 24 e 25 del d.lgs. 6 settembre 2005, n. 206 (cd. codice del consumo): da una parte, pratiche qualificabili come ingannevoli, in quanto Facebook «non informerebbe adeguatamente e immediatamente l'utente, in fase di attivazione dell'account, dell'attività di raccolta e utilizzo, per finalità informative e/o commerciali, dei dati che egli cede, rendendolo edotto della sola gratuità della fruizione del servizio, così da indurlo ad assumere una decisione che non avrebbe altrimenti preso

[11] È da preferire la locuzione «diritto del consumo», piuttosto che quella di «diritto dei consumatori», sulla scorta dell'insegnamento di G. Benedetti, *Tutela del consumatore e autonomia contrattuale*, in *Riv. dir. proc. civ.*, 1998, pp. 17 ss. L'attributo «consumatore» – spiega l'insigne Autore – ha invero una «intonazione più sociologica che giuridica», valendo esso ad «individuare in termini soggettivi l'atto di consumo», più che una «precisa categoria tecnico-giuridica». Ed aggiunge che «gli interventi normativi determinati dalle fonti comunitarie dimostrano un tale grado di frammentarietà e settorialità da rendere improbabile, se non arbitrario, intraprendere un processo di generalizzazione volto alla costruzione d'una categoria giuridica definita e univoca, che metta capo a un autonomo soggetto di diritto: il consumatore. A tale stregua si deve affermare che consumatore non significa nient'altro dal comune soggetto di diritto, rispetto al quale trovano applicazione certe tutele in relazione alle modalità oggettive del suo operare nel traffico giuridico, con i limiti e per le finalità caratterizzate da un particolare ambito di rilevanza. Perciò l'attenzione finisce con il concentrarsi sulle specifiche finalità perseguite dalle regole poste a tutela del privato», v. in particolare pp. 21-22.

[12] Cfr. V. Zeno Zencovich, *Do "Data Markets" Exist?,* in *MediaLaws - Rivista di diritto dei media*, 2/2019, p. 22 ss.; nella stessa rivista, S. Thobani, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws - Rivista di diritto dei media*, 3/2019, p. 132, in particolare nota 1, in cui l'Autrice afferma che «il valore economico dei dati personali è indubbio, nonostante permangano seri dubbi su quale sia il modo più accurato per misurarlo»; Id., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano 2018, p. 160 ss.; G. Resta, V. Zeno Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, p. 436 ss.; C. Langhanke, M. Schmidt-Kessel, *Consumer data as consideration*, in *Journal of European Consumer and Market Law*, 6, 2015, p. 218 ss.; A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 67 ss.; A. Metzger, *Data as Counter-Performance: What Rights and Duties do Parties Have?*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8, 2017, p. 1 ss.

(registrazione e permanenza sulla piattaforma)»; dall'altra, pratiche qualificabili come aggressive, consistenti nell'esercizio di «un indebito condizionamento nei confronti dei consumatori registrati, i quali, in cambio dell'utilizzo di Facebook, verrebbero costretti a consentire a Facebook/terzi la raccolta e l'utilizzo, per finalità informative e/o commerciali, dei dati che li riguardano in modo inconsapevole e automatico, tramite un sistema di preselezione del consenso alla cessione e utilizzo dei dati».

La piattaforma, tuttavia, a seguito della pronuncia del TAR Lazio, confermativa del provvedimento dell'Autorità garante della concorrenza e del mercato, si adeguava solo parzialmente al provvedimento, sì eliminando il *claim* sul carattere gratuito del servizio offerto dalla *homepage* ("Iscriviti. È gratis e lo sarà per sempre"), ma senza fornire indicazioni chiare circa l'uso commerciale dei dati degli utenti.

In particolare, i giudici amministrativi di primo grado sostenevano che «a fronte della protezione del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati» (cfr. par. 6). Sicché i giudici di Palazzo Spada, discostandosi dalla qualificazione di dato personale offerta in sede di impugnativa da parte di Facebook come *res extra commercium*, evidenziano piuttosto come «la patrimonializzazione del dato personale, che nel caso di specie avviene inconsapevolmente, costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato – e della profilazione dell'utente – a fini commerciali».

Segnatamente, il Consiglio di Stato si sofferma sulle convergenze tra diritto consumeristico e privacy, onde precisare che, «allorquando il trattamento investa e coinvolga comportamenti e situazioni disciplinate da altre fonti giuridiche a tutela di altri valori e interessi (altrettanto rilevanti quanto la tutela del dato riferibile alla persona fisica), l'ordinamento – unionale prima e interno poi – non può permettere che alcuna espropriazione applicativa di altre discipline di settore, quale è quella, per il caso che qui interessa, della tutela del consumatore, riduca le tutele garantite alle persone fisiche».

Per il Collegio «può quindi confermarsi che, diversamente da quanto ritenuto dalla società appellante, la disciplina della tutela della privacy e il Codice del consumo presentano ambiti operativi differenti e non contrastanti». In questa prospettiva, il Consiglio di Stato aderisce all'orientamento secondo cui, «per pacifica giurisprudenza, l'obbligo di estrema chiarezza gravante sul professionista deve essere da costui assolto sin dal primo contatto, attraverso il quale debbono essere messi a disposizione del consumatore gli elementi essenziali per un'immediata percezione della offerta pubblicizzata» (cfr., *ex multis*, Cons. Stato, Sez. VI, 14 ottobre 2019 n. 6984, 15 luglio 2019 n. 4976 e 23 maggio 2019 n. 3347). Come già rilevato dall'AGCM e dal giudice di prime cure, tale obbligo di chiarezza non risulta, nel caso di specie, rispettato. Come rilevato, le riflessioni sollecitate dalla pronuncia sono numerose e ne sottendono una, ancor più profonda, attorno all'ormai conclamata tensione tra *data economy*, *privacy* e diritto del consumo[13].

3.3. Profilazione e patrimonializzazione dei dati personali

Come emerge chiaramente dalle argomentazioni della Corte, tutela del consumatore e della privacy vengono poste in un rapporto di complementarità[14]. Quest'ultima funzionale alla protezione del dato personale, inteso quale diritto fondamentale della persona[15]; la prima,

[13] Sia consentito il rinvio a L. CASALINI, *Dati personali all'intersezione tra diritto del consumo e tutela della privacy*, in *Resp. civ. prev.*, 5, 2021, p. 1605; ID., *La patrimonializzazione dei dati personali nella giurisprudenza del Consiglio di Stato*, in *Dir. risp.*, 2, 2021, e, nella stessa rivista, *Data economy, privacy e diritto del consumo*, in *Dir. risp.*, 1, 2022.

[14] Sull'intreccio dei diversi piani di tutela, dei consumatori da un lato, e degli interessati dall'altro, cfr., per tutti, G. RESTA, *Digital platforms and the law: contested issues*, in *MediaLaws - Rivista di diritto dei media*, 1, 2018, p. 245 ss.

[15] Il modello personalistico, che fa perno sull'indisponibilità dei diritti fondamentali della persona, entro cui ricondurre i dati personali, è stato autorevolmente sostenuto da S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 82, ove rimarca l'inadeguatezza dell'impostazione che pretende di considerare la disciplina della circolazione delle informazioni unicamente nella dimensione proprietaria, trattando delle informazioni come di proprietà esclusiva dell'interessato, che può liberamente negoziarne la cessione; nonché da D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 339 ss.; G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 3, 2017, p. 727, il quale, sulla normativa europea in materia di protezione dei dati personali, ammonisce che «Non è […] accettabile l'idea che la persona eserciti un diritto di proprietà sui propri dati e ne possa disporre liberamente».

vola a far assumere una scelta economica consapevole al consumatore[16].

A questo riguardo, come rilevato dalla migliore dottrina, la direttiva 2005/29/CE ha avuto l'indubbio pregio di conferire, in uno, carattere di generalità e unitarietà alla disciplina consumeristica, contribuendo a potenziare quella *vis expansiva* che garantisce uno strumentario di tutele anche in quei rapporti che non trovano una facile collocazione nell'orizzonte ordinamentale, destinato ad allargarsi sempre di più con l'incessante evolvere dell'innovazione tecnologica[17]. Così, se il diritto delle pratiche commerciali (s)leali si è idealmente (e tradizionalmente) collocato accanto al diritto della concorrenza, a presidio del corretto funzionamento del mercato interno, ora è altresì evidente la contiguità tra il diritto del consumo e la disciplina sulla privacy, specialmente in quei peculiari rapporti che nascono e si sviluppano in rete, potenzialmente di durata indeterminata[18].

Quest'ultimo rilievo non sorprende se si pone mente al fatto che la disciplina delle pratiche commerciali scorrette ha avuto anche il merito di aver posto al centro la persona – similmente alla disciplina sulla privacy – così ponendo l'accento sulle condizioni soggettive di vulnerabilità rilevanti nell'assunzione di decisioni di natura commerciale libere e consapevoli, attraverso la previsione di un obbligo generale di attenzione posto a carico del professionista (*duty of care*)[19].

---

[16] In questo senso cfr. J. LITMAN, *Information Privacy/Information Property*, in 52 *Stanford Law Review*, 2000, p. 1283, tra i primi assertori della tesi proprietaria e del corollario del potere dispositivo del dato personale.

[17] Art. 3, par. 1, direttiva n. 2005/29/CE; cfr. S. ORLANDO, *Le informazioni*, Padova, 2012, p. 98, in cui l'Autore riconosce la portata innovativa della direttiva 2005/29/CE, il cui «carattere generale» e il cui obiettivo di armonizzazione completa hanno attribuito «unità ed identità normativa» ad una materia prima oggetto di sole normative settoriali; cfr. S. PERUGINI, *Le pratiche commerciali scorrette*, in *Diritto dei consumi – Soggetti, atto, attività, enforcement*, a cura di L. ROSSI CARLEO, Torino, 2015, p. 162.

[18] Allo sviluppo delle pratiche commerciali "leali", come finalità fondamentale della disciplina, fa espressamente riferimento il considerando 2 della direttiva: «lo sviluppo di pratiche commerciali leali all'interno dello spazio senza frontiere interne è essenziale per promuovere le attività transfrontaliere». Cfr. L. NIVARRA, *Diritto privato e capitalismo: regole giuridiche e paradigmi di mercato*, Editoriale Scientifica, 2010, p. 77 ss.; M. RADEIDEH, *Fair Trading in EC Law Information and Consumer Choice in the Internal Market*, Groningen, 2005, p. 259.

[19] Cfr. S. ORLANDO, *ult. op. cit.,* p. 99 ss. Al riguardo, giova rammentare che la disciplina delle pratiche commerciali sleali recata dalla direttiva 2005/29/CE non impone ai professionisti requisiti di contenuto positivo, con ciò rinunciando a individuare gli elementi al ricorrere dei quali una pratica può definirsi "leale". La direttiva, piuttosto, si limita a porre un unico, generale divieto, ovvero quello di ricorrere a pratiche commerciali sleali, cui segue la fissazione dei criteri e dei parametri in applicazione dei quali può stabilirsi se e in quale misura detto divieto debba considerarsi violato; cfr. G. DE CRISTOFARO, *Il divieto di pratiche commerciali sleali. La nozione generale di pratica commerciale «sleale» e*

Nella vicenda posta all'attenzione dell'AGCM e, in seguito, del TAR Lazio, è di tutta evidenza che tali condizioni siano venute a mancare contribuendo ad incidere negativamente su quella dinamica negoziale del consenso, che involge tanto aspetti della persona in quanto consumatore, tanto aspetti della persona in quanto utente[20].

Coerentemente con questa impostazione, si rinsalda quel binomio che già negli anni '90 la migliore dottrina indicava come costitutivo della tutela dei dati personali, fulcro attorno cui edificare l'intera disciplina: la riservatezza e la trasparenza[21].

Solo così ogni soggetto viene effettivamente posto nelle condizioni di esercitare quella "sovranità su di sé" che è tipica di ogni società democratica. La raccolta dei dati riconducibili alla persona avviene in sede di erogazione di servizi di tipo diverso: alcuni servizi online intanto possono essere erogati, in quanto siano stati previamente (e necessariamente) forniti alcuni dati dell'utente (si pensi all'indirizzo di domicilio o residenza, qualora si chieda la consegna di un bene acquistato attraverso una piattaforma di *e-commerce*).

Altri dati, invece, vengono richiesti per finalità diverse ed ulteriori, ovvero per scopi di *marketing* o di profilazione dell'utente. Solo questi ultimi contribuiscono, evidentemente, al fenomeno di

i parametri di valutazione della «slealtà», in *Le «pratiche commerciali sleali» tra imprese e consumatori – La direttiva 2005/29/Ce e il diritto italiano*, a cura di ID., Torino, 2007, pp. 124-125.

[20] Cfr. R. DI RAIMO, *Autonomia privata e dinamiche del consenso*, Napoli 2003, p. 138 ss. Sulla duplicità del soggetto immerso in questi rapporti e le relative tutele che allo stesso devono essere accordate, in quanto "utente" ed in quanto "interessato", cfr. S. TOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente, cit.,* p. 131.

[21] Il riferimento va ineludibilmente a Stefano Rodotà, allora Presidente dell'Autorità Garante della Protezione dei Dati Personali, il quale nella consueta Relazione annuale (1997), nel sottolineare il passaggio fondamentale del diritto «ad essere lasciato solo», al diritto del cittadino «immerso nel flusso della comunicazione, che plasma in ogni momento anche le relazioni interpersonali e sociali» afferma che «così la tutela dei dati personali non recide il legame sociale, né uccide la trasparenza, ma si presenta come il luogo d'un difficile equilibrio sempre da verificare, tra valori diversi». E mette in guardia dalle insidie che spesso si celano dietro ad alcune espressioni tipiche riferite alla privacy: «L'uomo di vetro è metafora totalitaria perché, reso un omaggio di facciata alle virtù civiche, nella realtà lascia il cittadino inerme di fronte a chiunque voglia impadronirsi di qualsiasi informazione che lo riguardi». Per poi lanciare un monito sul binomio riservatezza/controllo: «La privacy cammina ormai con due gambe: la riservatezza e il controllo. Alla prima si addice il silenzio, all'altra la trasparenza. Non basta rimanere al riparo dall'indiscrezione altrui: è indispensabile non perdere il controllo sulle proprie informazioni. Viviamo, infatti, in una società nella quale lasciamo continuamente tracce, cediamo informazioni in cambio di servizi». Riflessioni poi confluite in S. RODOTÀ, *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997.

patrimonializzazione dei dati, stante la loro assimilazione al "corrispettivo" nel rapporto di scambio posto in essere dalle parti[22].

Alla luce di quest'ultima accezione, la decisione in commento offre l'abbrivio per sviluppare alcune riflessioni sul valore assunto dai dati personali, sia da un punto di vista giuridico che economico. Il TAR, infatti, non sembra revocare in dubbio la sussistenza di un rapporto di consumo tra utente e social network, così accogliendo definitivamente la tesi, ormai maggioritaria in dottrina, secondo cui non possano qualificarsi come gratuiti *sub specie juris* tali rapporti[23].

La questione si era già posta in termini non dissimili alle stesse autorità, amministrativa e giudiziaria, che, dinanzi ad un problema di trasparenza dell'offerta di beni o servizi pubblicizzati come gratuiti – dietro però il consenso al trattamento dei dati personali –, ribadivano la necessità di un corretto inquadramento come rapporto di consumo[24].

---

[22] Cfr. S. THOBANI, *op. cit.*, in particolare p. 132, nota 2; V. ZENO ZENCOVICH, *op. cit.*, p. 22. Qui l'Autore si pone l'interrogativo centrale nel dibattito, ovvero se possa o meno configurarsi un vero e proprio mercato dei dati. A questo riguardo, si fa riferimento al mercato per così dire primario dei dati, nel senso di mercato in cui sono gli interessati stessi a immettere i dati nei circuiti di circolazione e, in senso diverso, al mercato secondario dei dati, in cui i titolari del trattamento, una volta raccolti i dati, li fanno a loro volta circolare.

[23] Per l'assenza di gratuità e, conseguente, applicabilità della disciplina consumeristica, v. G. DE NOVA, *I contratti per l'accesso ad Internet*, in *Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 1, 1996, p. 42-43; F. DELFINI, *I contratti dei consumatori e Internet*, in C. VACCÀ (a cura di), *Consumatori, contratti, conflittualità. Diritti individuali, interessi diffusi e mezzi di tutela*, Milano, 2000, p. 337; S.F. BONETTI, *La tutela dei consumatori nei contratti gratuiti di accesso ad internet: i contratti dei consumatori e la privacy tra fattispecie giuridiche e modelli contrattuali italiani e statunitensi*, in *Diritto dell'informazione e dell'informatica*, 6, 2002, p. 1129 ss.; P. SAMMARCO, *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del web 2.0*, in *Diritto dell'informazione e dell'informatica*, 4-5, 2010, p. 640; F. AGNINO, *Fino a che punto è possibile disporre contrattualmente dei propri diritti?*, in *Giurisprudenza di merito*, 12, 2012, p. 2559. Anche in sede europea, l'orientamento prevalente è quello di considerare applicabili le norme a tutela dei consumatori.

[24] Cfr. per l'AGCM, provv. nn. 10276, 10277, 10278 e 10279, 20 dicembre 2001, in *Boll. sett. AGCM n. 51-52*, 7 gennaio 2002, p. 148-165. Segnala come si tratti della prospettiva emersa nell'ordinamento statunitense M. GRAZIADEI, *Collusioni transatlantiche: consenso e contratto nel trattamento dei dati personali*, in F. DI CIOMMO, O. TROIANO (a cura di), *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, Piacenza, 2018, p. 367. Sulla possibile scorrettezza delle pratiche in questione v. A. DE FRANCESCHI, *op. cit.,* p. 101 ss. Sull'applicabilità della normativa in materia di pratiche commerciali scorrette ai casi di raccolta di dati personali v. anche M. RHOEN, *Beyond consent: improving data protection through consumer protection law*, in *Internet Policy Review*, 5, 2016, p. 7-8 (il quale accenna anche alla possibilità di applicare le norme in materia di clausole vessatorie); N. VAN EIJK, C.J. HOOFNAGLE, E. KANNEKENS, *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, in *European Data Protection Law Review*, 3, 2017, p. 334, i quali svolgono l'analisi con riguardo sia all'ordinamento statunitense che a quello europeo; C. GOANTA, S. MULDERS, *'Move Fast and Break Things': Unfair Commercial Practices and Consent on Social Media*, in *Journal of European Consumer and Market Law*, 4, 2019, p. 141 ss. Sulla rilevanza della necessità di fornire

Parafrasando il ragionamento dei giudici in queste pronunce, ciò che deve emergere con tutta chiarezza, affinché l'utente possa essere messo nelle condizioni di adottare scelte libere e consapevoli, è il nesso sinallagmatico che, almeno di fatto, si instaura tra la fornitura di un bene o di un servizio e la prestazione del consenso al trattamento dei dati personali. Pertanto, potrà essere sanzionata come pratica commerciale scorretta l'aver dichiarato che la gratuità del servizio, quando in realtà l'utente è costretto, per accedervi, a "pagare" acconsentendo al trattamento dei propri dati. Rientrerà anche in questo perimetro di scorrettezza, quella pratica commerciale tesa ad offrire un servizio prevedendo per l'utente la scelta se acconsentire o meno al trattamento dei propri dati, ma senza rendere tale possibilità chiara ed esplicita[25].

Nell'ottica di tutela del mercato, si pongono anche i recenti interventi legislativi dell'Unione Europea, in particolare con la direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, che esplicita nitidamente la prassi di scambiare beni o servizi con dati personali[26]. Qui è ancor più chiaro il fine di mettere al servizio dell'utente l'apparato rimediale a tutela dei consumatori, a prescindere da come sia stato "pagato" il servizio stesso[27].

In conclusione, la prestazione del consenso al trattamento dei dati, laddove prevista nell'ambito della fornitura di un bene o servizio, deve essere presa in considerazione al fine di applicare la disciplina a tutela dei consumatori. Tuttavia, se da un lato l'emersione del nesso di sinallagmaticità di fatto esistente tra servizio e consenso al trattamento vale ad assicurare la trasparenza delle operazioni economiche, e quindi del mercato, con le conseguenze che ne discendono in termini rimediali, dall'altro non sembra risolvere, salvo forzature, il problema

---

un'informazione completa e trasparente in merito al trattamento dei dati personali anche ai fini della valutazione sulla correttezza delle pratiche commerciali, cfr. TAR Lazio, sez. I, 11 aprile 2018, n. 5043.

[25] Cfr. S. THOBANI, *ult. op. cit.*, p. 135.

[26] Cfr., in particolare, la Direttiva 2019/770/UE del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. Essa è applicabile non solo qualora il contenuto o servizio digitale sia fornito al consumatore in cambio di un prezzo, ma anche «nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico» (art. 3, par. 1).

[27] Il pagamento in questo caso può avvenire tanto in denaro quanto in dati personali. Cfr., infatti, il considerando n. (24), in cui si precisa che «oltre a riconoscere appieno che la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce, la presente direttiva dovrebbe garantire che i consumatori abbiano diritto a rimedi contrattuali, nell'ambito di tali modelli commerciali».

inerente alla liceità di questo tipo di scambi, e quindi dell'esistenza stessa di questo tipo di mercato.

In questa prospettiva, quindi, si riuscirebbe a regolare la forma di tali operazioni, ma non la sostanza, rappresentando quest'ultima la soglia oltre la quale il sindacato di liceità non può spingersi[28].

3.4. Configurazione dei dati nel mercato unico digitale

Il regolamento generale sulla protezione dei dati personali (GDPR) sottolinea che «il diritto alla protezione dei dati personali non è un diritto assoluto; deve essere considerato in relazione alla sua funzione nella società ed essere bilanciato con altri diritti fondamentali, conformemente al principio di proporzionalità»[29].

Conseguentemente, la protezione deve adattarsi sia alle misure da adottare (ad es. *trasparenza*), sia alla base giuridica (ad es. il *consenso* preventivo dell'interessato o l'interesse legittimo di un responsabile del trattamento) necessario affinché il trattamento sia lecito ed equo. Un siffatto trattamento dei dati personali si rivela non solo legittimo, ma anche utile nell'ottica del perseguimento dell'interesse generale[30].

---

[28] In tal senso cfr. F. BILOTTA, *Consenso e condizioni generali di contratto*, in V. CUFFARO, V. RICCIUTO (a cura di), *Il trattamento dei dati personali*, Torino, 1999, II, 103-104. Come noto, ai sensi dell'art. 34, c. 2, cod. cons., il contenuto economico dei contratti tra professionisti e consumatori non è oggetto di valutazione, purché le condizioni contrattuali siano esposte in maniera chiara e trasparente. Il confine tra squilibrio economico e normativo dei contratti tra professionisti e consumatori costituisce un tema delicato e complesso. Cfr., *ex multis*, P. SIRENA, *sub Art. 1469-ter, 2° comma*, in G. ALPA, S. PATTI (a cura di), *Clausole vessatorie nei contratti dei consumatori*, in *Il codice civile. Commentario* fondato da P. SCHLESINGER e diretto DA F.D. BUSNELLI, Milano, 2003, p. 855 ss.; A. FICI, *sub Art. 34*, in E. NAVARRETTA, A. ORESTANO (a cura di), *Dei contratti in generale*, in *Commentario del codice civile* diretto da E. GABRIELLI, IV, Torino, 2011, p. 828 ss.

[29] Cfr. in particolare il considerando 4: «Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica».

[30] Cfr. N. ZORZI GALGANO, *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, dove si offre una lettura critica e autorevole della nuova disciplina sulla privacy, con particolare attenzione alle due anime del GDPR: la tutela della persona di fronte al trattamento dei dati personali, da una parte, e la libertà di circolazione di tali dati, dall'altra parte. Oggetto dell'indagine sono il rapporto tra persona e mercato dei dati personali, la proprietà dei dati personali, i dati personali come oggetto

In tale contesto, i dati – ed in particolare le informazioni relative alla vita e alle abitudini di ciascuno – sembrano costituire un bene molto prezioso che può offrire benefici agli individui stessi (semplificando la loro vita), alle imprese (poste nelle condizioni di predire il comportamento dei consumatori) e ai Governi (consentendo sistemi di controllo pubblico, ad esempio, per contrasto al terrorismo), diventando così «una nuova fonte di immenso valore economico e sociale»[31].

Secondo un approccio orientato al mercato, i dati personali avrebbero valore commerciale e potrebbero essere impiegati per questo tipo di sfruttamento. In questo senso, sarebbero etichettati come "personali" in virtù del fatto che "appartengono" all'interessato, in senso dominicale, ovvero sulla base di un diritto di proprietà.

Gli individui avrebbero il potere di impedire la divulgazione e l'utilizzo non autorizzati delle informazioni personali e, quindi, il potere di impedire ad altre persone di accedervi. Seguendo un simile approccio, la questione se i dati personali possano essere beni negoziabili dovrebbe essere risolta caso per caso, considerando l'interesse che si intenda proteggere. Ciò significa che se i dati personali sono considerati simili a una merce o a beni che possono essere destinati ad essere appropriati o sfruttati commercialmente, si applicherebbe il regime di protezione e circolazione adeguato a tali beni, essendo mutuabile ora dalla legge sul diritto d'autore, ora dal diritto del consumo o, più in generale, dal diritto dei contratti, quale piena espressione di autonomia negoziale[32].

---

di operazione economica, la circolazione dei dati personali e l'autonomia privata, il trattamento dei dati per finalità di profilazione e le decisioni automatizzate, il diritto alla portabilità dei dati, il diritto all'oblio, gli altri diritti dell'interessato, gli obblighi e gli adempimenti a carico del titolare del trattamento, il ruolo del Garante, il trasferimento all'estero dei dati personali, la responsabilità da illecito trattamento dei dati personali.

[31] *Ex multis*, cfr. O. TENE - J. POLONETSKY, *Privacy in the Age of Big Data: A Time for Big Decisions*, in 64 *Stanford Law Review Online*, 2012, p. 63.

[32] Questo approccio è stato particolarmente sostenuto nella letteratura giuridica americana: cfr. R.A. POSNER, *The Right of Privacy*, in 12 *Georgia Law Review*, 1977, p. 393-422; J. LITMAN, *op.cit.;* A. BARTOW, *Our Data, Ourselves: Privacy, Propertization, and Gender*, in 34 *University of San Francisco Law Rev.,* 2000, p. 633; J. ZITTRAIN, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, in 52 *Stanford Law Rev.*, 2000, p. 1201-1250; L. LESSIG, *Privacy as Property*, in 69 *Social Research*, 2002, p. 247-269; P.M. SCHWARTZ, *Property, Privacy and Personal Data*, in 7 *Harvard Law Rev.*, 2004, p. 2056-2128. In Italia, cfr. L.C. UBERTAZZI, *Banche dati e privacy*, in *Diritto industriale*, 2002, p. 633, in cui l'Autore osserva che il diritto delle persone a consentire il trattamento dei propri dati personali ha lo stesso quadro giuridico dei diritti di proprietà intellettuale; V. ZENO ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Diritto dell'informazione e dell'informatica*, 1993, p. 547. *Amplius*, nel dibattito europeo, cfr. Y. POULLET, Data *Protection between Property and Liberties. A Civil Law Approach*, in H.W.K. KASPERSEN e A. OSKAMP eds, *Among Friends*

Negli ultimi interventi di diritto eurounionale, inoltre, si fa espresso riferimento alla protezione dei dati come "contenuto digitale" e se ne ammette l'uso commerciale, riservando ad essi un trattamento speciale[33].

Quando, invece, sono in gioco i diritti fondamentali, si dovrebbe applicare la legge sulla protezione dei dati, nella misura in cui le forme di protezione da essa stabilite risulterebbero più adatte a garantire esclusivamente gli interessi relativi alla persona.

La tesi della natura ibrida della protezione dei dati personali, che involgerebbe sia diritti economici che diritti fondamentali della personalità dell'individuo, è stata argomentata considerando la scelta che il legislatore europeo avrebbe compiuto nella Carta dei diritti fondamentali, consistente nella separazione in due distinte disposizioni del diritto al rispetto della vita privata e familiare, *ex* art. 7, e del diritto alla protezione dei dati personali, *ex* art. 8. Ciò avrebbe determinato l'evoluzione, a partire dalle due fondamentali norme richiamate, di due concetti molto distinti tra loro: di tal guisa, i dati personali, ancorché espressione di diritti fondamentali della persona, troverebbero maggiore e più compiuta protezione per il loro valore di mercato[34].

Inoltre, il presupposto che sta alla base di questo approccio utilitaristico alla protezione dei dati personali è fornito da un'osservazione empirica della pratica odierna nel mercato e nella vita sociale, specialmente nel mondo online, dove grandi quantità di dati personali vengono trasferiti nell'ambito di acquisizioni per fusione e altre operazioni straordinarie tra imprese[35]. In Internet, le persone pongono in

---

in Computer and Law. A Collection of Essays in Remembrance of Guy Vandenberghe, The Hague: Kluwer Law International, 1990, p. 160; L.A. BYGRAVE, *Data Protection Law. Approaching its Rationale, Logic and Limits,* The Hague: Kluwer Law International, 2002, p. 120; N. PURTOVA, *Property Rights in Personal Data: a European perspective*, The Hague: Kluwer Law International, 2011, p. 1.

[33] Cfr. dapprima la direttiva 2011/83/UE in relazione ai diritti del consumatore, che protegge espressamente il "contenuto digitale" in base alla sua definizione di «dati prodotti e forniti in forma digitale» (cfr. art. 2, n. 11); direttiva 2019/770/UE del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, che prende direttamente in considerazione la prassi di scambiare beni o servizi con dati personali (cfr. art. 3, par. 1); direttiva 2019/771/UE del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di vendita di beni, che modifica il regolamento 2017/2394/UE e la direttiva 2009/22/CE, e che abroga la direttiva 1999/44/CE.

[34] Sul punto, cfr. PRINS, *Property and Privacy: European Perspectives and the Commodification of our Identity*, in L. GUIBAULT - P.B. HUGENHOLTZ eds, *The Future of the Public Domain*, Netherlands: Kluwer Law International, 2006, p. 244.

[35] Come visto nella questione che ha visto coinvolti WhatsApp e Facebook, cfr. AGCM, proc. PS10601 CV154, provv. 26597, del 11 maggio 2017, in Bollettino settimanale 18/2017.

essere accordi per la divulgazione, la raccolta, l'uso e il riuso dei propri dati personali; in alcuni casi, ricevono una qualche forma di compenso, quindi sfruttano economicamente anche dati personali sensibili[36].

Nelle teorie sopra esposte, il presupposto per l'applicazione della logica proprietaria e mercantilistica con riferimento ai dati personali riposa sul fatto che i dati possono essere sottoposti a un processo di lavorazione e mercificazione (potrebbe dirsi secondo un processo assimilabile al *manufacturing*), che li identifica con qualsiasi altro tipo di merce negoziabile. La mercificazione delle informazioni sarebbe inevitabile, soprattutto per i consumatori in relazione ai loro dati personali, come nel caso che ci occupa. Un tale processo di estensione, inoltre, assicurerebbe – in adesione a questa tesi – un livello più elevato di protezione, prendendo come riferimento, ad un tempo, i diritti di proprietà (industriale ed intellettuale) e la disciplina consumeristica[37].

Cionondimeno, un tale approccio orientato al mercato sembra essere insoddisfacente, almeno entro i confini europei, perché il concetto di protezione dei dati personali non sembra adatto ad una definizione in termini di scambio di valore, o inquadrabile *tout court* nel granitico schema proprietario.

Ciò è ancora più evidente se si pone mente al fatto che è assai difficile trovare un'idea generale relativa al diritto di proprietà, che sia condivisa dai più importanti codici civili adottati nel secolo scorso dagli Stati europei[38].

La legge sulla protezione dei dati non conferisce esplicitamente agli interessati un diritto esclusivo di utilizzare e godere della proprietà dei propri dati, tantomeno di disporne[39]. Inoltre, va notato che lo

---

[36] Cfr. G. RESTA, V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete, cit.*, p. 417, ove gli autori sostengono che «È davvero singolare la tesi che vorrebbe che tale sterminata fortuna derivasse da operazioni prive di rilievo giuridico-economico perché "gratuite". Piuttosto sorge il dubbio che la situazione si possa rovesciare: sono gli utenti che forniscono un servizio (i dati) a determinate imprese e vengono da questi remunerati con dei servizi digitali. Posto che il valore sta nei dati (*sub specie* «Big Data»), la concorrenza innovativa sta nel creare nuovi servizi che possano essere considerati un corrispettivo per la loro cessione. Non ci sarebbe dunque nulla di strano se una impresa versasse un contributo monetario (ad es. sotto forma di uno sconto sul prezzo) all'utente che le fornisce i dati».

[37] In questo senso sempre L. LESSIG, *op. cit.*, p. 255.

[38] Anche a voler considerare la categoria giuridica della proprietà e i suoi requisiti di circolazione e trasferimento, come formulati nel *Draft of Common Frame of Reference* (DFCR), ai sensi dell'articolo VIII.-1: 202 e dell'articolo VIII.-2: 101, dovremmo sostenere che i dati personali non possono essere investiti di diritti di proprietà.

[39] C. VON BAR, *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR)*, Munich: Sellier European Law Publishers, 2009, p. 422.

sfruttamento commerciale dei dati personali non può essere distaccato da quegli aspetti riguardanti la *vulnerabilità* dell'interessato. Ed è qui che sembrerebbero intrecciarsi ancor più intensamente le maglie tra disciplina sulla privacy e disciplina consumeristica.

Il problema che emerge con ogni evidenza attiene alle possibili interferenze tra le diverse discipline che dovrebbero trovare applicazione a diversi e distinti aspetti: così, ad esempio, la creazione e la vendita sul mercato di una vasta banca dati, ottenuta attraverso la profilazione di un gran numero di cittadini e persino attraverso il trattamento dei loro dati sensibili, può apparire lecito se visto dalle sole prospettive della legge sul diritto d'autore e del diritto dei contratti, ma tale operazione può comportare la violazione di norme sulla protezione dei dati aventi un carattere obbligatorio, che può rendere l'intero contratto - o alcune sue clausole – annullabile o persino nullo[40]. L'opinione che renderebbe commercializzabili i dati personali solleverebbe, dunque, non poche perplessità e spesso si rivela incompatibile non solo con le regole del trattamento dei dati, ma anche con le caratteristiche essenziali del consenso e con l'obiettivo ultimo di salvaguardare efficacemente i diritti in questione.

Ciò condurrebbe, inoltre, ad una falsa prospettiva, giacché i dati personali non sono semplicemente *informazioni*. Essi si riferiscono ad una persona fisica particolare, identificata o identificabile, e possono essere in grado di rivelare alcuni degli aspetti più intimi e delicati della personalità della persona, come il suo stato di salute o la vita sessuale.

In questa prospettiva, il loro valore non è legato al criterio economico e quantitativo della commerciabilità, ma piuttosto ad una logica basata sulla protezione dei diritti e dei valori della persona[41]. Questo emerge con forte evidenza dalla produzione legislativa che è stata espressamente dedicata a garantire la protezione dei dati personali e

[40] Cfr. P.M. SCHWARTZ, *op. cit.*, p. 2060-2094, il quale sostiene che «this hybrid inalienability regime will permit an initial transfer of personal data from the individual, but only if the concerned individual is granted an opportunity to block further transfers or uses by unaffiliated entities. Moreover, this ability to block will generally be set as an opt-in, which means that further use or transfer will not be allowed unless the individual affirmatively agrees to it». Ed aggiunge che: «The proposed hybrid inalienability follows personal information through downstream transfers and limits the negative effects that result from "one-shot" permission to all personal data trade». Cfr. altresì F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008, p. 235-242.

[41] *Ibidem*, p. 149-152. Sulle modalità di quantificazione del valore economico dei dati personali, v. invece G. MALGIERI, B. CUSTERS, *Pricing privacy – the right to know the value of your personal data*, in *Computer Law & Security Review*, 34, 2017, p. 294-297. Cfr. in proposito F.G. VITERBO, *Freedom of contract and the commercial value of personal data*, in *Contratto e impresa Europa*, 2, 2016, p. 606-607.

ciò indipendentemente dal fatto che tali dati possano essere dotati di un valore economico. In nessun intervento legislativo, nazionale o sovranazionale, volto alla protezione dei dati personali, è previsto un tipo di contratto atto a consentire all'interessato o al responsabile del trattamento di disporre dei dati personali. Allo stesso modo, non vi è spazio per lo sfruttamento commerciale dei dati personali nella formulazione e nella logica degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea.

Tuttavia, è proprio a questo proposito che i dati personali sembrano differire da tutti gli altri beni nell'ordinamento giuridico italiano e, più in generale, dell'Unione Europea. Da un lato, come evidenziato, si pongono come elementi costitutivi dell'identità personale dell'interessato; dall'altro, i dati personali possono servire come una risorsa importante che può formare oggetto, non già di appropriazione, ma piuttosto di accesso ad un determinato bene o servizio[42]. Alla luce di quanto precede, i dati personali possono essere considerati come beni immateriali, non (direttamente) trasferibili e funzionali allo sviluppo della persona[43].

Infine, un'altra tesi in dottrina, non molto dissimile dalla precedente, ha inteso considerare i dati personali come beni intermedi e strumentali, piuttosto che finali. In questa chiave, i dati personali non avrebbero un valore intrinseco, ma piuttosto derivante dal loro utilizzo ed elaborazione, al fine di ottenere opportunità di guadagno o, in qualche altra misura, utilità o benessere[44]. In base a questo approccio,

---

[42] Cfr. S. Spiekermann, A. Acquisti, R. Böhme, K.L. Hui, *Personal Data Markets*, 25 *Electronic Markets*, 2015, p. 91, i quali osservano che i dati personali «non sono solo un normale bene negoziabile» e che «possono essere altamente sensibili e rivelare l'identità di una persona». Ed aggiungono che «L'elaborazione è legalmente limitata dalle leggi sulla protezione dei dati e sulla privacy. In molti paesi, la privacy e il diritto all'autodeterminazione delle informazioni sono riconosciuti come un diritto umano». Questo punto di vista è stato confermato di recente da Giovanni Buttarelli nel parere 8/2016 del Garante europeo della protezione dei dati (GEPD) sull'applicazione coerente dei diritti fondamentali nell'era dei big data, il 23 settembre 2016, paragrafo 4, in cui sostiene che «nell'Unione Europea, le informazioni personali non possono essere concepite come una mera risorsa economica».

[43] Così considerati, i dati potrebbero agevolmente farsi rientrare nella migliore definizione che di *beni comuni* è stata offerta da parte della Commissione Rodotà (2007) che, come noto, non ha ancora trovato pieno accoglimento nel nostro ordinamento giuridico, ma che purtuttavia si conferma d'ausilio anche nella comprensione del fenomeno che sta investendo i dati personali nell'era digitale. Riprendendo il nucleo forte di tale definizione, questi particolari beni sono «cose che esprimono utilità funzionali all'esercizio dei diritti fondamentali, nonché al libero sviluppo della persona».

[44] Questa analisi è stata elaborata da Richard A. Posner: « People invariably possess information, including facts about themselves and contents of communications, that they will incur costs to conceal. Sometimes such information is of value to others: that is, others will incur costs to

gli unici beni mercantili e commerciabili sembrano essere i benefici e le utilità (economiche) che il responsabile del trattamento riceve solo dopo il trattamento dei dati personali, a condizione che tale trattamento sia effettuato nel pieno rispetto della legge sulla protezione dei dati personali[45].

Da questo punto di vista, quando si fa riferimento ai dati personali, il concetto di trattamento implicherebbe che un insieme speciale di regole debba essere applicato a tutte le questioni relative ai dati personali e alla loro circolazione sul mercato. Questo regime si configura totalmente autonomo e non si sovrappone alle norme di diritto comune relative al trasferimento di proprietà (anche intellettuale). Pertanto, il problema non è stabilire come e quando un soggetto possieda i dati personali o quando, viceversa, non li possieda. Il vero nocciolo della questione diventa stabilire se e come i dati personali possano circolare, il ché equivale a dire se e come possano essere trattati[46].

Sul versante della normativa a tutela della privacy emerge, dunque, come lo scopo del fondamentale intervento del legislatore europeo del 2016 sia stato quello di garantire che i dati personali venissero trattati nel rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati. Le limitazioni alla commerciabilità dei dati derivano proprio da questo humus. A fortiori, da ciò derivano le norme che dettano i requisiti di validità del consenso, che deve essere libero. Si giustappongono, dunque, due tipi di interessi: da un lato, quello alla libera circolazione dei dati, in un'ottica di sviluppo del mercato unico digitale; dall'altro, quello alla protezione dei dati personali come

discover it. Thus, we have two economic goods, "privacy" and "prying". We could regard them purely as consumption goods, the way economic analysis normally regards turnips or beer; and we would then speak of a "taste" for privacy or for prying. But this would bring the economic analysis to a grinding halt because tastes are unanalyzable from an economic standpoint. An alternative is to regard privacy and prying as intermediate rather than final goods, instrumental rather than ultimate values. Under this approach, people are assumed not to desire or value privacy or prying in themselves but to use these goods as inputs into the production of income or some other broad measure of utility or welfare», in R.A. POSNER, *op. cit.*, p. 394.

[45] In questo senso, cfr. S. THOBANI, *op. cit.,* p. 144, ove afferma che «occorre sottolineare che il diritto alla protezione dei dati personali non rappresenti in sé un bene finale da tutelare, ma sia strumentale alla tutela di altri interessi».

[46] Da questo punto di vista, sarà interessante analizzare l'estensione della libertà contrattuale nell'ambito della protezione dei dati personali. Infatti, sebbene non tutte le regole di trattamento abbiano lo stesso campo di applicazione, la separazione delle regole di circolazione da quelle che regolano il trattamento dei dati personali non sembra comunque possibile. Sul punto cfr. F.G. VITERBO, *op. cit.*, p. 156-158., e F. FERRETTI, *A European Perspective on Data Processing. Consent through the Re-conceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously*, in ERPL, 2012, p. 481.

espressione di un diritto fondamentale, consacrato dall'art. 8 della Carta dei dritti fondamentali dell'Unione Europea.

Tali interessi non hanno esclusivamente natura individuale, ma riguardano anche la collettività e, pertanto, è fortemente avvertita l'esigenza di tutela di interessi collettivi[47].

Con questo regolamento, ed in continuità con i precedenti interventi in materia[48], il legislatore europeo intende tutelare non solo gli interessi dei singoli, ma principalmente interessi collettivi che possono essere pregiudicati dal trattamento posto in essere con le nuove tecnologie, e dunque a carattere massivo. Come rilevato da attenta dottrina, questo pare essere il punto di vista privilegiato dell'analisi dei dati, imperniato sui rapporti di massa: l'aggregazione dei dati è utile per il perseguimento di fini diversi e ulteriori, che trascendono il singolo utente cui appartengono, tant'è che lo stesso può persino conferirli in forma anonima o pseudonimizzata[49].

3.5. Considerazioni conclusive

Lasciate sullo sfondo le implicazioni di carattere concorrenziale[50], il focus del dibattito permane sulla patrimonializzazione dei dati

[47] Sul punto, cfr. A. MANTELERO, *Personal data for decisional purposes in the age of analytics: From an individual perspective to a collective dimension of data protection*, in *Computer Law & Security Review*, 32, 2016, p. 239 ss.

[48] Il regolamento si pone in linea di continuità con gli strumenti normativi che in materia lo hanno preceduto: la direttiva 96/45/CE, che restringeva anch'essa il proprio campo di applicazione al trattamento automatizzato dei dati e a quello, anche non automatizzato, dei dati contenuti in archivi; la convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale adottata a Strasburgo il 28 gennaio 1981 (ratificata dall'Italia con l. 21 febbraio 1989, n. 98), che è applicabile solo alle «elaborazioni automatizzate di dati a carattere personale».

[49] «In quest'ottica, la limitazione dello sviluppo di un mercato di dati personali pare essere in buona parte volta alla tutela di interessi collettivi. Al titolare del trattamento interessa poco chi sia la persona cui i dati si riferiscono considerata nella sua individualità, la quale è invece tenuta in conto unicamente come punto di riferimento di informazioni, la cui aggregazione è utile per lo svolgimento di attività ulteriori (come inviare pubblicità mirata, effettuare ricerche di mercato o analisi predittive) in cui l'individuo è preso in considerazione come parte di una massa», così S. THOBANI, *op. cit.,* p.145. L'A. giunge alla conclusione che «si utilizza […] uno strumento di tutela individuale […] per proteggere in realtà interessi generali messi a rischio dai trattamenti di massa».

[50] Solo uno sparuto numero di *players* sul mercato digitale può accedere ad un incalcolabile quantitativo di dati e sopportarne i relativi costi di aggregazione e trattamento. Inoltre, sul rapporto tra libertà economiche e il diritto alla protezione dei dati personali v. O. POLLICINO, M. BASSINI, *Bridge is Down, Data Truck Can't Get Through…A Critical View of the Schrems Judgment in the Context of European Constitutionalism*, in G. ZICCARDI CAPALDO (a cura di), *The Global Community. Yearbook of International Law and Jurisprudence, Oxford,* 2016, p. 254.

personali e la conseguente emersione di un vero e proprio mercato dei dati, che esige regole nuove per il suo corretto funzionamento. Profili che pongono all'interprete due questioni fondamentali, su cui è auspicabile una riflessione corale in dottrina e giurisprudenza, soprattutto alla luce degli ultimi dati normativi forniti dal regolatore europeo[51]. Entrambe le questioni attengono ai dati: la prima, in senso statico, reclama una tassonomia degli stessi, volta a distinguere, *in primis*, il dato personale dal dato non personale; la seconda, in senso dinamico, attiene alla *governance*, all'accesso e all'uso dei dati, opportunamente distinti tra loro [52].

Un vero e proprio statuto dei dati, dunque, che possa, al contempo, preservare le dinamiche di un corretto gioco del mercato e garantire la tutela della persona, nella duplice veste di interessato e consumatore, fuori e dentro la dimensione digitale.

[51] Il riferimento va alle direttive europee del 2019 nn. 770 (relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali) e 771 (relativa a determinati aspetti dei contratti di vendita di beni); nonché, da ultimo, alla proposta di regolamento della Commissione per regolare l'accesso e l'uso dei dati (cd. *Data Act*). Questa rappresenta la seconda iniziativa regolamentare europea dopo il *Data Governance Act*: mentre quest'ultimo crea procedure e strutture per facilitare la condivisione dei dati da parte di aziende, privati e settore pubblico, il *Data Act* chiarisce chi può creare valore dai dati e a quali condizioni. Tra gli obiettivi dichiarati, vi è quello di rimuovere le barriere all'accesso ai dati il cui valore attualmente non viene raccolto a causa di una serie di fattori. In sintesi, non v'è chiarezza in merito alla possibilità di utilizzare e accedere ai dati generati dai prodotti; inoltre, le Pmi spesso non sono in grado di negoziare accordi equilibrati di condivisione dei dati con soggetti del mercato più forti; infine, troppi ostacoli al passaggio tra *cloud* competitivo e affidabile e servizi all'avanguardia, unita ad una limitata capacità di combinare dati provenienti da diversi settori. Il *Data Act* mira a garantire che i dati siano condivisi, archiviati ed elaborati nel pieno rispetto delle norme europee e, secondo i suoi promotori, si candida a costituire la pietra angolare di un'economia digitale europea forte, innovativa e sovrana.

[52] Con riferimento al profilo relativo alla necessità di una tassonomia dei dati, Cfr. G. COMANDÈ, G. SCHNEIDER, *Regulatory challenges of data mining practices: the case of the never-ending lifecycles of "health data"*, in *European Journal of Law*, 25, 2018, p. 284-307, dove si prendono le mosse per una classificazione a partire dagli *"health data"*. Con riferimento ad una prima distinzione tra dati personali e non, in particolare cercando di definire l'estensione dei primi, cfr. C. IRTI, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *juscivile*, 2, 2020, p. 379 ss., in particolare p. 382, dove l'Autrice sostiene che «[r]iuscire a definire con esattezza cosa s'intenda con questa locuzione [*dati personali, ndr.*] è, di conseguenza, presupposto essenziale per comprendere quale sia l'ambito effettivo di estensione della tutela ad essi riconosciuta».

4. I procedimenti amministrativi di vigilanza sul mercato dei servizi digitali

Filippo D'Angelo (Università di Sassari)

4.1. La proposta della Commissione n. 2020/361 del 15 dicembre 2020 per un regolamento sul «mercato unico dei servizi digitali»

Il 15 dicembre 2020 l'Unione europea ha pubblicato la proposta n. 2020/361 per adottare un regolamento sul «mercato unico dei servizi digitali»; dopo una lunga attesa il documento è intervenuto a colmare un vuoto legislativo non più procrastinabile e ha dettato «norme armonizzate sulla prestazione di servizi intermediari nel mercato interno»[1].

Questi i suoi obiettivi: «stabilire un ambiente online sicuro, prevedibile e affidabile»[2]; contrastare la diffusione di «contenuti illegali» in

[1] Art. 1, par. 1; come chiarisce il cons. n. 4 il nuovo regolamento introduce una «serie mirata di norme obbligatorie uniformi, efficaci e proporzionate a livello dell'Unione al fine di tutelare e migliorare il funzionamento del mercato interno. Il presente regolamento stabilisce le condizioni per lo sviluppo e l'espansione di servizi digitali innovativi nel mercato interno».

[2] Art. 1, par. 2, lett. b.

rete[3]; garantire la neutralità delle piattaforme telematiche[4]; tutelare i diritti fondamentali degli utenti[5].

La nuova normativa si applicherà a tutti i «servizi intermediari prestati a destinatari il cui luogo di stabilimento o di residenza si trova nell'Unione» (il riparto delle funzioni di vigilanza segue dunque un criterio territoriale)[6]; e riguarderà nello specifico i servizi di semplice trasporto ("mere conduit"), di memorizzazione temporanea ("caching") e di memorizzazione su richiesta dell'utente ("hosting")[7].

In quest'ultima categoria rientrano le «piattaforme online», come i social network o i mercati digitali[8], che possono assumere «dimensioni molto grandi» se «prestano i loro servizi a un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni», ossia al 10% della popolazione totale dell'Unione[9].

4.2. La coamministrazione delle funzioni di vigilanza

L'esecuzione del nuovo regolamento è stata affidata a un «sistema comune» di autorità amministrative formato dalla Commissione, dai coordinatori nazionali dei servizi digitali e dal comitato che li riunisce[10]; in base al disposto regolamentare essi «cooperano tra loro»

[3] Cioè «qualsiasi informazione che, di per sé o in relazione ad un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme alle disposizioni normative dell'Unione o di uno Stato membro» (art. 2, lett. g).

[4] Cons. n. 20.

[5] Che ai sensi del cons. n. 41 sono la libertà d'informazione e di espressione; il diritto alla riservatezza e alla vita privata; la libertà d'impresa; la tutela della proprietà intellettuale.

[6] Art. 1, par. 3.

[7] Art. 2, lett. f) che include nel concetto di «servizio intermediario»: un «servizio di semplice trasporto ("*mere conduit*"), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire accesso a una rete di comunicazione; un servizio di memorizzazione temporanea ("*caching*"), consistente nel trasmettere, su una rete di comunicazione, informazioni fornite dal destinatario del servizio, che comporta la memorizzazione automatica, intermedia e temporanea di tali informazioni al solo scopo di rendere più efficiente il successivo inoltro delle informazioni ad altri destinatari su loro richiesta; un servizio di "*hosting*", consistente nel memorizzare informazioni fornite da un destinatario del servizio su richiesta di quest'ultimo».

[8] Cons. n. 13.

[9] Art. 25, par.1.

[10] Cons. n. 45.

secondo collaudati meccanismi di coamministrazione delle funzioni di vigilanza[11]. La proposta di regolamento ha assegnato alla Commissione e alle autorità nazionali rilevanti poteri istruttori (possono richiedere informazioni ai prestatori di servizi digitali; possono ispezionare i loro locali aziendali; possono sequestrare documenti; possono verbalizzare qualunque dichiarazione ricevuta) e altrettanto incisivi poteri decisionali (possono ordinare la cessazione di comportamenti illeciti; possono imporre misure correttive e accettare impegni vincolanti; possono adottare misure cautelari; possono irrogare sanzioni pecuniarie e penalità di mora) da esercitare nel rispetto del principio del contraddittorio coi destinatari[12].

La vigilanza settoriale spetta in prima battuta alle autorità nazionali (secondo il menzionato criterio del luogo di stabilimento dell'impresa vigilata), anche se sono previsti specifici meccanismi di interlocuzione con la Commissione; le autorità pubbliche dell'Unione e degli Stati membri sono infatti collegate attraverso raccordi di natura procedimentale ed è qui che si può apprezzare più nitidamente l'intensità della loro collaborazione.

4.3. La collaborazione procedimentale tra i «coordinatori dei servizi digitali» nazionali e la Commissione

Tanto accade, ad esempio, nella procedura di «cooperazione transfrontaliera tra coordinatori dei servizi digitali» e la Commissione che si svolge nel seguente modo.

Il procedimento è avviato da qualunque coordinatore nazionale dei servizi digitali che può chiedere al coordinatore competente per territorio di «valutare la questione e di adottare le misure di indagine e di esecuzione necessarie» qualora vi sia il sospetto che un prestatore di servizi intermediari abbia violato le norme del nuovo regolamento[13]. La richiesta è motivata in punto di fatto e diritto ed è corredata delle prove necessarie[14]. Ricevuta l'istanza il coordinatore interpellato avvia

[11] Art. 38, par. 2.

[12] Art. 41, par. 1 e par. 2 (per quanto concerne le autorità di vigilanza nazionali); artt. 54-63 (per quanto riguarda la Commissione).

[13] Art. 45, par. 1.

[14] Art. 45, par. 2.

l'indagine ed entro due mesi comunica la propria valutazione del caso, indicando le eventuali misure adottate[15].

Laddove l'autorità proponente «non abbia ricevuto una risposta» alla propria richiesta nel termine previsto, oppure «non concordi con la valutazione del coordinatore dei servizi digitali» interpellato[16], può deferire la questione alla Commissione che la esamina entro tre mesi. Se giunge a conclusioni diverse da quelle dell'autorità nazionale che ha condotto l'indagine la Commissione le può chiedere di «valutare ulteriormente la questione e di adottare le misure di indagine o di esecuzione necessarie» nei successivi due mesi[17].

Tuttavia il procedimento non termina qui: se l'indagine riguarda una «piattaforma online di grandi dimensioni» e il coordinatore dei servizi digitali competente non ha svolto il supplemento istruttorio richiesto dalla Commissione[18], quest'ultima può richiamare a sé il procedimento di vigilanza e da quel momento il «coordinatore dei servizi digitali del luogo di stabilimento interessato non è più autorizzato ad adottare alcuna misura di indagine o di esecuzione in relazione alla pertinente condotta della piattaforma online di dimensioni molto grandi interessata»[19]. Egli può solo coadiuvare la Commissione, fornendole il fascicolo d'indagine con tutte le informazioni necessarie affinché questa possa adottare la decisione più appropriata nei confronti della piattaforma telematica vigilata[20].

4.4. (segue): la vigilanza congiunta sulle piattaforme digitali di ingenti dimensioni

Un procedimento in parte analogo si osserva per la «vigilanza rafforzata sulla piattaforme online di dimensioni molto grandi». In base alle disposizioni del nuovo regolamento quest'ultime sono soggette ad

---

[15] Art. 45, par 3 e par. 4.

[16] Art. 45, par. 5 e par. 6.

[17] Art. 45, par. 7.

[18] Il presupposto previsto dall'art. 51, par. 1, lett. a) è che la piattaforma di grandi dimensioni «abbia violato una qualsiasi delle disposizioni del presente regolamento senza che il coordinatore dei servizi digitali del luogo di stabilimento abbia adottato alcuna misura di indagine o esecuzione a seguito della richiesta della Commissione di cui all'articolo 45, paragrafo 7, dalla scadenza del termine stabilito in tale richiesta».

[19] Art. 51, par. 2.

[20] Art. 51, par. 3.

alcuni specifici oneri comportamentali come ad esempio: adottare misure cicliche di attenuazione dei rischi sistemici (ossia la manipolazione dei dati e la loro illegale divulgazione); sottoporsi ogni anno ad audit indipendenti; detenere un registro dei dati pubblicitari diffusi al pubblico; istituire un ufficio di contatto con le autorità di settore[21]. In caso di una o più sospette violazioni la Commissione, il comitato dei coordinatori o almeno tre coordinatori nazionali dei servizi digitali possono interpellare il coordinatore competente per territorio e chiedergli di avviare un'indagine[22].

Aperto il procedimento l'autorità agente prende subito contatto con la piattaforma telematica vigilata e le può anzitutto chiedere di elaborare un «piano di azione in cui precisi come intende far cessare o porre rimedio alla violazione»[23]; e poi di sottoporsi a un «audit indipendente supplementare che consenta di valutare l'efficacia di tali misure nel far cessare o porre rimedio alla violazione»[24]. Esauriti tali passaggi istruttori il coordinatore dei servizi digitali comunica alla Commissione, al comitato e alla piattaforma online se ritiene o meno che le misure intraprese abbiano rimediato alla violazione riscontrata; dopodiché egli «non è più autorizzato ad adottare alcuna misura di indagine o di esecuzione»[25].

Il motivo è presto spiegato: qualora infatti persista una violazione regolamentare spetta solo alla Commissione il potere di intervenire, al posto dell'autorità nazionale, nei confronti della piattaforma digitale con una decisione puntuale[26]. Si ripete allora lo stesso schema già visto nel precedente procedimento: la Commissione avvia un'indagine in autonomia, ma col supporto dell'autorità nazionale, e al termine adotta il provvedimento di vigilanza più adatto a reprimere la violazione, ricostituendo in unità l'esercizio del potere decisionale inizialmente condiviso con l'altro ente.

[21] Artt. 26-32.
[22] Art. 50, par. 1.
[23] Art. 50, par. 2.
[24] Art. 50, par. 3.
[25] Art. 50, par. 4.
[26] Art. 51, par. 1, lett. c).

4.5. Alcune considerazioni sul procedimento amministrativo e sul suo valore organizzativo

Sicuramente è prematuro avanzare previsioni sull'impatto che avrà il nuovo regolamento sui servizi digitali dell'Unione all'indomani della sua entrata in vigore; un dato, tuttavia, appare di estremo valore e si deduce dalla struttura dei due procedimenti appena analizzati che forniscono importanti elementi di riflessione sul tema generale dell'organizzazione e del procedimento amministrativo.

Andando infatti oltre il profilo puramente esteriore rappresentato dalla contitolarità della funzione tipica dei fenomeni di coamministrazione, emerge con evidenza che in entrambi i procedimenti il legislatore dell'Unione ha posizionato una relazione organizzativa che esprime il momento culminante della collaborazione tra le autorità amministrative coinvolte. I due procedimenti si caratterizzano, a ben vedere, per il potere della Commissione di sostituirsi al coordinatore nazionale dei servizi digitali nei casi tipicizzati dal regolamento; e in questo senso possiedono valenza organizzativa[27].

La regolamentazione settoriale sui servizi digitali sembra dunque comprovare, ove ce ne fosse ancora bisogno, l'elevato potenziale scientifico che si annida nei «sistemi comuni» dell'Unione; e conferma l'utilità di studiare la disciplina del procedimento amministrativo non solo sul piano formale (la scansione in fasi) o sul piano sostanziale (l'esercizio del potere pubblico), ma anche nei suoi immanenti aspetti organizzativi: cioè dalla (poco esplorata) prospettiva delle relazioni organizzative che attengono al momento dell'azione e realizzano fenomeni

[27] Si vedano per i saggi M.R. SPASIANO, *Storia, fondamento e attualità del potere sostitutivo nella pubblica amministrazione: dalla logica della straordinarietà all'amministrazione alternativa*, in *Dir. e soc.*, 1, 2019, 41 ss.; A. POLICE, *Il potere sostitutivo dello Stato nei confronti delle regioni: condizioni e limiti di esercizio*, in *I controlli sulle autonomie nel nuovo quadro istituzionale*, Milano, 2007, 653 ss.; M. CAMMELLI, *Poteri sostitutivi*, in G. Falcon (a cura di), *Lo Stato autonomista. Funzioni statali, regionali e locali nel decreto legislativo n. 112 del 1998 di attuazione della legge Bassanini n. 59 del 1997*, Bologna, 1998, 32 ss.; U. BORSI, *Intorno al cosiddetto controllo sostitutivo*, in *Studi senesi*, 3, 1916, 7 ss. Per le opere monografiche si vedano invece M. SCUDIERO, *I controlli sulle regioni sulle province e sui comuni nell'ordinamento costituzionale italiano*, I, Napoli, 1963; E. ESPOSITO, *Il potere sostitutivo. Amministrazione centrale ed enti locali*, Napoli, 1968; G. SIRIANNI, *Inerzia amministrativa e poteri sostitutivi*, Milano, 1991; C. BARBATI, *Inerzia e pluralismo amministrativo. Caratteri – sanzioni – rimedi*, Milano, 1992; M. BOMBARDELLI, *La sostituzione amministrativa*, Padova, 2004.

di compartecipazione soggettiva all'esercizio di funzioni amministrative unitarie[28].

Tali relazioni – di solito inquadrate nelle elaborazioni dottrinali su un piano esclusivamente statico[29] – sono lo specchio di un'organizzazione pubblica che nel tempo ha mutato pelle ed è passata da un sistema compatto a un complesso disaggregato e multilivello anche per effetto dell'integrazione amministrativa europea che ha segnato il formale trapasso verso un sistema reticolare di poteri e interessi pubblici collocati anche al di fuori del territorio nazionale[30].

---

[28] Si confronti F. BENVENUTI, *I controlli amministrativi dello Stato sulla regione*, in *Riv. trim. dir. pubbl.*, 2, 1972, 596-597.

[29] Lo ricorda M. BOMBARDELLI, *La sostituzione amministrativa*, cit., 76: in «questo modello si assume che il potere amministrativo possa essere concentrato in modo stabile nel vertice dell'organizzazione e da qui venire poi eventualmente distribuito per quote decrescenti verso i gradi inferiori della gerarchia e verso le articolazioni periferiche dell'organizzazione, secondo un principio per cui tutti i compiti possono essere ripartiti *ex ante*, in modo prevedibile e statico. I collegamenti fra le diverse parti dell'organizzazione vengono considerati come articolati secondo linee verticali, in cui le relazioni sono asimmetriche ed orientate in modo univoco e non variabile in senso discendente, perché chi occupa una posizione sovraordinata o centrale ha per definizione più potere di chi ha una posizione subordinata o periferica e mantiene sempre questo differenziale attivo, qualsiasi sia la relazione posta in essere. Si ritiene che tutti i rapporti organizzativi si svolgano sulla base di questo differenziale di potere, in base al quale l'organo subordinato agisce unicamente sulla base di quanto gli viene richiesto dai livelli gerarchici superiori, mentre l'organo sovraordinato può sempre agire sovrapponendosi all'ufficio subordinato, determinandone l'azione e indirizzandola secondo un percorso esattamente prevedibile. Il vertice della piramide è così il necessario punto di passaggio e di intermediazione di tutti i collegamenti che si possono stabilire fra le diverse unità organizzative subordinate o periferiche. Le interdipendenze fra le diverse parti dell'organizzazione sono considerate come del tutto condizionate dagli impulsi che derivano dal vertice e per questo stabili, invarianti e prevedibili»; si vedano anche G. D'ALESSIO, *I giuristi e l'organizzazione amministrativa*, in *Queste istituzioni*, 2, 1983, 11-13 e M.S. GIANNINI, *Amministrazione pubblica*, in *Enciclopedia delle scienze sociali*, I, 1991, 182 ss.

[30] Per un rilievo in questo senso si veda E. CARLONI, *Lo Stato differenziato. Contributo allo studio dei principi di uniformità e differenziazione*, Torino, 2004, 296, per il quale lo «scenario con cui si confronta chi voglia analizzare lo sviluppo contemporaneo delle istituzioni pubbliche deve tenere conto di un dato difficilmente controvertibile: la natura plurale e composita delle pubbliche amministrazioni» che «viene ad essere percepita, ed assunta come tale anche dallo stesso legislatore». Per conseguenza è «venuta meno la certezza che l'organizzazione amministrativa inerisca all'ordinamento statale e consista di una porzione dell'elemento organizzazione proprio di questo, poiché il diritto positivo mostra sconfinamenti sempre più marcati in altri ordinamenti, sicché elementi organizzativi di ordinamenti diversi compartecipano all'esercizio di funzioni amministrative. Di più, queste funzioni si svolgono talora tra più ordinamenti, o

Nella rinnovata fisionomia dell'ordinamento contemporaneo le relazioni organizzative, all'inizio concettualizzate per un sistema ordinato per gradi, fanno ora leva su un'esigenza di flessibilità e di elasticità più adatta a un'amministrazione frammentata in un coacervo di poteri concomitanti[31]. Qui i rapporti tra le persone giuridiche pubbliche rifuggono all'evidenza ogni tentativo di rigida partizione come avveniva nella passata esperienza; e reclamano invece un'altra qualità che è quella di sapersi adattare ai differenti settori di governo della società e alle specifiche necessità di pubblico interesse che lì si manifestano[32]. Poco importa sapere ogni volta chi è sovraordinato, chi è parificato, chi sta in posizione strumentale; non si dànno collocazioni invariabili; non vi è più un unico soggetto, un attore privilegiato, da cui fuoriescono tutte le attribuzioni e le competenze amministrative[33].

Le relazioni organizzative, per come tramandate di consueto, certo permangono anche nel nuovo quadro dell'amministrazione, e non potrebbe essere altrimenti; ma quel che adesso rileva è il diverso scenario in cui esse si collocano (l'ordinamento declinato al plurale[34]) e il

comportano comunque l'attività di più soggetti, oltre lo Stato, talché si è proposta la più vasta e precisa definizione di apparato di pubblici poteri, come l'insieme dei soggetti (e del relativo elemento organizzante) che compartecipano di funzioni amministrative» (così S. VALENTINI, *Figure, rapporti, modelli organizzatori. Lineamenti di teoria dell'organizzazione*, in G. Santaniello (diretto da), *Trattato di diritto amministrativo*, IV, Padova, 1996, 5).

[31] La natura composita dell'attuale sistema amministrativo è evidenziata tra i tanti da L. TORCHIA, *Il riordino dell'amministrazione centrale: criteri, condizioni e strumenti*, in *Dir. pubbl.*, 3, 1999, 691; nonché da S. CASSESE, *Concentrazione e dispersione dei poteri pubblici*, in *Studi in onore di Paolo Biscaretti di Ruffia*, I, Milano, 1987, 153-154; e prima ancora da G. GUARINO, *L'organizzazione pubblica*, Milano, 1977, 88-89.

[32] Utili spunti riflessivi in M. CAMMELLI, *Amministrazione di risultato*, in *Annuario 2002*, Milano, 2003, 118.

[33] È la conclusione di G. DI GASPARE, *Organizzazione amministrativa*, in *Dig. disc. pubbl.*, X, Torino, 1995, 524.

[34] Il punto è colto ancora da M. BOMBARDELLI, *La sostituzione amministrativa*, cit., 155: la «complessità dei problemi da affrontare richiede che le diverse componenti dell'organizzazione amministrativa agiscano in modo fortemente interdipendente, il che impone loro di adottare modelli organizzativi flessibili e dinamici, che non consentono più di guardare all'organizzazione amministrativa secondo un disegno unitario, armonico e stabile». Le «relazioni organizzative si allontanano quindi dalla loro immagine tradizionale, ordinata in un quadro sempre riconducibile alla piramide gerarchica e articolata in riferimento quasi esclusivo ai suoi punti di vertice. La loro evoluzione avviene in coerenza ad un modello diverso, in cui il legame tra le diverse competenze e l'ordine reciproco che essere vengono ad assumere non si reggono solo sull'equilibrio statico della loro distinzione formale, ma si appoggiano anche sui punti

risultato pratico cui esse aspirano (la cura congiunta dell'interesse pubblico[35]): due fattori che condizionano le modalità di collegamento tra gli enti interessati.

Ecco allora che in un contesto caratterizzato da una galassia di poteri congeneri le relazioni organizzative, altrimenti evanescenti se inquadrate secondo la loro tradizionale versione teorica, riscoprono un ruolo essenziale di collante sistemico; e lo fanno nella sede che, meglio di altre, è in grado di governare la moltiplicazione delle competenze presenti in un'organizzazione in perenne movimento, conferendole la necessaria agilità di manovra: il procedimento amministrativo[36].

Il passaggio è di fondamentale importanza.

L'attenuazione del modello gerarchico, e la sua tendenziale sostituzione ad opera di un principio di legittimazione a carattere procedimentale, hanno ridefinito il volto delle relazioni organizzative per come tradizionalmente intese; in origine configurate per una amministrazione costruita secondo un ideale di rigida gradualità, esse hanno dovuto rinnovare se stesse nel momento in cui la dimensione piramidale dell'organizzazione si è slegata in una miriade di figure soggettive autonome che di regola agiscono attraverso il veicolo procedimentale[37].

Il punto di svolta sta, insomma, nell'avvento del procedimento amministrativo come modulo ordinario di svolgimento delle funzioni

---

mutevoli di equilibrio dinamico individuati dalle connessioni organizzative temporanee e variabili che sono necessarie per affrontare le complessità del reale e possono fornire all'amministrazione pubblica la flessibilità necessaria per consentirle di raggiungere nel modo migliore i risultati che le sono affidati».

[35] Inteso come l'insieme di diritti (e di doveri) costituzionali che appartengono alla collettività secondo L.R. PERFETTI, *L'organizzazione amministrativa come funzione della sovranità popolare*, in *Dir. econ.*, 1, 2019, 58-59.

[36] La disciplina procedimentale finisce così per tracciare le linee di un'organizzazione dinamica frutto di un'amministrazione complessa e policentrica in cui agiscono soggetti diversi, ma al contempo connessi; il procedimento diviene, in altre parole, «regola di organizzazione della funzione amministrativa e regola di misurazione della reciproca rilevanza, nel processo decisionale, di interessi, diversi e a volte anche contrapposti, la cui cura è attribuita a soggetti distinti, ma il cui coordinamento si impone per il raggiungimento del risultato complessivo: la definizione dell'interesse, o meglio della risultante della composizione di interessi, tutelato come pubblico» (così G. SALA, *Sui caratteri dell'amministrazione comunale e provinciale dopo la riforma del Titolo V della Costituzione*, in *Le Regioni*, 1, 2004, 17).

[37] Si veda A. ROMANO TASSONE, *Sui rapporti tra legittimazione politica e regime giuridico degli atti dei pubblici poteri*, in *Dir. e proc. amm.*, 1, 2007, 108 (ID., *Note sul concetto di potere giuridico*, in *Ann. Messina*, 2, 1981, 457).

amministrative in un'organizzazione complessa e come canale di collegamento dinamico tra poteri pubblici. È qui che la legge intende ricomporre in unità il pluralismo che connota la società contemporanea; ed è ancora qui che oramai albergano le relazioni organizzative che (ri)acquistano così piena evidenza esteriore e rinforzata dignità sul piano della teoria giuridica.

Nella loro nuova veste esse rilevano entro, e non oltre, il perimetro del procedimento amministrativo ed emergono in occasione di esso; è per questo che hanno il carattere della duttilità in quanto scandiscono connessioni variabili in base al tipo di funzione ideata dalla legge. Fuori dal procedimento amministrativo non vi possono essere, se non da un punto di vista astratto, relazioni organizzative[38]; è questo il diverso orizzonte di inserimento che esse hanno (ri)guadagnato nella dogmatica giuridica dell'organizzazione pubblica.

Le relazioni organizzative vanno adesso inquadrate nella logica di risultato tipica dell'intelaiatura procedimentale. La loro è una dimensione che si potrebbe definire contingente – ma non casuale – perché scaturisce dalla specifica fisionomia della funzione amministrativa e dal modo in cui la legge sceglie di aggregare, volta per volta e in modi sempre diversi, gli enti pubblici che ne fanno parte[39]. La flessibilità delle relazioni organizzative importa che una figura soggettiva che ricopre per legge un certo ruolo all'interno di una funzione, ne può poi assumere un altro in un diverso contesto procedurale; si tratta, insomma, di una stabilità cinetica e fluttuante che si rinnova nella continua tensione dell'attività amministrativa al suo scopo naturale: l'interesse pubblico.

L'esempio dei procedimenti di coamministrazione è in questo senso eloquente: sono infatti procedimenti che rilevano anche in chiave organizzativa – si direbbe quasi che diano luogo a una organizzazione procedimentale – e che si adattano alle esigenze specifiche dei settori

[38] Essendo oramai chiaro che le relazioni organizzative sono concepite dall'ordinamento come mezzi giuridici di collegamento soggettivo e servono a realizzare fattispecie complesse in cui la funzione amministrativa è scomposta in segmenti imputabili ad agenti diversi, ma diretti a produrre un solo effetto (cfr. G. MARONGIU, *L'attività direttiva nella teoria giuridica dell'organizzazione*, Padova, 1989, 113).

[39] In tal modo le singole figure soggettive «acquistano ciascuna una posizione relativa (un senso di posizione volta per volta variabile e relativo), in funzione del risultato da perseguire» (così D. D'ORSOGNA, *Contributo allo studio dell'operazione amministrativa*, Napoli, 2005, 279).

in cui il diritto dell'Unione intende conseguire un effetto di integrazione tra figure soggettive autonome.

L'eterogeneità dei fini rilevabili nei settori comuni richiede di modellare relazioni organizzative procedimentali differenziate e capaci di adattarsi alle cangianti necessità di pubblico interesse indicate dalla legge; la quale ogni volta può decidere di raccordare in modo diverso persone giuridiche in principio poste su un piano di reciproca indifferenza[40]. Emerge con evidenza la loro logica intrinseca: nella realtà contemporanea – di cui l'Unione europea è parte costitutiva – è frequente che una pluralità di soggetti, e quindi di poteri pubblici, formalmente separati venga attivata per risolvere un solo problema amministrativo. In simili occasioni assume preminente centralità l'esigenza del loro collegamento dinamico per raggiungere il risultato previsto; e la trama organizzativa è esattamente il prodotto dei nessi giuridici che inquadrano le figure soggettive all'interno della procedura amministrativa. Quando ciò accade subentrano appunto le relazioni organizzative come modi normativi per coniugare enti autonomi in procedimenti complessi diretti a uno scopo comune[41].

4.6. Relazioni organizzative (procedimentali) e buon andamento dell'azione amministrativa

Quanto precede testimonia allora l'utilità di inquadrare le relazioni organizzative in una prospettiva dinamica e giustifica il breve approfondimento svolto che vuole rinverdire, in chiave problematica, la riflessione su un tema talvolta liminale nel panorama della letteratura giuridica domestica.

Se un elemento di sintesi è emerso dal nostro discorso è che le relazioni organizzative, ricollocate nella loro appropriata dimensione topologica, assicurano il buon funzionamento dell'apparato

[40] Lo ricorda anche G. SYDOW, *Cooperazione amministrativa nell'Unione europea*, in *Studi parlamentari e di politica costituzionale*, 203-204, 2019, 31 ss. (studio che si pone in linea di continuità col lavoro monografico *Verwaltungskooperation in der Europäischen Union*, Tübingen, 2004).

[41] Così che si può definitivamente affermare – usando le parole di G. BERTI, *La parabola della persona Stato (e dei suoi organi)*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, II, 1982/83, 1028 – che il procedimento amministrativo «riflette l'organizzazione», rispecchia l'immanenza dell'attività nell'organizzazione.

amministrativo, la sua tangibile epifania nel momento della azione. Nella dinamica relazionale – perché di ciò si tratta – le singole figure soggettive sono chiamate a esercitare i propri poteri in una condizione di reciprocità da cui non si possono sottrarre. Il collegamento plurisoggettivo può assumere morfologia diversa a seconda dei contesti d'intervento, ma ciò che conta è l'intelaiatura procedimentale che è finalmente in grado di mostrare il potenziale delle relazioni organizzative nella produzione degli effetti della funzione amministrativa[42].

Le relazioni organizzative, ogni volta che sono previste dalla legge, divengono un mezzo per consentire all'attività amministrativa di proseguire senza ostacoli verso i suoi obiettivi. In quest'ordine di idee si può sostenere che le relazioni organizzative, e l'intreccio collaborativo che esse esprimono, possiedono un sostrato di immanente doverosità; nel senso che sono legate a funzioni qualificate come obbligatorie per il grado di inderogabilità dei fini segnati dalla legge[43].

---

[42] Di «complesso plurisoggettivo» parla M. NIGRO, *L'edilizia popolare come servizio pubblico (Considerazioni generali)*, in *Scritti giuridici*, I, Milano, 1996, 380, per designare il collegamento di «vari soggetti (e della loro attività), per garantire anche da un punto di vista organizzativo, la convergenza delle attività verso l'unico fine».

[43] È questa l'esigenza che, ad esempio, sembra ispirare l'architettura istituzionale, a trazione direttiva, incaricata di attuare il piano nazionale di ripresa e resilienza finanziato con i capitali dell'Unione ai sensi del regolamento n. 241/2021 del 12 febbraio 2021.

In via preliminare si ricorda che ai sensi del citato regolamento i piani elaborati a livello nazionale devono coprire determinate aree d'intervento (ecologia, digitalizzazione, crescita economica e sociale, salute, politiche giovanili) e sono approvati di concerto dal Consiglio e dalla Commissione che possono sospendere o revocare i finanziamenti in caso di elusione degli impegni assunti dagli Stati membri.

Ai sensi del d.l. 31 maggio 2021, n. 77 convertito in legge 29 luglio 2021, n. 108 il sistema di gestione del piano di ripresa economica italiano ruota attorno a un organo centrale con «poteri di indirizzo» (denominato «cabina di regia» ai sensi dell'art. 2) coadiuvato da un ufficio di segreteria, tre uffici tecnici, due strutture di missione e un collegio consultivo.

La «gestione» dei singoli interventi inclusi nel piano chiama in causa le amministrazioni centrali dello Stato che, tramite le proprie strutture, coordinano le relative attività, vigilano sulle procedure di assegnazione dei fondi dell'Unione e sul loro corretto impiego, assicurano il celere raggiungimento dei traguardi fissati (art. 8). La «realizzazione operativa» degli interventi spetta invece, a cascata, agli enti regionali e alle amministrazioni locali secondo le rispettive competenze (art. 9).

Lo scopo generale perseguito dal sistema descritto è di «agevolare la realizzazione dei traguardi e degli obiettivi stabiliti dal Piano Nazionale di Ripresa e Resilienza» dal momento che «assume preminente valore l'interesse nazionale alla sollecita e puntuale realizzazione degli interventi» programmati (art. 1, commi 1 e 2). A tal fine il governo è abilitato a esercitare poteri sostitutivi in caso di mancato rispetto, omissione o ritardo di uno o più progetti inclusi nel piano (art. 12).

Per loro natura le relazioni organizzative garantiscono la continuità dell'azione amministrativa, evitano interruzioni nella cura degli interessi pubblici e danno la misura di come, in un'organizzazione complessa, il potere esercitato dalle singole autorità è molto spesso un ingranaggio di un più ampio meccanismo rivolto a conseguire determinati risultati; così facendo esse creano una rete di connessioni – di tipo procedimentale – fra i diversi centri di cura di interessi pubblici a struttura composita (come testimoniano i casi esaminati di coamministrazione).

Per le stesse ragioni le relazioni organizzative sono un antidoto al problema dell'inefficienza amministrativa e un viatico per una migliore amministrazione in risposta alla frammentazione delle competenze in un'organizzazione policentrica. Nella loro quotidiana applicazione esse compongono l'azione amministrativa e i suoi fini entro un sistema unitario che li riconduce alla fonte immediata della loro giustificazione nella società[44]. Nel concreto le relazioni organizzative attuano il precetto costituzionale del buon andamento tutte le volte che il legislatore intende fare in modo che l'azione degli apparati pubblici

Come si può notare l'impianto organizzativo e l'articolazione delle competenze intestate alle varie figure soggettive coinvolte nell'attuazione del piano economico nazionale sono chiaramente ispirati a una logica direttiva che vede nella cabina di regia il motore del sistema e nelle amministrazioni centrali e territoriali il braccio operativo. Quel che emerge è il carattere di doverosità della relazione organizzativa e al contempo la sua indefettibilità. Ciò dipende dal fatto che l'esecuzione tempestiva del piano è ineludibile, e ad essa è subordinata la provvista dei fondi stanziati dall'Unione. La cabina di regia svolge un'azione di impulso che mira a trasportare gli indirizzi del piano nella fase realizzativa – cioè procedimentale – che costituisce il punto d'incidenza dell'organizzazione sulla realtà esterna; suo precipuo compito è incanalare in un alveo unitario i vari atti di esecuzione del programma che non lascia spazio a separazioni di competenze rispetto all'interesse pubblico perseguito (in tema si veda L. GIANI, *L'amministrazione tra appropriatezza dell'organizzazione e risultato: spunti per una rilettura del dialogo tra territorio, autorità e diritti*, in *Nuove Autonomie*, 3, 2021, 575). È così dimostrato con un esempio concreto quanto si è inteso affermare nel testo in termini generali: e cioè che il carattere fondante delle relazioni organizzative è di assicurare un collegamento in vista di risultati che si pongono con grado di precettività nei confronti della pubblica amministrazione. In tali casi il procedimento è il canale che permette di raggiungere gli obiettivi prefissati e in esso si risolve l'organizzazione nello stesso modo in cui al suo interno si dispiega, sotto altro e diverso profilo, l'esercizio del potere amministrativo.

[44] Osservazioni in tema si possono leggere in A. POLICE, *Il potere, il coraggio e il tempo nel decidere. Corpi tecnici e loro valutazioni nel trentennale della legge sul procedimento amministrativo*, in A. Bartolini – T. Bonetti – B. Marchetti – B.G. Mattarella – M. Ramajoli (a cura di), *La legge n. 241 del 1990, trent'anni dopo*, Torino, 2021, 369-371.

avanzi senza indugi alla sua meta; e tale conclusione riposa sul connubio insolubile tra attività e organizzazione consacrato nel testo fondamentale agli artt. 97 e 98: da una parte il potere, come forza giuridica, con i suoi intrecci dinamici; dall'altra il dovere di risultato che sta alla base della funzione e che esprime il vincolo che lega l'amministrazione all'ordinamento e quindi alla sua comunità[45].

Le relazioni organizzative, ricollocate all'interno del procedimento, sono l'anello di congiunzione tra la statica e la dinamica amministrativa, tra la funzione e l'organizzazione come ha provato a dimostrare la serie di esempi proposti. I rapporti di sovraordinazione nelle loro evocate sfaccettature; i momenti di necessaria equiordinazione tra poteri interferenti a un pari livello di incidenza; le posizioni di strumentalità variamente declinate sono tutti accomunati dalla stessa esigenza di rilievo costituzionale: assicurare il buon andamento dell'attività amministrativa – inteso come spedito e inostacolato perseguimento di risultati di pubblico interesse, da parte di figure soggettive collegate, alla cui elastica realizzazione esse cospirano[46]. Si è dunque al cospetto di congegni normativi (formali e perciò prevedibili) intesi a razionalizzare l'amministrazione complessa e a rimuovere le barriere che la separano dalle finalità (unitarie) che essa deve raggiungere per ragioni di efficienza[47].

---

[45] Dovere che affonda le sue radici nel testo costituzionale italiano ed europeo (si veda per tutti F. MERUSI, *L'"imbroglio" delle riforme amministrative*, Modena, 2016, 46 ss.) e al cui servizio le relazioni organizzative sono preordinate per rispondere alle aspettative che la collettività nutre verso l'apparato amministrativo. Attraverso di esse (e grazie alla legge che le tipicizza) il buon andamento penetra nell'amministrazione e si può avverare l'ideale non più astratto dell'«incremento del benessere individuale, e sociale cui è dedicata tutta la struttura della pubblica amministrazione» (così V. CAPUTI JAMBRENGHI, *Introduzione al buon andamento della pubblica amministrazione*, in *Scritti in memoria di Roberto Marrama*, I, Napoli, 2012, 114). Nell'intersezione tra organizzazione e attività le relazioni organizzative, reinquadrate nella loro dimensione procedimentale, riescono a trovare un più che plausibile aggancio nel testo costituzionale.

[46] Collegando l'attività di più soggetti amministrativi le relazioni organizzative esprimono la rilevanza del principio di buon andamento, e ciò per effetto di due momenti concomitanti: da un lato la combinazione di competenze distinte; dall'altro l'attività considerata nel suo fluire verso un fine comune; ma ciò che più conta notare è che si tratta di meccanismi legali intesi a raccordare sul piano procedimentale entità soggettive quando lo richiedono ragioni specifiche di rapidità ed efficienza per realizzare certi obiettivi – inderogabili e quindi rilevanti in punto di buon andamento – cui sono preordinate le funzioni amministrative.

[47] Ossia il «miglior proporzionamento, al fine stabilito, dell'attività erogata» (così ancora M. NIGRO, *Studi sulla funzione organizzatrice della pubblica amministrazione*, Milano, 1974,

Una ricerca sul tema delle relazioni organizzative che voglia conseguire un traguardo, pur minimo, di utilità sul versante teorico ne deve mostrare anche le ricadute sul piano empirico; ed è questo forse l'indicatore più affidabile per misurare la persistente utilità dell'amministrazione pubblica (e della sua dogmatica giuridica) e per saggiarne la reale capacità, pur tra numerosi travagli, di adempiere alla sua missione quotidiana al servizio della collettività[48].

85, nel descrivere l'impatto organizzativo del canone giuridico di buon andamento dell'azione amministrativa).

[48] Che poi altro non è se non la tangibile realizzazione del «principio democratico» – di cui parla V. OTTAVIANO, *Merito (diritto amministrativo)*, in *Nov. dig. it.*, X, Torino, 1964, 576 – da porre in relazione ai compiti che l'amministrazione quotidianamente «svolge a favore dei cittadini».

5. Profili di tutela delle persone vulnerabili nell'ecosistema digitale. Il divieto di profilazione dei minori di età ai fini di *marketing*

Ilaria Garaci (Università Europea di Roma)

5.1. Le vulnerabilità nell'ecosistema digitale

Le tecnologie digitali sono diventate parte integrante della esperienza quotidiana, capaci non solo di migliorare la realtà esistente, ma altresì di offrire nuove opportunità di crescita individuale e globale. Sono sempre più evidenti i vantaggi conseguibili attraverso lo sviluppo dell'economica digitale, anche nella prospettiva del raggiungimento degli obiettivi di cui all'Agenda 2030 per lo sviluppo sostenibile. La crisi pandemica, determinata dal virus Covid-19, ha, peraltro, evidenziato l'imprescindibilità delle nuove tecnologie nei più variegati settori (sanità, lavoro, istruzione, cultura, intrattenimento, socializzazione, commercio, ecc.). Al contempo la stessa pandemia ha mostrato i punti di debolezza dello spazio digitale[1], l'emersione di nuove forme di vulnerabilità[2], nonché l'amplificazione di quelle tradizionali. Si consideri, a questo ultimo riguardo, la condizione in cui versano quei

[1] Si pensi, per fare qualche esempio, alla più facile disponibilità dei prodotti contraffatti, alla diffusione dei contenuti illegali, all'aumento delle frodi, dei furti e degli attacchi informatici, all' impatto della disinformazione e dei discorsi d'odio, all'insorgenza dei nuovi divari digitali (per es. fra zone urbane ben connesse e territori rurali isolati; tra coloro che hanno un più facile accesso allo spazio digitale e coloro che per ragioni socio-economiche o culturali non lo hanno; fra le imprese già in parte digitalizzate che hanno potuto sfruttare appieno e più rapidamente le potenzialità offerte dall'ambiente digitale e quelle meno digitalizzate). Cfr. *Comunicazione della Commissione europea del 9.3.2021*, "Bussola per il digitale 2030: il modello europeo per il decennio digitale".

[2] Quelle in particolare derivanti dalle asimmetrie strutturali di potere tra le imprese e gli individui (o le imprese di dimensioni minori) nell'ambiente digitale.

soggetti che, per motivi di salute o di età o per ragioni socio-economiche, non hanno capacità o strumenti adeguati a comprendere e/o a gestire i pericoli sottesi all'uso delle tecnologie più avanzate, rimanendo per ciò maggiormente esposti al rischio di subire lesioni (di natura patrimoniale e non) e/o di essere discriminati o emarginati, non solo dalla realtà digitale ma anche da quella sociale. Così, in generale, i minori di età, quando navigano *on line*, in ragione della scarsa consapevolezza (o incuranza) dei numerosi pericoli[3] disseminati nella rete vedono certamente acuita la loro condizione di debolezza. In una situazione di vulnerabilità ancor più accentuata si trovano inoltre: le persone con difficoltà o disabilità più o meno gravi, anche temporanee; i bambini e gli adolescenti provenienti da contesti socio-economici svantaggiati; i soggetti anziani che, per ragioni varie (perché inattivi, pensionati, ecc.), non hanno avuto occasione di confrontarsi con le nuove tecnologie. La condizione di debolezza di questi ultimi si esprime sotto un duplice profilo: da un lato, data la loro minore inclinazione all'uso degli strumenti digitali, sono maggiormente esposti ai pericoli della rete, quali per esempio le frodi, gli attacchi informatici; dall'altro lato, se non costantemente coadiuvati nell'impiego di determinate applicazioni, rischiano una condizione di emarginazione[4]. In relazione a questa ampia classe di soggetti (i vulnerabili fra i vulnerabili) lo sviluppo delle tecnologie, se non accompagnato da una progettazione inclusiva che agevoli l'accesso ai servizi digitali, garantendone la sicurezza, nonché da un sostegno educativo adeguato, rischia di determinare discriminazioni o emarginazioni o comunque di esacerbare le disuguaglianze già esistenti[5]. Di qui l'invito da parte delle istituzioni europee

[3] In linea generale possono individuarsi i seguenti gruppi di rischi: rischi di esposizione a contenuti inappropriati e a informazioni false o inesatte; 2. rischi di abuso e sfruttamento sessuale online; 3. rischi connessi al *cyberbullismo* (attivo e passivo); 4. rischi derivanti dal trattamento dei dati personali; 5. rischi di sviluppare dipendenza.

[4] E. ANDREOLA, *Minori e incapaci in Internet*, Napoli, 2019, p. 13.

[5] Osserva Aurelio Gentili come le situazioni di fragilità umana possano avere un' origine naturale (la minore età, la malattia, la disabilità, l'anzianità, ecc.) oppure sociale (la povertà, la condizione di rifugiati o di immigrati, l'appartenenza a culture e a confessioni religiose minoritarie, ecc..), quando hanno "origine nella naturale non si trasformerebbero in vulnerabilità *sociale* se il dato naturale, che in sé stesso potrebbe anche non essere un attentato al benessere, non divenisse socialmente occasione per non poter tenere il passo degli altri, o peggio per esserne feriti, discriminati, emarginati. Se la natura è l'*origine* del rischio è la società l'*autrice* del danno" (A. GENTILI, *La vulnerabilità sociale. Un modello teorico per il trattamento legale*, in *Riv. crit. dir. priv*., 2019, p. 42)

agli Stati membri di promuovere investimenti, politiche e misure proattive che, tenendo conto delle specificità soggettive delle persone, favoriscano, anche nell'ecosistema digitale, la piena esplicazione della persona, unitariamente considerata, al riparo dai rischi e nella prospettiva di cogliere dalle stesse tecnologie le opportunità di crescita individuale[6] e collettiva.

5.2 L'autodeterminazione del minore di età nell'ambiente digitale

Benché designati come "nativi digitali", i minori di età sono, dallo stesso ordinamento, considerati meritevoli di una protezione rafforzata nel contesto digitale, luogo in cui possono determinarsi lesioni importanti alla sfera della persona. La riconosciuta condizione di debolezza dei minori di età non funge tuttavia da ostacolo alla esplicazione della loro capacità di autodeterminazione[7], la quale, sulla linea tracciata dalle fonti internazionali ed euro-unitarie, ha nel tempo registrato una progressiva espansione[8], fino ad interessare anche il

[6] Gli stessi strumenti digitali, se progettati su misura della persona anziana o della persona con difficoltà o disabilità e supportati da un'adeguata educazione all'uso degli stessi, possono migliorare la qualità della vita e favorire l'inserimento dei soggetti più vulnerabili nella comunità.

[7] La condizione del minore si è infatti evoluta profondamente nel corso degli ultimi decenni. Da indifferenziato "oggetto di protezione" (l'espressione è di F. D. BUSNELLI, *Capacità e incapacità di agire del minore*, in *Dir. fam. pers e succ*., 1982, p. 56), incapace di gestire e curare i propri interessi e, come tale, sottoposto alla patria potestà, il minore, dotato di discernimento è oggi ritenuto capace di autodeterminarsi nelle scelte che si rivelano funzionali alla esplicazione della sua personalità (Cfr. P. STANZIONE, *Diritti fondamentali dei minori e potestà dei genitori,* in *Rass. dir.civ.,* 1980, p. 449). La nuova dimensione dialogica della relazione genitori-figli, come confermata e delineata nella disciplina della responsabilità genitoriale, di cui alla riforma legislativa sulla filiazione del 2012 e 2013, richiede che i genitori, nell'adempimento del loro compito educativo, rispettino l'identità del figlio, nel suo divenire (F. GIARDINA, *Morte della potestà e capacità del figlio*, in *Riv. dir. civ.*, 2016, p. 1609 ss.) e favoriscano la sua autodeterminazione, pur non rinunciando all'esercizio dei poteri/doveri di protezione, richiesti dalla responsabilità genitoriale per realizzare il "superiore interesse del minore".

[8] La capacità decisionale del minore, dotato di discernimento, con riguardo alle scelte di natura personale si estende, di fatto, anche alla sfera patrimoniale, non solo in relazione ai c.d. atti minuti della vita quotidiana, ma, secondo le più recenti ricostruzioni, anche con riferimento agli atti di natura patrimoniale strumentali all'esplicazione della personalità del minore, che sono quindi diretti a soddisfare interessi della vita sociale, strettamente attinenti alla dimensione identitaria della persona (c.d. atti

rapporto con la realtà digitale[9]. Fra le importanti novità apportate dalla nuova legislazione sulla privacy, a seguito del Regolamento UE/2016/679 (c.d. GDPR), si segnala infatti la previsione dell'età minima (14 anni) per esercitare in autonomia il consenso al trattamento dei dati personali, necessario per accedere ai servizi della società dell'informazione[10]. Pur circondato di cautele[11], il consenso rilasciato dal minore, nonché quello prestato dal genitore per consentire l'accesso al minore infra-quattordicenne, non vale a scongiurare i pericoli ai quali il minore risulta sempre più esposto durante la navigazione *on line*, né appare idoneo a garantire allo stesso quella autodeterminazione informativa che l'ordinamento astrattamente intende riconoscergli[12], a causa della opacità e complessità dei nuovi processi di raccolta

identitari) In tal senso R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, Torino, 2020, p. 31 ss.

[9] Nell'ambito della normativa dettata per contrastare il *cyberbullismo* (Legge 29 maggio 2017, n. 71) si prevede (art. 2, co.1) che il minore ultraquattordicenne possa inoltrare autonomamente al gestore del sito o del social media o comunque al titolare del trattamento (e in caso di inerzia di quest'ultimo al Garante), un'istanza di oscuramento, rimozione o blocco di qualsiasi dato personale che sia stato diffuso in rete in occasione di episodi di *cyberbullismo* che lo riguardino.

[10] L'art. 8 del GDPR dispone che "per quanto riguarda l'offerta diretta dei servizi della società dell'informazione ai minori" il trattamento è lecito ove questi abbia compiuto 16 anni, mentre per il minore infra-sedicenne il consenso è valido solo se prestato da chi esercita la responsabilità genitoriale. Il legislatore italiano, a seguito di un ampio dibattito, avvalendosi della deroga prevista dallo stesso GDPR di prevedere un'età diversa, non inferiore comunque ai 13 anni, ha ritenuto di abbassare la soglia ai 14 anni (art. 2-*quinquies* Codice della privacy, come modificato dal d.lgs 2018 n. 101). Al di sotto della suddetta soglia è necessario il consenso genitoriale.

[11] Il legislatore impone al titolare del trattamento specifici obblighi di trasparenza: per rivolgersi direttamente al minore occorre utilizzare un linguaggio semplice, chiaro, facilmente comprensibile dal minore stesso. Inoltre, il GDPR chiarisce che tali regole sul consenso lasciano comunque impregiudicate le disposizioni generali dei paesi membri in relazione alla validità, formazione o efficacia dei contratti stipulati dai minori.

[12] Sulla insufficienza del modello di tutela basato soltanto sul consenso Cfr. S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 82; A.M. GAMBINO, *Big data e fairness. Il ruolo delle authorities*, in *Nuovo dir. civ*., 2020, p. 298; D. POLETTI, *Comprendere il Reg. UE 2016/679: un'introduzione*, in A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, p. 12; I. A. CAGGIANO, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione*, in *Dir. merc. tecn*., 25 gennaio 2017, consultabile su https://www.dimt.it/index.php/it/la-rivista/16175-il-consenso- al-trattamento-dei-dati-personali-tra-nuovo-regolamento-europeo-gdpr-e-analisi-comportamentale- iniziali-spunti-di-riflessione, spec. pp. 13-14 ss.; G. FINOCCHIARO, *Il quadro d'insieme.*

dei dati personali, nonché dei limiti alla concreta libertà di scelta[13], considerato che la maggior parte delle volte il consenso è "imposto" quale condizione per accedere al servizio offerto[14]. Peraltro, nel GDPR non sono indicate le modalità per procedere all'accertamento dell'età anagrafica, che resta tutt'ora un problema aperto. Le relative piattaforme, ancorché prevedano il limite di età, di fatto non svolgono alcuna verifica, affidandosi alla mera dichiarazione dell'utente, consentendo in questo modo l'accesso anche ai minori appartenenti a fasce di età molto basse[15]. In ragione di tale emancipazione precoce del ("grande" come del "piccolo") minore nell'ambiente digitale assume particolare rilievo il *munu*s educativo dei genitori[16], come del resto confermano le diverse pronunce giurisprudenziali adottate in relazione agli illeciti compiuti *on line* dai minori, che si esprimono a favore di un ampliamento dei doveri di vigilanza e di educazione discendenti dalla responsabilità genitoriale[17]. L'educazione, arricchita della dimensione

sul Regolamento europeo, in ID., (diretto da), Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali, Bologna, 2017, p. 3 ss.

[13] A. MANTELERO, *Responsabilità e rischio nel Reg UE 2016/679*, in *Nuove Leggi civ. comm*., 2017, p. 148.

[14] L. BOZZI, *I dati del minore fra protezione e circolazione: per una lettura non retorica del fenomeno,* in *Europa dir.priv*., 2020, p. 251 ss. (in Banca dati de jure, p. 11).

[15] Al riguardo, a seguito di alcune drammatiche vicende di cronaca che hanno interessato la piattaforma Tik tok sono al vaglio diverse soluzioni per l'accertamento dell'età anagrafica: dal ricorso a strumenti di verifica in grado di salvaguardare l'anonimato in rete, all'impiego di sistemi di intelligenza artificiale, soluzione quest'ultima da considerare con cautela perché rischia di incrementare l'attività di profilazione dell'utente.

[16] B. AGOSTINELLI, *L'educazione della prole tra antiche prerogative genitoriali e nuovo interesse del minore*, in *Riv. dir. civ*., 2021, p. 180-181.

[17] Cfr. Tribunale Teramo 6 gennaio 2012; Tribunale Caltanissetta 8 ottobre 2019, dove in particolare si legge che "i genitori sono tenuti non solo ad impartire ai propri figli minori un'educazione consona alle proprie condizioni socio-economiche, ma anche ad adempiere a quell'attività di verifica e controllo sulla effettiva acquisizione di quei valori da parte del minore". E ancora: "Il dovere di vigilanza dei genitori deve sostanziarsi in una limitazione sia quantitativa che qualitativa di quell'accesso, al fine di evitare che quel potente mezzo fortemente relazionale e divulgativo possa essere utilizzato in modo non adeguato da parte del minore"; Cfr Tribunale Parma 5 agosto 2020 per il quale "i contenuti presenti sui telefoni cellulari dei minori andranno costantemente supervisionati da entrambi i genitori, evitando la comparsa di materiali non adatti all'età ed alla formazione educativa dei minori. La stessa regola vale per l'utilizzo eventuale del computer, al quale andranno applicati i necessari dispositivi di filtro.

digitale[18], assume certamente un ruolo prioritario. Di qui l'importanza di investimenti e programmi, sollecitati dall'Unione europea, orientati a promuovere l'alfabetizzazione digitale e a formare e a fornire supporto ai diversi attori educativi (famiglia, scuola e servizi socio-educativi di sostegno genitoriale).

Nondimeno, l'edificazione di uno spazio digitale inclusivo, ma sicuro, non può prescindere da un controllo dall'interno, *by design*, sulle architetture della rete e sulle funzionalità tecnologiche degli spazi di comunicazione[19]. Le aziende del settore tecnologico devono ricorrere ad un più rigoroso impiego della "tecnologia conformata"[20] in grado di prevenire già a livello tecnico i comportamenti vietati o comunque privando di offensività una tecnologia potenzialmente lesiva[21]. Il GDPR, nella prospettiva di prediligere la tutela preventiva, ha seguito l'approccio *risk-based* fondato sul cd. principio di *accountabilty*[22], il quale impone al titolare (e al responsabile) del trattamento l'adozione di misure protettive (tecniche e organizzative) in grado di garantire la riservatezza dell'utente finale e dei suoi dati personali fin dalla fase della progettazione dei prodotti e dei servizi (*privacy by design*). Il medesimo approccio, basato sulla necessità di limitare i rischi determinati dalle nuove tecnologie, assicurando un livello elevato di protezione dei diritti fondamentali, caratterizza inoltre la strategia europea per lo sviluppo dell'intelligenza artificiale[23], ma risulta ancora più evidente

---

[18] A. THIENE, *Gioventù bruciata on line: quale responsabilità per i genitori?,* in A. ANNONI, A THIENE (a cura di), *Minori e* privacy. *La tutela del dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Jovene editore, Napoli, p. 52 ss.

[19] E.MAESTRI, *L'identità perduta, Internet of things, smart devices e privacy dei minori sul web*, in A. ANNONI, A THIENE (a cura di), *Minori e* privacy, cit., p. 32.

[20] A. MANTELERO, *Regole tecniche e regole giuridiche: interazioni e sinergie nella disciplina di internet*, in *Contr. impr.*, 2005, p. 672.

[21] A. SANTOSUOSSO, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto,* Milano, 2020, p. 189.

[22] R. CARLEO, *Il principio di* accountability *nel GDPR: dalla regola alla auto-regolazione*, in *Nuovo dir.civ.*, 2021, p. 359.

[23] Nell'ambito delle misure normative destinate ad affrontare i problemi posti dallo sviluppo e dall'utilizzo dell'Intelligenza Artificiale si segnala in particolare la proposta di Regolamento per la introduzione di regole armonizzate sull'intelligenza artificiale elaborata dalla Commissione e sottoposta al Parlamento e al Consiglio il 21 aprile 2021 [COM (2021) 206 final] (*Intelligence Artificial Act*). L'obiettivo principale della proposta è di assicurare il buon funzionamento del mercato interno fissando regole armonizzate, in relazione allo sviluppo, all'immissione sul mercato dell'Unione e all'utilizzo di prodotti e servizi che ricorrono a tecnologie di intelligenza artificiale nel rispetto dei diritti fondamentali.

nell'ambito della strategia europea per il mercato unico digitale. Nella recentissima "legge sui servizi digitali" (*Digital Services Act*)[24] si prevedono infatti nuovi obblighi per i gestori delle piattaforme digitali e in particolare di quelle di dimensioni molto grandi, nonché nuove misure volte a garantire maggiore trasparenza dei sistemi algoritmici e delle tecniche di comunicazione commerciale. Proprio con riguardo alle nuove forme di comunicazione commerciale l'interesse del minore, e in generale delle persone vulnerabili, riceve una più incisiva considerazione in ragione dell'acquisita consapevolezza delle potenzialità lesive delle strategie di *design* persuasivo, correlate allo sviluppo delle nuove tecnologie, orientate ad attrarre in misura crescente l'attenzione dell'utente.

5.3. Profilazione e pubblicità personalizzata

Le attuali forme di comunicazione commerciale, realizzate nell'ambiente *on line*, grazie al meccanismo della profilazione[25] e al costante sviluppo degli algoritmi analitici e predittivi, consentono di realizzare pubblicità sempre più efficaci, in quanto personalizzate e mirate, ben distanti dalle tradizionali tecniche pubblicitarie, rivolte in modo indifferenziato ad una platea molto ampia di destinatari[26]. Tali nuove forme di pubblicità, benché foriere di indubbi vantaggi per le imprese, nonché per i consumatori, che vedono ridotto il tempo dedicato alla ricerca dei prodotti o dei servizi rispondenti alle proprie preferenze e standard, possono in realtà incidere sulla vita privata, sulla libertà di pensiero e di scelta delle persone, sulla democrazia, nonché agevolare la manipolazione e la discriminazione[27]. Si pensi, per esempio, al rischio

[24] Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

[25] Per «profilazione» si intende "una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona" (definizione contenuta nel Considerando 71 del GDPR).

[26] G. Proietti, *La pubblicità nell'era delle nuove tecnologie*, in G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020 p. 162.

[27] A.Jabłonowska, Maciej Kuziemski, A M., Nowak, H.W. Micklitz, P. Pałka, G. Sartor, *Consumer law and artificial intelligence Challenges to the EU consumer law and*

al quale è esposto il consumatore di subire una "discriminazione di prezzo"[28]- che si ottiene praticando un prezzo diverso a ciascun consumatore in base alla "disponibilità a pagare" di ciascun utente inferita dalla estrapolazione dei suoi stessi dati personali - oppure al rischio, in generale per l'utente profilato, di rimanere chiuso in una "gabbia costruita da altri"[29], anche definita "bolla"[30], in quanto destinatario di messaggi pubblicitari esclusivamente conformi ai gusti e agli interessi presuntivamente ricavati durante l'attività *on line*. Tali tecniche, inoltre, si rivelano ancor più insidiose ed efficaci quando sono rivolte ai minori di età, i quali sono meno in grado, rispetto agli adulti, di comprenderne i rischi, ma non per questo meno incoraggiati ad esplorare e a sperimentare la loro identità nell'ecosistema digitale[31]. Dal gioco interattivo alla visualizzazione di un video o dal semplice uso di *smart toys* o di altri dispositivi IoT (*Internet of Things*), le aziende sono in grado di inferire informazioni, anche sensibili, preziosissime che non si limitano alle sole caratteristiche, abitudini e preferenze dell'utente, ma includono anche le sue condizioni di salute, le sue abilità cognitive, i suoi stati d'animo, le sue vulnerabilità, consentendo quindi, grazie alle tecniche analitiche e predittive, la realizzazione di profili accurati relativi ai singoli consumatori, verso i quali indirizzare pubblicità mirate e personalizzate, servendosi, peraltro, di tecniche particolarmente persuasive, come l'*influencer marketing* e la pubblicità c.d. gamificata[32] al fine di orientarne i comportamenti. Ne discende una considerevole limitazione della libertà di autodeterminazione dell'utente minorenne in grado di estendersi ben oltre la sfera economica e che né lo strumento del consenso, né la trasparenza formale del trattamento dei dati sono, in ogni caso, in grado di escludere.

---

policy stemming from the business' use of artificial intelligence, EUI Working Paper LAW 2018/11, p. 48.

[28] R. MONTINARO, *Il consumatore nei mercati online: la disciplina del commercio elettronico e delle pratiche commerciali scorrette alla prova dell'evoluzione tecnologica,* in A. CATRICALÀ, M.P. PIGNALOSA (a cura di), *Saggi di diritto dei consumi,* Torino, 2020, p. 106.

[29] S. RODOTÀ, *Il diritto di avere diritti*, Laterza & Figli, Roma-Bari, 2012, p. 304.

[30] M. BIANCA, *La* filter bubble *e il problema dell'identità digitale*, in *Media Laws*, 2019, p. 1 ss.

[31] D. LUPTON, B. WILLIAMSON , *The Datafied Child: The Dataveillance of Children and Implications For Their Rights'*, in *New Media and Society*, Vol 19, Issue 5, 2017, pp. 780 ss.

[32] Forma particolare di pubblicità che grazie al sistema premiale (punti, livelli da raggiungere, ricompense) è in grado di orientare ancora più facilmente il comportamento degli utenti.

5.4. La profilazione dei minori ai fini di marketing nel Regolamento (UE) 2016/679

Nel Regolamento (UE) 2016/679 non è previsto un divieto assoluto di profilare i minori ai fini commerciali, come riconosciuto anche nelle Linee guida del Gruppo di Lavoro "Articolo 29" (oggi sostituito dall'*European Data Protection Board*). Benché dai considerando 38 e 71 del GDPR si evinca l'intenzione di escludere i minori dalla profilazione, in quanto possono essere "meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate, nonché dei loro diritti in relazione al trattamento dei dati personali" l'art. 22, che prevede una importante limitazione riguardo la profilazione in generale, nel consentire, in via eccezionale, le decisioni automatizzate e le profilazioni in determinati casi non distingue tra soggetti adulti e soggetti minori, lasciando quindi intendere la liceità delle decisioni automatizzate e delle profilazioni "autorizzate", se basate sul consenso dell'interessato. Il consenso che, ai sensi dell'art. 2-*quinquies* del Codice della *Privacy*[33] e art. 8 del GDPR, è legittimamente prestato, in autonomia, dal minore quattordicenne per accedere ai servizi della società dell'informazione, dovrebbe dunque autorizzare l'operatore, titolare del trattamento, ad utilizzare i relativi dati personali anche ai fini commerciali. Nelle medesime Linee guida si raccomanda tuttavia agli operatori, in generale, di astenersi dal profilare i minori per finalità di marketing, in quanto ritenuti particolarmente "vulnerabili nell'ambiente *online* e più facilmente influenzabili dalla pubblicità comportamentale" e, attraverso il richiamo all'art. 40 del Regolamento, si invitano gli Stati membri a recepire tali indicazioni nell'ambito dell'autoregolazione. Nella prospettiva del Regolamento dunque l'effettività della tutela dei minori nei confronti delle tecniche di marketing diretto, basate sulla profilazione, appare esclusivamente affidata all'adozione in concreto dei codici di condotta, nonché alla possibilità di sanzionare la violazione degli impegni volontariamente assunti[34].

[33] Come modificato dal D.Lgs. n. 101/2018.

[34] F. Di Porto, *La libertà di espressione del minore e il diritto all'accesso ai mezzi di comunicazione e alla riservatezza*, in nel volume a cura dell'Autorità Garante per l'Infanzia e l'Adolescenza, *La Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza. Conquiste e prospettive a 30 anni dall'adozione*, 2019, p. 237.

5.5. Il divieto della pubblicità mirata e comportamentale ai minori nella nuova strategia dell'UE per il mercato unico digitale

La finalità di tutelare le persone vulnerabili dalle nuove forme di comunicazione commerciale appare più chiaramente delineata nell'ambito della nuova strategia europea per il mercato unico digitale. Nella Direttiva UE/2018/1808 sui servizi media audiovisivi[35] è previsto espressamente che "i dati personali dei minori raccolti o altrimenti generati dai fornitori di servizi di media a norma del paragrafo 1 non sono trattati a fini commerciali, quali *marketing* diretto, profilazione e pubblicità mirata sulla base dei comportamenti" rilevati. Tale previsione è stata quindi recepita nell'art. 36 del Testo unico dei servizi di media audiovisivi e radiofonici, come modificato dal D.Lgs. 8 novembre 2021, n. 208. Analogo divieto è altresì contenuto nel *Digital Services Act* (DSA). L'art. 28 del DSA, dopo aver specificato che i fornitori delle piattaforme online accessibili ai minori debbano mettere in atto misure adeguate e proporzionate per garantire un elevato livello di privacy, sicurezza e protezione dei minori (1° paragrafo), fa agli stessi divieto "di presentare sulla loro interfaccia pubblicità basata sulla profilazione come definita all'articolo 4, punto 4), del regolamento (UE) 2016/679 che usa i dati personali del destinatario del servizio se sono consapevoli, con ragionevole certezza, che il destinatario del servizio è minore" (2° paragrafo). Coerentemente con tale disposizione è fatto altresì divieto ai fornitori delle piattaforme online di progettare, organizzare o gestire le loro interfacce online in modo tale da ingannare o manipolare (in generale tutti) i destinatari dei loro servizi o da distorcere o compromettere la capacità degli stessi di prendere decisioni libere e informate (art. 25 e cons. 67 del DSA)

Si evince la finalità del legislatore europeo di garantire la libertà di autodeterminazione dell'utente tutelata a prescindere dal rilascio del consenso, nonché dalla necessità che la pratica sia idonea a determinare un danno fisico o psicologico. Sotto questo profilo, la normativa

[35] La Direttiva 2018/1808/UE modifica la direttiva 2010/13/UE estendendo le regole previste nell'ambito delle comunicazioni audiovisive tradizionali alle piattaforme *on demand* e di condivisione dei video, prevede in capo ai fornitori di media digitali l'obbligo di adottare misure idonee per tutelare i minori in relazione a programmi, video (generati dagli utenti) e comunicazioni commerciali che possano nuocere al loro sviluppo fisico, mentale o morale.

risulta più garantista, rispetto a quanto previsto nell'art. 5 (paragrafo 1) della proposta di Regolamento sull'Intelligenza artificiale, pubblicata dalla Commissione europea il 21 aprile 2021 (*Artificial Intelligence Act*), nella misura in cui le due discipline possano concorrere nell'applicazione concreta. In quest'ultima disposizione infatti, nel disporre il divieto di usare sistemi di IA che utilizzano tecniche subliminali per distorcere il comportamento della persona, senza che la stessa ne sia consapevole o che sfruttano "una qualsiasi vulnerabilità di un gruppo specifico di persone a causa della loro età, disabilità o specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di una persona appartenente a tale gruppo" si specifica che tali impieghi siano idonei a provocare, o a provocare con ragionevole probabilità, un danno fisico o psicologico alla persona[36]. Il divieto formulato nel DSA sembra operare indipendentemente sia dalla consapevolezza che ne abbia l'utente (e quindi dal rilascio del consenso), sia dalla necessità che la pratica sia idonea a determinare un danno fisico o psicologico.

Nel considerando 89 è fatto inoltre espresso richiamo al "best interest of the child" che, in particolare, i fornitori di piattaforme digitali (e i motori di ricerca) di grandi dimensione devono tenere sempre presente nell'adattamento del *design* dei loro servizi e interfacce online, soprattutto quando i servizi sono rivolti ai minori o sono utilizzati prevalentemente da questi ultimi. Sotto tale profilo quindi il regolamento sui servizi digitali recepisce le indicazioni contenute nel *General Comment* n. 25, del 2 marzo 2021, del Comitato Onu alla Convenzione di New York del 1989 sui diritti dell'infanzia e dell'adolescenza, che indica come i diritti dei minori, affermati nella Convenzione, debbano essere applicati nell'ambiente digitale. In questo documento, infatti, si fa riferimento ai rischi che sorgono in relazione alle nuove forme di pubblicità commerciale e alle strategie di *design* persuasivo correlate ai prodotti e ai servizi digitali. Si legge, in particolare, come gli Stati parte dovrebbero garantire che le imprese non si rivolgano ai minorenni "utilizzando tecniche progettate per dare priorità agli interessi commerciali rispetto a quelli del minore". Monito che troviamo in senso analogo espresso anche nel considerando 83 e nell'art. 34 del DSA, laddove si richiede agli operatori digitali di compiere la valutazione

[36] Sui limiti della portata della disposizione cfr. M.VEALE, F. Z. BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 2021, p. 99.

d'impatto anche dei rischi sistemici che possono sorgere, in relazione alla progettazione di interfacce online che sfruttano, intenzionalmente o meno, le debolezze e l'inesperienza dei minori o che possono causare comportamenti di dipendenza e in generale qualsiasi effetto negativo concreto o prevedibile sulla tutela della salute pubblica e dei minori, nonché sul benessere fisico e mentale della persona.

In effetti i prodotti e i servizi tecnologici appaiono progettati e programmati per attirare in modo crescente l'attenzione degli utenti, orientandoli verso comportamenti che possono incidere significativamente sul loro stato di salute, fisico e mentale[37]. La "dipendenza da Internet" [38] è ormai scientificamente riconosciuta e definita come una patologia, un disturbo ossessivo/compulsivo, che spinge una persona ad un uso eccessivo dello strumento tecnologico e comprende una grande varietà di comportamenti e problemi di controllo degli impulsi[39]. Nondimeno, occorre evidenziare come il modello di analisi del rischio accolto nel DSA appare più aperto ed evoluto rispetto a quello accolto nel GDPR[40], in quanto in grado di prendere in considerazione sia le implicazioni negative (effettive e) "prevedibili" (che potrebbero verificarsi – ma anche non verificarsi - nel medio lungo periodo), sia le conseguenze etico-sociali (di natura quindi collettiva e non solo individuale) riconducibili all'uso di certe nuove tecnologie, anche a

[37]Peraltro, la pandemia da Covid-19, avendo prolungato il tempo di esposizione dei bambini e degli adolescenti agli schermi, ha acuito tali fenomeni, ma, allo stesso tempo, ha maggiormente sensibilizzato la comunità scientifica nell'approfondire l'impatto delle tecnologie sul benessere dei soggetti minori di età e nel diffonderne i relativi risultati.

[38]Termine coniato dal medico Ivan Golberg nel 1995, che propose di introdurre la sindrome "*Internet Addiction Disorder*" (IAD) nel Manuale diagnostico e statico dei disturbi mentali DSM, per la forte analogia dei segni e sintomi al gioco d'azzardo patologico.

[39]Alle forme più gravi di dipendenza, quale la sindrome di *Hikikomori* (che porta i giovani ad isolarsi e ad abbandonare gli studi e la frequentazione di amici), si affiancano una serie di stati emotivi (es. la c.d. "Fear of missing out" (FoMO), con cui si indica la preoccupazione ossessiva di perdere un evento postato on line, o comunque di essere "essere tagliati fuori" dalle esperienze vissute dagli amici; la "no mobile phone fobia", ossia la paura di rimanere senza il proprio cellulare da cui può derivare uno stato di ansia molto forte) che inducono l'utente a comportamenti compulsivi, quali il controllo ossessivo del proprio smartphone, che nel tempo possono dare luogo a dipendenza. Cfr. M. D. GRIFFITHS, D. J. KUSS, *Adolescent social media addiction* (revisited), in *Education and Health*, 2017, Vol. 35, n. 3, p. 49.

[40] Sui limiti del modello individualistico adottato nel GDPR si vedano le considerazioni di A. MANTELERO, *Responsabilità e rischio nel Reg UE 2016/679*, in *Nuove Leggi civ. comm.*, 2017, p. 164.

prescindere dal fatto che queste conseguenze producano un pregiudizio dei diritti e delle libertà fondamentali. Al fine di dare effettività a tale previsione, è inoltre sottolineata l'importanza del ricorso, nella valutazione e mitigazione dei rischi, ad adeguate forme di partecipazione dei soggetti destinatari dei servizi e dei gruppi potenzialmente impattati da tali servizi (cons. 90 del DSA) , attraverso il coinvolgimento dei loro rappresentanti , di esperti indipendenti e delle organizzazioni della società civile.

Sembra quindi, con riguardo all'impatto delle nuove tecnologie sui minori di età e in generale sui gruppi di persone vulnerabili, che vi siano le premesse verso una più incisiva regolamentazione, la quale, per la sua effettività dovrà essere comunque accompagnata da una autoregolazione, oltre che da un maggiore intervento delle autorità competenti.

6. Diritti fondamentali e ambienti digitali: prime note di una ricerca sul diritto a non essere sottoposto a una decisione interamente automatizzata

Daniele Imbruglia (Università di Roma La Sapienza)

"(…) *an algorithm – an opinion formalized in code*"
Cathy O'Neil

6.1. *Onlife*, la quarta rivoluzione

Uno dei più influenti filosofi contemporanei, Luciano Floridi, ha introdotto il termine 'on-life' per riferirsi a quelle attività, oggi largamente prevalenti nella vita quotidiana, che si collocano oltre la tradizionale distinzione tra *off-line* e *on-line*. Secondo la definizione offerta dal filosofo italiano, il termine starebbe ad indicare "*the new experience of a hyperconnected reality which it is no longer sensible to ask whether one may be online or offline*"[1]. Si pensi, ad esempio, alla guida di un veicolo secondo le istruzioni che si riceve dal proprio smartphone, alla visione di un film su una smart-tv, e via di seguito. In tutte queste situazioni è difficile, nonché certamente opinabile, rispondere alla domanda se la persona che guida o che guarda il film sia *off-line* oppure *on-line*.

Lo stesso filosofo descrive il più generale impatto delle attuali tecnologie dell'informazione della comunicazione in termini di rivoluzione, la quarta. Dopo quella copernicana che ci ha costretto a smettere

---

Questo articolo costituisce uno sviluppo della relazione tenuta dall'A. alla *Summer School* '*La responsabilità civile nell'era digitale*' del Dipartimento di Giurisprudenza dell'Università di Foggia dal 6 al 10 settembre 2021. Una versione ridotta del testo è pubblicato anche nel volume che raccoglie tutte le relazioni lì svolte, con il titolo *Diritti fondamentali e ambienti digitali. Appunti per una ricerca*. Un lavoro più definito è in corso.

[1] L. FLORIDI, *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Heidelberg – New York – Dordrecht – London, Springer, 2015, p. 1.

di credere alla centralità della terra nell'universo, quella darwiniana che ha smentito l'assunto per cui l'uomo sia al centro del regno biologico e quella freudiana che ha rotto la percezione della coscienza come di un luogo puro e trasparente, vi sarebbe ora una nuova rottura – appunto una quarta rivoluzione – che depone l'uomo "dalla posizione privilegiata ed esclusiva che avevamo nel regno del ragionamento logico, della capacità di processare informazioni per assolvere un determinato compito" [2].

Ancora. La quantità di attività che sino a qualche tempo fa era di esclusiva competenza dell'essere umano e che oggi è svolta da tecnologie informatiche è in continuo aumento. D'altronde, il vantaggio dell'utilizzo di tali tecniche è lampante. A parità di tempo, il numero di operazioni che si possono così svolgere è infinitamente maggiore rispetto a quello che un essere umano è in grado di processare. Non solo. Affidandosi a questi strumenti, la persona fisica in ipotesi preposta a quella attività potrebbe svolgere compiti diversi, meno ripetitivi e per i quali è necessaria la specifica capacità dell'uomo[3].

6.2. I diritti fondamentali in ambiente digitale

Rispetto a questo contesto in continua evoluzione, si deve registrare un profluvio di dichiarazioni che riconoscono e affermano il rispetto di certi diritti fondamentali in ambienti digitali[4]. Questi testi dimostrano come si stia affermando la consapevolezza circa l'esigenza di una regolazione[5] e che, onde evitare di trovarsi ancora una volta davanti a degli "*unforeseen disbenefits*"[6] dell'innovazione tecnologica, non

[2] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaele Cortina Editore, 2017, p. 105.

[3] Si pensi al passo di LEIBNIZ, citato in W. JORDAN, *Die Leibniz'sche Rechenmaschine*, in *Zeitschrift für Vertnesaungsweaen*, 1897, p. 307, per cui "*Indignum enim est excellentium virorum horas servili calculandi labore perire, qui Machina adhibita vilissimo cuique secure transcribi posset*".

[4] Con riferimento all'intelligenza artificiale, ad esempio, si veda il grafico disponibile in https://wilkins.law.harvard.edu/misc/PrincipledAI_FinalGraphic.jpg.

[5] In argomento, classici i riferimenti alla tesi di F.H. EASTERBROOK, *Cyberspace and the Law of the Horse*, in *Univ. Chi. Legal. Forum*, 1996, 207 e alle repliche di L. LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, in *Harv. Law Rev.*, 1999, p. 501 e, più di recente, R. CALO, *Robotics and the Lessons of Cyberlaw*, in *Cal. Law Rev.*, 2015, p. 513.

[6] M. KRANZBERG, *Technology and History: "Kranzberg's Laws"*, in *Techn. Cult.*, 1986, p. 548.

sia sufficiente un approccio in termini di etica[7]. Il mancato intervento del diritto o la sua articolazione secondo esigenze prettamente capitalistiche e di profitto può determinare un fallimento nell'assicurazione del benessere sociale[8] nonché una mancata tutela di posizioni giuridiche che pure sono al centro del nostro ordinamento e della nostra società (es. i diritti inviolabili della persona)[9].

Se è vero che si tratta di carte e dichiarazioni che, nella maggior parte dei casi, sono prive di valore giuridico, si deve osservare che tale carattere non ne giustifica una valutazione in termini di irrilevanza e insignificanza, come se questi sforzi non fossero che banali tentativi politici o di mera gestione del consenso. La storia, infatti, ha dimostrato a più riprese come "[p]er molti diritti, anche quelli ritenuti nell'attuale fase di evoluzione pacificamente "giustiziabili", l'approdo della difesa in giudizio non è stato quasi mai un dato originario, quanto piuttosto un punto di conquista, attraverso la progressiva crescita delle rivendicazioni sociali e della forza culturale che tali diritti sono riusciti col tempo ad esprimere"[10].

Oltre a rappresentare un importante tentativo di regolazione di un fenomeno in divenire, tali documenti si lasciano apprezzare perché non si esauriscono nella affermazione dei diritti fondamentali esistenti *off-line* anche negli ambienti digitali, ma al loro interno prevedono anche nuove situazioni giuridiche così innovando il catalogo dei diritti fondamentali, i quali, come noto, non vanno intesi come un qualcosa di fuori dalla storia e assoluto: "[a]nche i diritti dell'uomo sono diritti storici, che emergono gradualmente dalle lotte che l'uomo combatte per la propria emancipazione e dalla trasformazione delle condizioni di vita che queste lotte producono"[11].

Nel prosieguo di questo lavoro, intendo avanzare una possibile ricerca su tali diritti. Il contributo è diviso in due parti. Nei paragrafi immediatamente successivi darò brevemente conto di due recenti dichiarazioni così da rendere il lettore edotto del fenomeno *de qua*. La scelta dei documenti è dettata dal tempo: si tratta di alcuni dei testi più

[7] Per tutti, D. TAFANI, *What's wrong with "AI Ethics" narratives*, in *Boll. tel. fil. pol.*, 2022.

[8] Per tutti, U. PAGANO, *The crisis of intellectual monopoly capitalism*, in *Cambr. Jour. Econ.*, 2014, p. 1409.

[9] Per tutti, S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, Laterza, 2012, p. 374.

[10] Così, A. D'ALOIA, *Generazioni future* (*diritto costituzionale*)(voce), in *Enc. dir., Ann.* IX, 2016, p. 354.

[11] N. BOBBIO, *L'età dei diritti*, Torino, Einaudi, 2020, p. 57-58.

recenti di quell'ampio insieme di carte digitali ora richiamato[12]. Nella seconda parte del lavoro, invece, cercherò di verificare come nasce e si afferma un diritto fondamentale digitale, discutendo l'ipotesi di decisioni assunte mediante procedimenti automatizzati e dei principi che si stanno via via affermando nelle corti e nella legislazione con riferimento a detto fenomeno.

6.3. La Carta derechos digitales

Il 14 luglio 2021, il governo spagnolo ha presentato la *Carta derechos digitales* ('*Carta*'), un documento non normativo che afferma il valore della persona e della dignità umana nella definizione delle regole e delle politiche della nuova realtà digitale[13]. Redatto da un gruppo di esperti di discipline diverse, la *Carta* è il risultato di circa un anno di lavori e di due consultazioni pubbliche. Il testo si compone di ventotto disposizioni suddivise in sei sezioni e anticipate da un preambolo che dà conto delle ragioni dell'intervento, centrale nella c.d. *Plan España Digital 2025*.

La prima sezione della *Carta*, intitolata *Derechos de libertad*, si apre con il riferimento al rispetto negli ambienti digitali dei diritti fondamentali riconosciuti nelle diverse carte e dichiarazioni e prosegue con l'affermazione del diritto all'identità, alla protezione dei dati (con esplicito richiamo al regolamento europeo 2016/679, su cui *infra*) e al diritto all'utilizzo di uno pseudonimo. A tal proposito, la *Carta* prevede che tale pretesa possa essere limitata solo quando l'identificazione personale sia necessaria e che sia comunque possibile la identificazione dell'utente ove richiesto dalla autorità giudiziaria. La medesima sezione prevede poi che il ricorso a sistemi di analisi che impieghino decisioni automatizzate o la profilazione degli individui sia possibile solo quando ammesso dalla normativa nonché il diritto di tutte le persone a strumenti di sicurezza adeguati a un trattamento dei dati sicuro. La sezione si chiude demandando la disciplina del diritto all'eredità digitale (ossia di tutti i beni e e diritti che, nell'ambiente digitale, erano detenuti dalla persona deceduta) al legislatore.

---

[12] In tempi recenti, è altresì intervenuta la *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, adottata lo scorso 26 gennaio 2022 (Com (2022)28)e il cui testo è disponibile in https://eur-lex.europa.eu.

[13] Il testo della Carta è disponibile in https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf.

La sezione successiva, dal titolo di *Derechos de igualidad*, contiene cinque articoli. Oltre al diritto alla non discriminazione, al diritto all'accesso e al contrasto al divario digitale, la sezione prevede una ricca disposizione in merito alla protezione dei minori. Tale disciplina (art. X) si apre ponendo a carico dei soggetti responsabili (es. i genitori) il compito di assicurare un uso responsabile degli ambienti digitali per garantire il corretto sviluppo del minore. Tra le altre cose, l'articolo X prevede l'introduzione di procedure per la verifica dell'età, il diritto di ricevere una formazione e un'informazione adeguata alle capacità del minore e un generale divieto di trattamento dei dati personali dei minori a fini di profilazione.

La terza sezione della *Carta* contiene disposizioni in tema di partecipazione e di informazione tramite ambienti digitali. Essa si apre con il riferimento alla neutralità della rete Internet e prosegue poi affrontando il tema dell'informazione in ambiente digitale. In particolare, l'art. XV afferma il diritto a ricevere informazioni veritiere e conformi ai protocolli sulla trasparenza (in base ai quali comunicare se l'informazione è stata elaborata mediante processi automatizzati o se ha carattere pubblicitaria o meno). La sezione in parola si conclude con tre articoli che affermano il diritto della cittadinanza alla partecipazione per mezzi digitali, a ricevere una educazione digitale e ad avere rapporti digitali con la pubblica amministrazione.

La quarta e la quinta sezione affrontano precise tematiche degli ambienti digitali. In una, si offrono indicazioni relative al rispetto dei diritti fondamentali dei lavoratori (art. XIX) e alla libertà di impresa in un contesto concorrenziale (art. XX) e nell'altra si affermano articoli in materia di ricerca scientifica, diritto alla salute e all'attività artistica-culturale, nonché all'impiego di programmi di intelligenza artificiale o di neuro-tecnologie. In tale quinta sezione, rubricata *Derechos digitales en entornos e specificos*, la *Carta* fa riferimento anche alla necessità dello sviluppo tecnologico di rispettare la sostenibilità ambientale e le generazioni future. La *Carta* si conclude con una sesta sezione, *Garantias y eficacia*, che riconosce la tutela dei diritti fondamentali anche in ambiente digitale.

Il testo spagnolo ricorda la *Dichiarazione dei diritti in Internet*, approvata dalla Camera dei Deputati nazionale nel 2015 e che conteneva già diverse disposizioni analoghe a quelle ora affermate nella *Carta* (*e.g.* neutralità della rete, inviolabilità dei sistemi informatici, protezione

dell'anonimato)[14]. Questa parziale coincidenza conferma la diffusione di nuovi diritti fondamentali. Si pensi, ad esempio, al diritto all'utilizzo di uno pseudonimo o alla navigazione anonima. È evidente che un tale diritto non ha senso fuori dagli ambienti digitali, così come è chiaro che esso costituisce uno strumento e una tecnica che consentono la massima libertà di espressione e di pensiero. L'articolo 10 della *Dichiarazione dei diritti in Internet* è esplicito in tal senso, allorché afferma "Ogni persona può accedere alla rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure". Tutto quanto ora detto sui nuovi diritti fondamentali, ovviamente, non sorprende: "[c]erte richieste nascono, infatti, solo quando nascono certi bisogni e nuovi bisogni nascono in corrispondenza del mutamento delle condizioni della società"[15].

6.4. Il Blueprint for an AI Bill of Rights statunitense

Lo scorso ottobre l'amministrazione statunitense ha pubblicato un documento teso a "*making automated systems work for the American people*" e noto come *Blueprint for ana AI Bill of Rights*[16]. Il testo si compone di una introduzione e di cinque principi, ciascuno dei quali accompagnato da una descrizione e da un commento. L'aspirazione del documento è quella di fornire un kit, una bussola, in grado di orientare le future decisioni politiche in materia di "*automated system*". Con tale espressione il documento intende riferirsi a quei *software* che usano calcoli computazionali per determinare risultati idonei a rilevare rispetto alla vita di individui o di comunità.

---

[14] Il testo della *Dichiarazione dei diritti in internet* è disponibile in www.camera.it. Sul c.d. *digital constitutionalism*, si v. i ricchi lavori di E. CELESTE, *Digital constitutionalism: a new systematic theorisation*, in *Int. Rev. Law Comp. Techn.*, 2018, p. 76; T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. informaz. informat.*, 2020, p. 465; G. DE GREGORIO, *The rise of digital constitutionalism in the European Union*, in *Int. Jour. Const. Law,* 2021, p. 41. A conferma della diffusione descritta nel testo è, poi, il dato per cui molti dei temi toccati dal testo spagnolo e prima ancora da quello italiano si rinvengono anche nella citata e recente *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*.

[15] C. FARALLI, *Introduzione*, in EAD. (a cura di), *La storicità del diritto*, Torino, Giappichelli, 2018, p. 8.

[16] Il testo è disponibile in https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

Il primo principio intende proteggere l'utente da "*unsafe or ineffective systems*". A tal fine, esso prevede che questi software siano sviluppati con la consultazione di diverse partecipanti, così che tutti i rischi e i diversi potenziali impatti del sistema siano rappresentati. Detti sistemi, poi, devono essere sottoposti a numerose verifiche, volte all'identificazione e alla riduzione dei rischi e a un monitoraggio continuo. Oltre a questi doveri di controllo e di coinvolgimento di rappresentanti sociali, il principio in esame prevede anche il divieto di progettazione di sistemi automatizzati tesi (o con la possibilità ragionevolmente prevedibile) a mettere in pericolo la sicurezza dell'utente o di una certa comunità. Il principio suggerisce di eseguire una valutazione indipendente che confermi la sicurezza e l'efficacia del sistema, compresa la comunicazione delle misure adottate per mitigare i potenziali danni, e i cui risultati devono essere resi pubblici.

Il secondo principio afferma il fondamentale divieto di discriminazione algoritmica ("*algorithmic discrimination*"). Tale patologia si verifica allorché il software determina un trattamento diverso ingiustificato o a un impatto sfavorevole sulle persone in base a razza, colore, etnia, sesso, religione, età, origine nazionale, disabilità, stato di veterano, informazioni genetiche o qualsiasi altra classificazione protetta dalla legge. È interessante notare come nel vocabolo 'sesso' il commento al principio in esame ricomprenda anche gravidanza, parto e condizioni mediche correlate, identità di genere, stato intersessuale e orientamento sessuale. Il divieto di questo genere di discriminazione impone a tutti i soggetti coinvolti nella costruzione del prodotto *software* (i progettisti, gli sviluppatori e i distributori) di adottare misure proattive e continue. Tra queste misure è incluso l'uso di dati rappresentativi e la protezione contro i proxy per le caratteristiche demografiche, i test e la mitigazione delle disparità prima dell'implementazione e in corso, nonché l'adozione di una chiara supervisione organizzativa. Anche qui si suggerisce la predisposizione di una valutazione indipendente dell'impatto dell'algoritmo, che includa i risultati dei test di disparità e le informazioni sulla mitigazione, e che sia reso pubblico e facilmente fruibile.

Il terzo principio prevede il divieto di pratiche abusive di trattamento dei dati e il diritto alla piena autonomia sull'utilizzo dei dati personali. Al fine di proteggere l'utente da violazioni della privacy, il documento insiste sull'importanza di scelte progettuali ('by design') che garantiscano l'inclusione di tali protezioni per impostazione

predefinita, tra cui la garanzia che la raccolta dei dati sia conforme alle aspettative ragionevoli e che vengano raccolti solo i dati strettamente necessari per il contesto specifico. Ancora una volta, tale principio si rivolge *in primis* ai soggetti che implementano detti software, i quali dovrebbero richiedere l'autorizzazione dell'utente e rispettare le sue decisioni in merito alla raccolta, all'uso, all'accesso, al trasferimento e alla cancellazione dei suoi dati nei modi più appropriati e nella misura più ampia possibile. Laddove ciò non sia possibile, si prevede l'obbligo di utilizzo di garanzie alternative di privacy *by design*. Accanto a questo aspetto, il principio in esame prevede il divieto di impiego di meccanismi di progettazione e di esperienza utente che offuschino la scelta dell'utente o che lo gravino con impostazioni predefinite invasive della privacy. Il principio insiste altresì sulla raccolta del consenso dell'utente: si afferma che questo possa utilizzato solo per giustificare la raccolta dei dati nei casi in cui può essere dato in modo appropriato e significativo e che le richieste di consenso siano brevi, comprensibili e redatte in un linguaggio semplice. In critica alle attuali pratiche di difficile comprensione, il documento insiste sull'importanza di dare all'utente la possibilità di decidere in merito alla raccolta dei dati e al contesto specifico di utilizzo dei propri dati.

Il penultimo principio concerne il diritto a essere informati sull'impiego di un *software* automatizzato. Tale diritto impone ai progettisti, agli sviluppatori e ai distributori di sistemi automatizzati di fornire una documentazione in un linguaggio semplice e generalmente accessibile, che con descrizioni chiare spieghi il funzionamento generale del sistema e il ruolo svolto dall'automazione, avvisando sull'eventualità che tali sistemi automatizzati siano in uso. Inoltre, l'utente deve sapere come e perché un esito che lo riguarda è stato determinato da un *software* automatizzato, anche quando il sistema automatico non è l'unico elemento che determina l'esito. Anche in questo caso si suggerisce la previsione di rendere pubblici i rapporti che, in un linguaggio semplice, includono informazioni sintetiche e delle valutazioni sulla chiarezza e sulla qualità dell'avviso e delle spiegazioni.

Infine, l'ultimo principio afferma che ciascun utente dovrebbe essere in grado *i*) di rifiutare un procedimento basato sull'impiego di software automatizzanti e *ii*) di avere accesso a una persona umana in grado di valutare e risolvere rapidamente i problemi che incontrate. Oltre che nelle ipotesi previste dalla legge, questa facoltà di rifiuto a favore di un'alternativa umana andrà riconosciuta ogni qualvolta sia

opportuno il ricorso a una valutazione da parte di un essere umano. L'accesso a detta valutazione dovrebbe essere affidabile e accessibile. In alcuni settori più sensibili, gli stessi software automatizzati dovrebbero prevedere e incorporare la partecipazione di un essere umane almeno per le decisioni più rilevanti.

6.5. Come nasce un diritto fondamentale digitale? Il problema del *machine learning*

Come anticipato, intendo sviluppare la ricerca qui accennata discutendo sul come simili diritti – storicamente dati e quindi tipicamente digitali – sorgano e circolino. In questo contributo, mi concentrerò nell'analisi di quella straordinaria tecnologia rappresentata dai *software* di intelligenza artificiale[17] che fanno applicazione del *machine*

[17] Ad oggi, non esiste una definizione comune e pacifica di cosa sia l'intelligenza artificiale (AI; *artificial intelligence*, IA) (in tal senso, tra gli altri, A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *Nuova giur. civ. comm.*, 2012, 497 e A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *Riv. Biodir.*, 2019, p. 8). Un *report* dell'Unione Europea – *AI Watch Defining Artificial Intelligence* – del 2020 elenca oltre cinquanta definizioni, proposte da Stati, istituzioni internazionali, euro-unitarie, accademici e soggetti privati (*AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence*, Luxembourg, 2020, doi:10.2760/382730, JRC118163; il testo è disponibile in https://publications.jrc.ec.europa.eu/repository/handle/JRC118163), ma resta il dato che nessuna delle definizioni lì richiamate sia riuscita ad imporsi e permane una grande eterogeneità e distanza tra le varie concezioni dell'intelligenza artificiale: si è tuttora in una fase in cui è ancora difficile tracciare "*a bright-line distinction between what constitutes AI and what does not*" (NATIONAL SCIENCE AND TECHNOLOGY COUNCIL COMMITTEE, *Preparing for the future of Artificial Intelligence*, 2016, 7 (in www.whitehouse.gov). Ciò detto, si può qui richiamare la definizione proposta in *National Artificial Intelligence Initiative Act*, adottato dal Congresso degli Stati Uniti d'America e che è entrato in vigore il 1° gennaio 2021 che definisce l'*artificial intelligence* come «*a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to* (A) *perceive real and virtual environments;* (B) *abstract such perceptions into models through analysis in an automated manner; and* (C) *use model inference to formulate options for information or action*», nonché quella contenuta nella recente proposta di regolamento europeo che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione (COM/2021/206 final, AIA *proposal*) e che individua un «sistema di IA» nel *software* sviluppato con approcci di apprendimento automatico, basati sulla logica e sulla conoscenza nonché quelli statisitici, che possa, per un dato insieme di obiettivi definiti dall'uomo, generare *output*, come contenuti, previsioni, raccomandazioni o decisioni, che influenzano gli ambienti con cui interagiscono.

learning, così definito da Tom Mitchell «*A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E*»[18]. Per fare ciò, ritengo doveroso premettere una breve, non completa, imperfetta e certamente sommaria descrizione della tecnologia in esame.

6.5.1. Esempi di *machine learning*

Si pensi all'attività di riconoscimento di immagini e si prenda l'esempio di un cane. Sino a qualche tempo fa, l'unico modo per determinare se un'immagine raffigurasse quell'animale era sottoporla a una persona fisica che fosse in grado di verificare la presenza di un cane nella figura. Per comprendere come, generalmente, una persona acquista questa capacità si pensi a un genitore che passeggia con il figlio di pochi anni per la città e che, davanti a ciascun cane (*input*) incontrato per strada, si ferma ripetendo il nome dell'animale (etichetta) al figlio. In poco tempo, questi collega la parola all'animale, così da impararne il nome (cane) e quando ne vede un altro esemplare lo chiamerà correttamente (*output*). Orbene, mentre l'essere umano impara a riconoscere un cane vedendone un numero tutto sommato ristretto di esemplari, realizzare una tecnologia in grado di rilevare le immagini che raffigurano un cane richiede tecniche complesse[19].

---

[18] T. MITCHELL, *Machine Learning*, New York, McGraw-Hill,1997. Per una definizione più recente e, a parere di chi scrive, preferibile, si v. J.D. KELLEHER, B. MAC NAMEE, A. D'ARCY, *Fundamentals of Machine Learning for Predictive Data Analytics*, Cambr. (Mass.), 2020, p. 5, in base alla quale esso è da intendersi come un "*automated process that extracts patterns from data*". Il *machine learning* è un sotto-campo dell'intelligenza artificiale, che, a sua volta, è un sotto-campo delle scienze informatiche, insieme all'ingegneria del *software* e al calcolo distribuito.

[19] Come noto, l'origine della espressione intelligenza artificiale risale a uno studio condotto nel 1956 presso il *Dartmouth College* (New Hampshire, USA) e che, per l'appunto, intendeva procedere «*on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it*» (J. MCCARTHY, M.L. MINSKY, N. ROCHESTER, C.E. SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 1955, p. 1, (testo disponibile in http://raysolomonoff.com/dartmouth/boxa/dart564props.pdf)). A partire da questo obiettivo ambizioso si è così parlato di *artificial general intelligence* (AGI) e si è cercato di costruire una macchina che avesse una intelligenza cognitiva generale, paragonabile a quella dell'uomo, e che fosse in grado di svolgere tutto ciò che l'essere umano abitualmente compie. Nonostante gli ingenti investimenti che questa linea di ricerca ha ricevuto sino alla fine degli anni Ottanta del secolo scorso, i risultati attesi

Una prima strada è quella di scrivere una procedura di elaborazione dei dati (programma, *software*) inserendo tutte le istruzioni necessarie all'operazione immaginata (es. riconoscimento cane), tra cui la regola (algoritmo) di soluzione del problema (es. la definizione di cane). Così scritto, questo *software* (c.d. tradizionale) realizza la verifica dell'immagine tramite l'esecuzione degli ordini impartiti. Grazie alle attuali capacità di calcolo automatizzato, tale compito verrà svolto con modalità (velocità, precisione) inconcepibili per l'essere umano.

Una strada diversa è quella che impiega metodi di apprendimento automatico (*machine learning*). Come nel caso del *software* tradizionale, anche in questo caso, a partire da un dato che viene inserito (*input*), l'esecuzione di un algoritmo scritto in linguaggio di programmazione (*software*) restituisce un dato-risultato (*output*). A differenza di quella prima ipotesi, però, i *software* di intelligenza artificiale che fanno applicazione di *machine learning* non sono forniti dell'algoritmo, il quale verrà elaborato automaticamente (*process*) dai dati inseriti (*input*) e poi applicato. Mentre i *software* tradizionali restituiscono un *output* che è il risultato della esecuzione di ordini, funzioni e formule impartitigli dal programmatore, in quelli di *machine learning* l'*output* è il prodotto dall'esecuzione automatica dell'algoritmo elaborato automaticamente (*process*) da certi dati (*input*).

Si tornerà immediatamente sulla descrizione di questa tecnica di *machine learning*, ma è bene comprendere sin d'ora che si tratta di una modalità profondamente e assolutamente diversa di realizzare la tecnologia con cui assolvere il compito immaginato. Mentre il presupposto della prima opzione (*software* tradizionale) è la conoscenza e la scrittura di tutte le istruzioni necessarie all'operazione immaginata (es. riconoscimento cane) tra cui anche la regola (algoritmo) di soluzione del problema, nei *software* di intelligenza artificiale non è necessario scrivere tale conoscenza e ciò in quanto il programma è scritto in modo tale da consentire l'elaborazione automatica di una regola (algoritmo) di soluzione del problema e poi applicarla.

Per elaborare questa regola necessaria ad assolvere il compito (es. riconoscimento delle immagini raffiguranti un cane) si fornisce il programma di un c.d. *training data set*. In una prima ipotesi, i dati forniti

non sono stati raggiunti e a tutt'oggi siamo lontani dall'avere una *machine* in grado di emulare tutte le capacità proprie dell'intelligenza umana (e, *in primis*, l'apprendimento): in argomento, per tutti, S. DEHANE, *Apprendre!, Les talents du cerveau, le défi des machines*, Paris, Odile Jacob, 2018, p. 67.

per l'elaborazione del modello sono etichettati, ossia vi sono *input* con l'indicazione dell'*output* richiesto (= esempi di immagini raffiguranti un cane). A partire da questi dati etichettati (o, *rectius*, esempi delle risposte che si attendono), il *software* elabora una regola di riconoscimento idonea ad assolvere il compito rispetto ad immagini che presentano variabili diverse da quelle degli esempi forniti (perché raffigurano cani in ambienti differenti da quelli degli esempi oppure di una razza diversa). In una seconda ipotesi, i dati forniti per l'elaborazione del modello non sono etichettati e il programma è rifornito dei soli *input*. Rispetto a questo *training data set* non etichettato, l'algoritmo elaborerà (*data mining*), ora per assimilazione, ora per riduzione, etc., un modello idoneo ad assolvere il compito rispetto ad immagini che non erano parte del *training data set* e che presentano variabili diverse da quelle degli esempi forniti (perché raffigurano cani in ambienti differenti da quelli degli esempi oppure di una razza diversa).

In entrambi i casi (dati etichettati e dati non etichettati) e una volta elaborato il modello a partire dai *training data set*, questo viene sottoposto a una verifica di affidabilità. Per fare ciò, si ricorre ad un altro *set* di dati, c.d. *test data set*, e si verifica se la risposta (l'algoritmo, la regola, il *pattern*, il modello) elaborata dal programma conduce ad *output* corretti. In caso di corrispondenza, si può dire che la regola di riconoscimento costruita dal *software* sia efficiente nell'assolvere il compito datogli.

6.5.2. Approcci di *machine learning*

A partire da questa ipotesi relativa all'utilizzo di un programma di riconoscimento immagini per identificare le figure che raffigurano un cane, si possono avanzare delle prime elementari definizioni dei metodi di apprendimento automatico (*machine learning*), c.d. *supervised* (dati etichettati) e *unsupervised* (dati non etichettati).

L'apprendimento automatico supervisionato (*supervised learning*) è un *software* che elabora in via automatica una regola (algoritmo, modello, *pattern*) a partire da esempi (*input* e *output*) forniti da un supervisore che ha il compito di guidare il *software* verso la definizione del criterio (algoritmo) idoneo all'adempimento del compito prefissato.

L'*output* può essere sia un valore numerico (regressione lineare), sia una classe o una categoria (classificazione). Un esempio del primo tipo è un *software* di valutazione di immobili. Si parte da un insieme di dati

relativi a immobili (dimensioni, caratteristiche, servizi, piano, localizzazione, etc.) e dai prezzi delle vendite (che costituiscono le c.d. etichette). A partire da questi dati etichettati, si ricava un algoritmo di apprendimento automatico supervisionato che, sulla base dei dati relativi alle vendite precedenti, è in grado di indicare un valore numerico (prezzo) per una casa nuova (non etichettata). Un esempio di *software* di apprendimento automatico supervisionato il cui *output* è una categoria (classificazione) è, invece, un programma *antispam*. Si parte da un insieme di *e-mails* e si etichettano come *spam* quelle indesiderate e come *no spam* quelle di un qualche interesse. A partire da questi dati etichettati, si ricava un algoritmo di apprendimento automatico supervisionato che, sulla base delle *e-mails* precedenti, è in grado di classificare il nuovo messaggio come *spam* o meno. Un classificatore molto importante è il c.d. *Nearest Neighbor*. A partire dai dati etichettati, il *software* costruisce due o più categorie o classi, così che poi considererà il dato da valutare come appartenente alla categoria con cui presenta le maggiori affinità (così, ad esempio, all'utente di una piattaforma *video on demand* che ha appena finito di vedere un certo film verrà suggerita la pellicola che piace ad altri *users* che hanno già visto quel primo film).

Per contro, l'apprendimento automatico non supervisionato (*unsupervised learning*) è quello in cui un programma è fornito unicamente degli *input* e dovrà elaborare una regola senza avere a disposizione gli *output* corretti. A partire dai dati disponibili, il *software* cerca delle regolarità, delle somiglianze o delle semplificazioni che consentano l'elaborazione automatica di un algoritmo da impiegare per svolgere il compito prefissato. Anche l'apprendimento automatico non supervisionato può essere impiegato per assegnare a ogni nuovo *input* un valore numerico (regressione lineare) o una categoria (classificazione). Oggi, esso è utilizzato, *inter alia*, per raccomandazioni e suggerimenti commerciali. Questi suggerimenti sono determinati dal *pattern* che il *software* ha, automaticamente, rilevato mediante l'analisi dei dati disponibili relativi, ad esempio, agli altri clienti o utenti. I principali approcci di apprendimento automatico non supervisionato sono quelli del *clustering* e dell'associazione. Nel primo caso, il *software* elabora una regola con cui raggruppare i dati secondo le proprietà che questi presentano. Nel secondo approccio, associazione, il programma ricava dai dati degli schemi che si ripetono, delle correlazioni o altri collegamenti che possono fornire una regola. Il vantaggio del ricorso a questo

tipo di metodo è duplice. Per un verso non è necessario avere dei dati etichettati (la cui formazione è necessariamente più lunga) e, per altro verso, dall'osservazione del *software* è possibile comprendere nuovi *pattern* e correlazioni inedite. Il rischio nell'utilizzo di questo tipo di apprendimento automatico *unsupervised* è non meno evidente ed è rappresentato dalla circostanza che, in assenza di etichette, l'affidabilità del modello elaborato automaticamente dal *software* può risultare meno alta e richiedere più dati.

Come è intuibile, i metodi di *machine learning* sono numerosi e spesso si combinano tra di loro. Si pensi al c.d. *semi-supervised learning*, che costituisce uno dei metodi oggi più utilizzati. In tale ipotesi, il *software* è rifornito di *input* solo parzialmente etichettati. Processando questi dati misti (etichettati e non etichettati), il programma elabora automaticamente un algoritmo in grado di valutare un nuovo dato e fornire un certo *output*. Ancora, in tempi recenti si è introdotto un ulteriore metodo c.d. *self-supervised learning*, molto promettente perché consente di svolgere compiti di apprendimento supervisionato (classificazione o regressione lineare), senza avere come *input* dati etichettati dall'uomo, la cui raccolta è necessariamente parziale, lenta, dispendiosa e costosa in termini di risorse. In tale metodo, il *software* riceve dati non etichettati e, per così dire, li etichetta automaticamente, ricercando correlazioni e osservando i dati visibili per ricostruire ciò che manca oppure delle strutture implicite. Svolta questa prima operazione ancillare (*pretext task*), il *software* utilizzerà la rappresentazione elaborata dai dati di *input* per svolgere compiti (*text task* o *downstream task*) di classificazione o di regressione lineare (es. riconoscimento oggetto di cui non era stato fornito esempio). In tempi recenti, diversi *social networks* hanno utilizzato questo metodo per elaborare *software* di *speech recognition* e, più in generale, il *self-supervised learning* è impiegato nel contesto dei programmi di comprensione del linguaggio naturale (*natural language processing*, NLP)[20].

Oltre ai metodi richiamati *supra*, si trova, poi, quello c.d. rinforzato (*reinforcement learning*), che si distingue dai precedenti per la fase di *input*. Al posto di dati da cui estrapolare un modello con cui assolvere il proprio compito, infatti, il programma riceve come *input* un obiettivo da raggiungere (es. non scottarsi al sole). A partire dall'osservazione dell'ambiente (sole\nuvoloso), il *software* assume una decisione

[20] Sul tema, si veda il contributo di S. ORLANDO, *Linguaggi di programmazione e responsabilità*, in questo Annuario (cap. 11).

(prendere\non prendere la crema di protezione) che riceve un *feedback* positivo (ricompensa) o negativo (penalità) a seconda del successo della decisione assunta rispetto all'obiettivo dato. Considerato che il *software* ha per scopo la massimizzazione del rinforzo, il programma ripeterà nel tempo le decisioni che hanno un *feedback* positivo (sole\crema). Questa modalità di apprendimento automatico è impiegata, ad esempio, nelle *self-driving cars*.

Peraltro, occorre tenere a mente che il *machine learning* è in continua evoluzione. Se i metodi di *supervised learning* e *unsupervised learning* costituiscono metodi classici di *machine learning*, a partire dagli anni Dieci del secolo attuale si è affermato il c.d. *deep learning*, che costituisce una tecnica di apprendimento automatico che utilizza livelli multipli (reti neurali) per elaborare progressivamente caratteristiche di livello superiore dall'*input* iniziale e così individuare in modo ancora più efficace possibili *pattern* da utilizzare come algoritmi. Oltre che nei menzionati *software* di NLP e in genere di *self-supervised learning*, un esempio molto discusso di rete neurale è la c.d. rete generativa avversaria (*Generative Adversarial Network*, GAN), dove un algoritmo genera e l'altro controlla fino a non rendere possibile per il controllore fare distinzioni tra i diversi risultati[21].

In pressoché tutti questi metodi, i dati disponibili (*input*) sono trattati (*process*) in modo tale da elaborare automaticamente un algoritmo che restituisce un certo risultato (*output*), variamente usato. Questo meccanismo (*Input*, *Process*, *Output*, c.d. *IPO model*) si sviluppa in modo diverso: nel *supervised learning*, ad esempio, il *software* è fornito di *input* e di *output*, mentre in quello *unsupervised* dei soli dati di *input*. Ciò che qui rileva, però, è la comprensione del *machine learning* come di un programma (*software*) che, a partire dai dati disponibili (*input*), elabora automaticamente (*process*) un algoritmo (modello, *pattern*, regola) la cui esecuzione, anche essa automatica, restituisce un certo dato-risultato (*output*). L'elaborazione automatica (apprendimento) dell'algoritmo la cui esecuzione restituisce un certo dato-risultato (*output*) è *data-based-inference* e risponde ai metodi della statistica (che, come visto, passano dalla semplice regressione lineare alle complesse reti neurali).

[21] Esempi impressionanti si rinvengono nel campo della generazione di immagini (c.d. *deep fake*): per tutti, si v. T. Karras, T. Aila, S. Laine, J. Lehtinen, *Progressive Growing of GANs for Improved Quality, Stability, and Variation*, in ICLR, 2018, (disponibile in https://arxiv.org/abs/1710.10196).

6.6. Il *software* di *machine learning* e il diritto: dalla personalità elettronica alle presunzioni

Nella elaborazione automatica di una regola di soluzione (algoritmo) la cui esecuzione automatica restituisce un *output* risiede l'elemento di forza dei *software* di intelligenza artificiale, ossia quella tecnologia che consente il processo automatico (e quindi in modalità inconcepibili per l'uomo per ciò che riguarda la velocità e la precisione) di certe operazioni anche senza disporre in partenza delle istruzioni necessarie (algoritmo) per lo svolgimento automatizzato del compito. Si è tante volte osservato che l'impiego di tale specifica capacità dei *software* di *machine learning* presenti dei rischi, non indifferenti, per la società e ciò, in particolare, allorché di essi se ne fa utilizzo predittivo rispetto a questioni sensibili[22]. Orbene, il necessario inquadramento giuridico di questa specifica capacità del *software* di intelligenza artificiale di elaborare automaticamente l'algoritmo (*pattern recognition*) da applicare al problema non è agevole.

Un primo orientamento ha spinto la discussione verso i concetti della «autonomia» e della «personalità elettronica»[23]. Addirittura, qualche anno fa il Parlamento dell'Unione Europea ha approvato una

---

[22] Letture già divenute classiche: E. PARISER, *The Filter Bubble: What The Internet Is Hiding From You*, New York, 2011; R. MACKINNON, *Consent of the networked: the worldwide struggle for Internet freedom*, New York, 2013; C. O'NEIL, *Weapons of math destruction: How big data increases inequality and threatens democracy*, New York, 2016; S. BAROCAS e A.D. SELBST, *Big Data's Disparate Impact*, in *Calif. Law Rev.*, 2016, p. 671; V. EUBANKS, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York, 2018; S. LEONELLI, *op. cit.*, p. 43; S.U. NOBLE, *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York, 2018; J. BRIDLE, *Nuova era oscura* (trad. it.), Roma, 2019; S. ZUBOFF, *op. cit.*; T. GEBRU, *Race and Gender*, in M.D. DUBBER, F. PASQUALE, S. DAS (eds), *Oxford Handbook of Ethics of AI,* Oxford, 2020, p. 253; K. CRAWFORD, *Né intelligente né artificiale. Il lato oscuro dell'IA* (trad. it.), Bologna, 2021; T. NUMERICO, *Big Data e algoritmi*, cit., p. 91 e p. 217.

[23] Si veda, in particolare, C. LEROUX – R. LABRUTO (eds), *Suggestion for a green paper on legal issues in robotics*, 2012, disponibile in www.unipv-lawtech.eu. Già all'inizio degli anni Novanta del secolo scorso, in un contesto in cui la maggioranza delle macchine era priva di connessione a internet, si era avanzata l'idea di attribuire di diritti e doveri a tali *software* e considerarli come persone (L.B. SOLUM, *Legal Personhood for Artificial Intelligences*, in *North Carol. L. Rev.*, 1992, p. 1231). In tempi recenti, S. BAYERN, *The Implications of Modern Business-Entity Law fot the Regulation of Autonomous Systems*, in *Stan. Tech. Law Rev.*, 2015, p. 93 afferma la possibilità di riconoscere "*effective legal personhood for nonhuman systems without wide-ranging legal reform and without resolving, as a precondition, any philosophical questions concerning the mind, personhood, or capabilities of nonhuman systems*".

risoluzione in cui invitava a valutare l'ipotesi dell'istituzione di «uno *status* giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi»[24]. Sulla falsa riga di uno studio di poco precedente[25], con tale formula ("*electronic personhood*") quella risoluzione intendeva così affrontare e risolvere il rischio di c.d. *liability gap*, ossia di carenze in materia di responsabilità rispetto a robot autonomi, i quali non potrebbero essere "considerati come meri strumenti nelle mani di altri", in quanto dotati della "capacità di prendere decisioni e metterle in atto nel mondo esterno, indipendentemente da un controllo o un'influenza esterna"[26]. Se, da un lato, tale capacità – definita come "autonomia" – dei robot li renderebbe "simili ad agenti che interagiscono con l'ambiente circostante e sono in grado di alterarlo in modo significati"[27], da altro, la stessa renderebbe le norme tradizionali non sufficienti "per attivare la responsabilità per i danni causati da un robot, in quanto non consentirebbero di determinare qual è il soggetto cui incombe la responsabilità del risarcimento né di esigere da tale soggetto la riparazione dei danni causati"[28].

---

[24] Art. 59, lett. F, *Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, (2015/2103(INL), 17 febbraio 2017, in *eur-lex.europa.eu*. Su quella risoluzione si vedano i commenti di G. TADDEI ELMI e F. ROMANO, *Il robot tra* ius condendum *e* ius conditum, in *Inf. Dir*., 2016, 115; A. ZORNOZA e M. LAUKYTE, *Robotica e diritto: riflessioni critiche sull'ultima iniziativa di regolamentazione in Europa*, in *Contr. impr. Eur*., 2016, p. 808; N. BUSTO, *La personalità elettronica dei robot: logiche di gestione del rischio tra trasparenza e fiducia*, in *Ciberspazio e dir*., 2017, 499; G. PASSAGNOLI, *Regolamento giuridico e tutele nell'intelligenza artificiale*, in *Pers. merc*., 2019, p. 79; G. DI ROSA, *Quali regole per i sistemi automatizzati "intelligenti"?*, in *Riv. dir. civ*., 2021, p. 823.

[25] C. LEROUX – R. LABRUTO (eds), *Suggestion for a green paper*, cit., p. 60.

[26] Conss. AB, AA, *Risoluzione del Parlamento europeo del 16 febbraio 2017*, cit. Nella letteratura, condividono la preoccupazione per cui "le regole ordinarie di responsabilità sono insufficienti e che sono necessarie nuove norme per aiutare a determinare cosa succede ora che gli strumenti possono produrre danni a causa delle loro "cattive" decisioni", A. ZORNOZA e M. LAUKYTE, *op. cit*., p. 810; in senso opposto, al termine di una rilettura delle norme codicistiche, nega l'esistenza di un tale rischio di *liability gap*, U. RUFFOLO, *Intelligenza Artificiale*, machine learning *e responsabilità da algoritmo*, in *Giur. it*., 2019, p. 1689.

[27] Cons. Z, *Risoluzione del Parlamento europeo del 16 febbraio 2017*, cit.

[28] Cons. AF, *Risoluzione del Parlamento europeo del 16 febbraio 2017*, cit.

Orbene, ferma la tradizionale distinzione nel termine persona[29] dell'essere umano (persona fisica) e dell'ente creato artificialmente per uno scopo giuridico (persona giuridica)[30] e irrevocata in dubbio la legittimità del legislatore di procedere in tal senso per risolvere problemi di responsabilità, va osservato come la proposta soluzione a questa presunta carenza – i.e. il riconoscimento della personalità elettronica – sia stata fortemente criticata fino ad essere completamente abbandonata dalle istituzioni europee[31].

A ben vedere, essa poggia su di un errore di valutazione della specifica capacità del *software* di intelligenza artificiale di elaborazione automatica dell'algoritmo la cui esecuzione automatica restituisce un certo *output*. In quell'automatismo, come visto, si è letto una manifestazione di "autonomia"[32]. In effetti, leggere una forma di coscienza

---

[29] *Ex multis*, J.CHIPMAN GRAY, *The Nature and Sources of the Law* (1909), London, 2020, p. 19; F. FERRARA, *Le persone giuridiche*, *Tratt. Vassalli*, II, 2°, 1958, p. 7.

[30] Di recente, si è soffermato sull'influenza del pensiero di Savigny" – cui si deve la definizione di "*juristiche Person*" come, appunto, di "*ein des Vermögens fähiges künstlicj angenommenes Subjekt*" – nel diritto italiano ed europeo, F. RANIERI, *L'invenzione della persona giuridica. Un capitolo nella storia del diritto dell'Europa continentale*, Milano, 2021.

[31] Si veda la lettera con cui centinaia di scienziati hanno criticato la proposta di istituire la personalità elettronica: l'*Open Letter to the European Commission Artificial Intelligence and Robotics*, in http://www.robotics-openletter.eu/. Nel senso della posizione del Parlamento europeo militano A. ZORNOZA e M. LAUKYTE, *op. cit.*, p. 8; invece, per una chiara critica alla tesi della personalità elettronica, si veda E. PALMERINI, Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea, in Resp. civ. prev., 2016, p. 1837, la quale bene evidenzia il carattere fuorviante, prematuro e inadeguato.

[32] A ben vedere, il ricorso ai concetti di autonomia, di *software* cosciente e di personalità elettronica si spiega più con la plurisecolare fantasia della macchina intelligente (in argomento, G. WOOD, *Edison's Eve. A Magical History of the Quest for Mechanical Life*, New York, 2002, nonché A. PUNZI, *L'ordine giuridico delle macchine*. *La Mettrie Helvétius D'Holbach. L'uomo-macchina verso l'intelligenza collettiva*, Torino, 2003) che con il dato reale. A conferma di questa influenza culturale è la circostanza per cui ogni articolo giuridico che discute la disciplina dell'intelligenza artificiale riprende una qualche immagine che, nel corso della storia, l'uomo si è dato a proposito della macchina animata. Talvolta, si cita l'etimologia del termine 'robot', il cui esordio si vuole risalente al 1923, quale traduzione del vocabolo ceco '*robotnik*' (lavoratore forzato), impiegato dallo scrittore Karel Capek nel suo dramma fantascientifico *Rossum's Universal Robots*, talaltra si richiama il mito di Pigmalione o il personaggio di *Frankenstein*. Ancora più diffuso è il richiamo alle tre leggi di Asimov, tratte da *Runaround* (1942), e la cui formulazione originaria così si sviluppa: «*A robot may not injure a human being or, through inaction, allow a human being to come to harm; A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law; A robot must protect its own existence as long as such protection does not conflict with the First or Second Law*». Tale tributo artistico-letterario, peraltro, non è una esclusiva della dottrina

(necessaria per darsi le regole) nella automatica elaborazione dell'algoritmo appare immotivato. Al più, tale automatismo, come è stato esattamente notato, integra la figura leibniziana dei pensieri ciechi[33].

Per avere un corretto inquadramento giuridico di questa tecnologia ed evitare fughe non si sa quanto ingenue verso la personalità elettronica, è sufficiente porre a mente la circostanza per cui il dato-risultato (*output*) ottenuto dall'applicazione dell'algoritmo elaborato (*process*) dai dati disponibili (*input*) non è una regola generale, ma un qualcosa di particolare come, d'altra parte, è particolare anche il dato di partenza (*input*). Tale aspetto (da particolare a particolare) consente di qualificare questi *software* di *machine learning* come un procedimento induttivo o inferenziale e non già come uno di tipo sussuntivo (dal generale al particolare) o per astrazione (dal particolare al generale). In tal senso il *machine learning* richiama la definizione di cui all'art. 2727 c.c. in materia di presunzioni ("le presunzioni sono le conseguenze che la legge o il giudice trae da un fatto noto per risalire a un fatto ignorato").

6.7. *Machine learning* e diritto: applicazioni pratiche

Nel campo del diritto, un'applicazione di questa intelligenza artificiale molto diffusa è quella della c.d. giustizia predittiva. Dato conto della capacità dell'intelligenza artificiale quale *software* in grado di produrre risultati elaborando i dati disponibili, non sorprende che in molti Paesi si siano avviati progetti di scrittura di programmi che a partire dai dati (*input*) relativi a procedimenti giudiziari elaborano delle regole che restituiscano risultati (*output*) in merito alla durata del procedimento, all'esito, all'ammontare del risarcimento e via discorrendo. Tali risultati possono essere letti come delle previsioni di un certo risultato processuale (da qui, appunto, l'espressione di giustizia predittiva)[34].

---

giuridica e la stessa citata risoluzione del Parlamento europeo sulle *Norme di diritto civile sulla robotica* del 16 febbraio 2017 si apre rilevando come «gli esseri umani» abbiano «fantasticato sulla possibilità di costruire macchine intelligenti, spesso androidi con caratteristiche umane».

[33] R. BODEI, *Automatismo del pensiero umano e macchine calcolatrici*, in *Mondo digitale*, 2016, p. 1.

[34] In argomento, v. i saggi raccolti in A. CARLEO (a cura di), *Calcolabilità giuridica*, Bologna, Il Mulino, 2017, nonché A. GARAPON , J. LASSÈGUE, *Justice Digitale. Révolution graphique et rupture anthropologique*, Paris, PUF, 2018; M. LUCIANI. *La decisione*

Tra le tante esperienze fin qui maturate, si può fare riferimento al progetto *DataJust*, avviato dalla Repubblica francese nei primi mesi del 2020 (*Décret* n. 2020-356)[35]. *DataJust* intende raccogliere i dati sui procedimenti giudiziari concernenti il risarcimento del danno conseguente a lesioni fisiche. In particolare, i dati (*input*) forniti al *software* ed estrapolati dalle decisioni di secondo grado rese tra il 2017 e il 2019 sono quelli relativi alla lesione, all'età delle parti, al loro sesso, alla residenza, all'eventuale rapporto familiare, alla vita professionale e finanziaria delle parti, alla lesione, al suo impatto, ai referti medici e alle spese sanitarie sostenute, ai precedenti penali e non. Il nome delle parti non è inviato al ministero. L'obiettivo del Ministero della Giustizia francese perseguito con questa iniziativa è quello di mettere a punto – nel tempo massimo di due anni – un *software* in grado di fornire dati (*output*) attendibili circa l'ammontare del risarcimento (regressione lineare), così che il programma possa rilevare come fonte di informazione utile per le vittime e come ausilio ai giudici per la quantificazione del danno conseguente a lesioni fisiche. L'attendibilità e l'affidabilità del *software* potrebbe giocare un ruolo, infine, molto importante per ridurre il contenzioso giudiziario, consentendo alle parti di avere una stima precisa dell'ammontare del danno.

Differente è poi l'impiego di un *software* di giustizia c.d. predittiva che restituisce come *output* la previsione sulla decisione di un certo organo giudicante. Ad esempio, uno studio americano di qualche anno fa ha costruito un algoritmo in grado di restituire un risultato coincidente, per circa il 70% delle volte, con le decisioni assunte dalla *Supreme Court* degli Stati Uniti in circa due secoli (1816-2015, si tratta di oltre 28000 casi). Per fare ciò, gli studiosi hanno utilizzato i dati disponibili nella banca dati della *Supreme Court* e individuato oltre duecento variabili[36]. Programmi analoghi sono comparsi un po' ovunque negli

giudiziaria robotica, in *Rivista AIC*, 2018, p. 22 (disponibile a: https://www.rivistaaic.it/images/rivista/pdf/3_2018_Luciani.pdf); G. TUZET, *L'algoritmo come pastore del giudice? Diritto, tecnologie, prova scientifica*, in *Riv. dir. media*, 2020, 1, p. 45; E. BATTELLI, *Giustizia predittiva, decisione robotica e ruolo del giudice*, in *Giust. Civ.*, 2020, p. 281; A. CARRATTA, *Decisione robotica e valori del processo*, in *Riv. dir. proc.*, 2020, p. 491; G. ZACCARIA. *Figure del giudicare: calcolabilità, precedenti, decisione robotica*, in *Riv. dir. civ.*, 2020, p. 277.

[35] Testo disponibile in https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041763205.

[36] DM. KATZ, MJ. BOMMARITO II, J. BLACKMAN, *A general approach for predicting the behavior of the Supreme Court of the United States*, in PLoS ONE 12(4), 2017: e0174698. https://doi.org/10.1371/journal.pone.0174698.

ultimi anni, sfruttando l'enorme mole di dati di cui si dispone, in particolare con riferimento ai giudizi di ultima istanza.

Questo genere di studi è estremamente interessante perché consente di fare supposizioni su quale elemento sia più rilevante nella decisione. Ad esempio, nel lavoro svolto rispetto alla giurisprudenza della Corte Europea dei Diritti dell'Uomo e in cui la percentuale di previsione corretta si è rivelata essere di circa il 79% si è evidenziata l'importanza del fatto, e della sua descrizione[37]. Anche in Italia vi sono degli studi, seri, in questo senso. Ad esempio, quello portato avanti dall'università di Bologna e di Pavia (*Legal Analytics for Italian LAw*, LAILA) e che intende occuparsi dell'applicazione dei metodi di analisi giuridica ad un vasto e diversificato insieme di informazioni giuridiche (legislazione, giurisprudenza e dati giuridici empirici), per estrarre conoscenze giuridiche, dedurre relazioni non ancora scoperte ed effettuare previsioni guidate dai dati[38]. Di recente, la Scuola Universitaria Superiore IUSS di Pavia e il Centro Elettronico di Documentazione della Suprema Corte di Cassazione hanno dato vita a un programma che, attraverso l'uso degli strumenti della c.d. *legal analytics* (*data science*, intelligenza artificiale, *machine learning*, *natural language processing* e statistica) ha l'obiettivo di «estrarre e rappresentare conoscenza giuridica, rinvenire correlazioni implicite, individuare tendenze ed effettuare previsioni relative agli orientamenti giurisprudenziali e/o legislativi in modo che sia meglio consultabile ed elaborabile in sede di attività giudiziaria e di ricerca scientifica»[39].

6.8. *Machine learning* e il diritto: il principio a non essere sottoposto a una decisione interamente automatizzata

Discorso ancora diverso e, di tutta evidenza, più delicato riguarda invece l'impiego di *software* di giustizia predittiva impiegati per

[37] N. Aletras, D. Tsarapatsanis, D. Preoțiuc-Pietro, V. Lampos, *Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective*, in *PeerJ Computer Science*, 2016, 2:e93 https://doi.org/10.7717/peerj-cs.93.

[38] Sul Progetto LAILA si veda: https://dsg.unibo.it/it/ricerca/progetti-di-ricerca/progetti-nazionali-e-di-ateneo/prin2017-laila-legal-analytics-for-italian-law

[39] Il testo dell'accordo tra la Corte di Cassazione e la Scuola Universitaria Superiore siglato lo scorso 5 ottobre 2021 è disponibile in https://www.cortedicassazione.it/corte-di-cassazione/it/dettaglio_ecs.page?contentId=ECS26105

decidere se rilasciare un detenuto su cauzione, se concedere la libertà vigilata oppure in quale zona della città inviare un maggiore numero di pattuglie di polizia. A tal proposito è interessante una decisione, divenuta celebre e che non a caso si rinviene in pressoché tutte le trattazioni sull'argomento, emessa da un organo giudicante statunitense. Si tratta della sentenza *State of Wisconsin v. Eric L. Loomis* resa dalla *Supreme Court* del Wisconsin il 13 luglio 2016[40].

Tale decisione aveva ad oggetto l'appello avverso una decisione di un tribunale locale (La Crosse) che aveva condannato il ricorrente, Eric L. Loomis, alla pena reclusiva di sei anni per una serie di reati connessi alla guida di una macchina rubata e che risultava essere stata impiegata per una sparatoria. In primo grado, l'imputato si era dichiarato colpevole rispetto ad alcune delle accuse mossegli e il Tribunale aveva proceduto a una indagine sul suo *background* per determinare gli anni di reclusione (*Pre-sentence Investigation*). La doglianza riguardava la circostanza per cui il Tribunale di La Crosse avesse utilizzato l'*output* del *software Correctional offender management profiling for alternative sanctions* (COMPAS) nel determinare l'entità della pena da irrogare.

COMPAS è un *software* di *risk assessments and recidivism data at sentencing*. Esso ha come compito quello di indicare il rischio di recidiva di un soggetto e i suoi bisogni, a partire dai dati presenti nel fascicolo, dell'interrogatorio che questi ha svolto e dei dati relativi alle persone con un passato simile. Il *software* assegna il profilo del soggetto da valutare al gruppo di persone più vicino (simile, affine), così che l'*output* – uno score relativo alle diverse tipologie di recidiva, processuale, generale e violante - rilevi come previsione circa la probabilità di sua recidiva e funga da ausilio al giudice (*to provide decisional support*). La *presentence investigation* indicava esplicitamente che l'*output* non dovesse essere considerato come l'unico elemento su cui basare il giudizio relativo all'ammontare degli anni di reclusione. Il Tribunale aveva assunto la sua decisione - sei anni di reclusione – anche sulla base dei risultati del *software*, alla luce dei quali aveva anche negato la concessione della libertà vigilata. Contro questo primo provvedimento del Tribunale, la difesa di Loomis aveva presentato una richiesta di revisione della decisione, contestando l'utilizzo del *software* COMPAS, la sua affidabilità nonché la assenza di trasparenza circa il modo in cui veniva raggiunto l'*output*. Contro il provvedimento che respingeva la

[40] *Supreme Court of Wisconsin*, 13.7.2016, (*881 N.W.2d 749* (*2016*)): il testo è disponibile in http://www.scotusblog.com/case-files/cases/loomis-v-wisconsin/

richiesta di revisione, Loomis decise di proporre ricorso in appello e nell'ambito di questo procedimento di impugnazione la questione viene deferita alla Corte Suprema.

Chiamata a decidere sull'ammissibilità dell'impiego di un *software* e sul diritto a una *individualized sentence based on the charges and the unique character of the defendant*» e ad una pena *based on accurate information*», la Corte Suprema del Wisconsin ha offerto una decisione estremamente chiara. Innanzitutto, la Corte ha osservato come l'*output* del *software* COMPAS non sia stato l'unico elemento utilizzato dai giudici del Tribunale di La Crosse per decidere l'ammontare della pena reclusiva e la mancata concessione della libertà vigilata. Accanto al dato prodotto dall'algoritmo sulla pericolosità di Loomis, infatti, i giudici avevano richiamato anche altri, dati come la gravità dei reati contestatigli e la condotta pregressa. Per quanto riguarda, l'assenza di trasparenza – COMPAS è un *software* di proprietà di un soggetto privato e il suo algoritmo è coperto da brevetto – la Corte ha ritenuto la conoscenza degli *score* che il soggetto riceve dal *software* e che possono essere contestati un elemento sufficiente. Al contempo, essa ha raccomandato che il programma sia correttamente aggiornato, di modo da ridurre il rischio di distorsioni e di *bias*, alcuni dei quali già emersi (gli imputati neri avevano molte più probabilità di essere erroneamente giudicati ad alto rischio di recidiva di quelli bianchi; allo stesso modo, gli imputati bianchi avevano più probabilità degli imputati neri di essere erroneamente segnalati come a basso rischio). Essa ha, infine, ribadito che il *software* non è pensato per essere determinante nella decisione sulla reclusione o sul suo ammontare e non è da intendersi come alternativo alla discrezionalità del giudice. Al contrario, la *Supreme Court* del Wisconsin ha spiegato come COMPAS rilevi quale strumento per fornire il tribunale di un dato attendibile circa la probabilità con la quale un profilo criminale come quello dell'imputato possa reiterare il reato. In particolare, essa chiarito che mentre «*using a risk assessment tool to determine the length and severity of a sentence is a p oor fit*», COMPAS può essere utile a) nell'identificare i detenuti che sono a basso rischio di recidiva ai fini del loro dirottamento verso alternative non carcerarie e aiuta a decidere se sospendere tutta o parte della pena di un detenuto; b) per valutare il rischio per la sicurezza pubblica del reo e rilevare nella decisione se il rischio di recidiva presentato dal reo può essere gestito in modo sicuro ed efficacemente ridotto attraverso la supervisione e i servizi della comunità; c) per orientare le decisioni

sui termini e le condizioni della libertà vigilata e della supervisione (le valutazioni del rischio possono essere utili per identificare i criminali a basso rischio che non richiedono una supervisione intensiva e programmi di trattamento). In particolare, può rilevare nelle decisioni quali i requisiti di segnalazione, i test antidroga, il monitoraggio elettronico, il servizio comunitario e le strategie di trattamento più appropriate.

6.9. Il principio a non essere sottoposto a una decisione interamente automatizzata e il GDPR

Il diritto affermato dalla *Supreme Court* del Wisconsin e che afferma il principio a non essere sottoposto a una decisione interamente automatizzata circola e attraversa anche altri spazi da quello, evidentemente delicato, del processo penale statunitense. In questa sede, si discuterà della profilazione, ossia di quell'inferenza con cui dalla raccolta di dati (*input*) e dalla loro analisi automatizzata si elabora (*process*) un modello (appunto, un profilo) la cui applicazione porta all'individuazione di caratteristiche (*output*) di comportamento, di capacità, di interessi, etc[41]. A livello europeo (e, quindi, nazionale), la disciplina rilevante è offerta dal regolamento generale sul trattamento dei dati personali (reg. EU/2016/679, *General Data Protection Regulation*, GDPR), adottato il 27 aprile 2016, entrato in vigore il 24 maggio dello stesso anno, operativo a partire dal 25 maggio 2018.

6.9.1. La profilazione

Il GDPR definisce la profilazione, come *i*) una qualsiasi forma di trattamento *ii*) automatizzato, *iii*) effettuato su dati personali *iv*) per valutare determinati aspetti personali[42].

Il primo elemento rilevante della definizione di profilazione offerta dal GDPR rimanda alla nozione di trattamento, definita come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio

[41] per la definizione di «profilazione» si v. art. 4, lett. 4) GDPR. Sui problemi sottesi alla profilazione, si v. S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 404.

[42] Con riferimento alla profilazione nell'esperienza interna precedente al GDPR, si v. l'art. 37, lett. d), d.lgs. 30 giugno 2003, n. 196 e, in giurisprudenza, Corte Cass., 8 novembre 2021, n. 32411, in http://www.italgiure.giustizia.it/sncass/ ("il trattamento con modalità automatizzata di dati personali con il fine di definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo").

di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

Il secondo elemento rilevante della definizione di profilazione offerta dal GDPR attiene all'essere tale trattamento di dati automatizzato. Come si legge nelle *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (nel prosieguo, *Guidelines WP 251/rev01*), la profilazione «*is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar*»[43]. Il terzo aspetto rilevante della definizione di profilazione contenuta nel GDPR riguarda invece i dati oggetto del trattamento automatizzato: i dati personali, ossia «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)»[44].

Infine, l'ultimo elemento costitutivo della nozione di profilazione adottata dal GDPR attiene alla circostanza per cui essa deve servire «per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Giova osservare che è necessario che ricorrano tutti gli elementi ora indicati: per esempio, il trattamento automatizzato di dati personali per finalità diverse da quelle di valutazione della persona fisica non rientra nella nozione di profilazione offerta dal regolamento. Per aversi una profilazione rilevante ai fini del GDPR, quindi, è necessario che il trattamento automatizzato dei dati personali sia finalizzato alla valutazione di aspetti personali dell'interessato (come accade, appunto, nell'esempio proposto relativo alla concessione del prestito). Una volta compresa la nozione di profilazione adottata dal GDPR occorre passare alla disciplina applicabile.

---

[43] *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* adottate *dall'Article 29 Data Protection Working Party* il 6 febbraio 2018 (testo disponibile in https://ec.europa.eu/newsroom/article29/items/612053).

[44] Per la definzione di «dato personale» si v. art. 4, lett. 1, GDPR.

Questa varia a seconda che il processo decisionale si basi sulla profilazione in modo esclusivo o meno.

6.9.2. La disciplina della decisione basata anche sulla profilazione

In questo paragrafo, si prenda l'ipotesi di una domanda di prestito formulata *on-line* sul sito internet di un istituto di credito, il quale prevede che la decisione sulla concessione del credito sia assunta da un proprio dipendente anche sulla base di un profilo elaborato con mezzi automatizzati (*software*). Ciò vuole dire che la decisione è assunta sulla base del trattamento automatizzato (profilazione), ma non unicamente: il dipendente della banca, infatti, decide se concedere il prestito considerando anche (= oltre alla profilazione) altri elementi (colloquio con il richiedente, etc.).

All'ipotesi qui descritta di decisione basata anche sulla profilazione (trattamento automatizzato di dati personali per valutare aspetti personali) si applica la disciplina generale del GDPR e ad essa occorre guardare, in modo sintetico, per comprendere le risposte alle domande tipiche del ragionamento presuntivo (quando si può procedere per presunzioni? quali presunzioni si possono utilizzare? come?).

Mentre il secondo comma dell'art. 2729 c.c. definisce in negativo i presupposti per il ricorso da parte del giudice al procedimento induttivo in materia probatoria, l'art. 6 GDPR individua esplicitamente, in positivo, i presupposti («condizioni» il cui ricorrere rende lecito l'attività altrimenti illecita) per il ricorso alla profilazione. In questo senso, l'art. 6 GDPR risponde alla domanda relativa al quando si può procedere per presunzioni con riferimento alla profilazione.

In particolare, il GDPR richiama il consenso[45] dell'interessato al trattamento[46] e la circostanza che il trattamento *de qua* sia necessario –

[45] Per la definizione di «consenso dell'interessato», si v. art. 4, lett. 11) GDPR; per la disciplina, si v. anche l'art. 7, GDPR. Si v. anche le *Guidelines on Consent under Regulation 2016/679*, adottate dall'*Article 29 Data Protection Working Party* il 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849.

[46] Limitando i riferimenti alla bibliografia in lingua italiana, sul consenso nel GDPR si vedano, tra gli altri, i contributi di A.M. GAROFALO, *Regolare l'irregolabile: il consenso al trattamento dei dati nel* GDPR, in S. ORLANDO – G. CAPALDO, *Annuario* 2021, *Osservatorio Giuridico sull'Innovazione Digitale*, Roma, Sapienza Università Editrice, 2021, p. 119; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Oss. dir. civ. comm.*, 2018, p. 67; F. CAGGIA, *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Riv. dir. comm.*, 2019, I, p.

requisito da intendersi restrittivamente – all'esecuzione del contratto o delle misure precontrattuali[47] oppure; all'adempimento di obblighi legali ai quali è tenuto il titolare del trattamento[48]; alla salvaguardia degli interessi vitali di una persona fisica anche diversa dall'interessato[49]; all'esecuzione di un interesse pubblico affidato al titolare del trattamento[50]; al perseguimento di un legittimo interesse anche di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore[51].

L'art. 9 GDPR, invece, stabilisce un generale divieto di trattare – anche in via automatizzata – dati personali che «rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». La medesima disposizione individua i casi in cui tale divieto viene meno[52] e, tra questi, spicca il riferimento all'ipotesi in cui l'interessato ha prestato «il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto»[53].

In conclusione, in un procedimento decisionale si può ricorrere alle presunzioni e alle inferenze proprie della profilazione autorizzata quando il titolare del procedimento abbia soddisfatto le «condizioni» (es. consenso dell'interessato) previste dal GDPR.

La profilazione è una attività complessa. A una prima fase di raccolta dei dati, segue una seconda di analisi automatizzata degli stessi e, quindi, una terza fase in cui si applica il modello elaborato (profilo) a una persona fisica così «da analizzare o prevedere aspetti riguardanti

405; L. Gatt, R. Montanari, I. A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, p. 363; S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv.*, 2016, p. 513.

47 Art. 6, para 1, lett. b) GDPR.

48 Art. 6, para 1, lett. c) GDPR.

49 Art. 6, para 1, lett. d) GDPR.

50 Art. 6, para 1, lett. e) GDPR.

51 Art. 6, para 1, lett. f) GDPR.

52 Art. 9, para 2, GDPR.

53 Art. 9, para 2, lett. a) GDPR.

il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[54]. Ciascuna delle tre fasi che compongono la profilazione rilevante ai fini GDPR è orientata dai principi affermati ex art. 5, GDPR i quali, appunto, rispondono alla domanda circa il come si possa utilizzare la profilazione in un procedimento decisionale.

Innanzitutto, si deve qui segnalare il principio della trasparenza del trattamento, che si traduce in una pregnante serie di obblighi informativi per il titolare del trattamento[55]. In particolare, questi dovrà spiegare come funziona la profilazione all'interessato[56], garantendogli altresì il diritto di accesso, ossia il diritto di ottenere informazioni dettagliate sui dati personali utilizzati per la profilazione[57].

Un ulteriore principio di grande importanza è quello della c.d. esattezza. Come la possibilità di basare una decisione giudiziale su dei collegamenti che non passano per leggi universali e scientifiche, ma per delle inferenze probabilistiche è ammessa nella misura in cui questi siano «gravi, precise e concordanti»[58], così per il ricorso alla profilazione in un procedimento decisionale è richiesto che i dati siano «esatti e, se necessario, aggiornati»[59].

Questo principio non sorprende. Il procedimento induttivo che caratterizza i *software* di intelligenza artificiale – e, tra questi, anche quelli che vengono impiegati per la profilazione – presenta un grosso rischio, relativo alla circostanza per cui se i dati di *input* sono inesatti, viziati, superati o parziali, il profilo (algoritmo) che ne deriva sarà distorto e così la decisione (*output*) che su di esso si basa (c.d. *garbage in, garbage out*, GIGO). Connessi a tale principio di esattezza sono, *inter alia*, il diritto di rettifica[60] e quello di cancellazione[61] i quali si applicano sia ai dati *input* sia a quelli *output*[62]. Il primo, in particolare, comporta la possibilità per l'interessato di ottenere «la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo», nonché, e tenuto

[54] Art. 4, lett. 4) GDPR.
[55] Art. 5, para 1, lett. *a*), GDPR.
[56] Artt. 13, 14, GDPR.
[57] Art. 15, GDPR; *adde Guidelines WP 251/rev01*, cit., p. 17.
[58] Art. 2729, co. 1, c.c.
[59] Art. 5, para 1, lett. *d*, GDPR.
[60] Art. 16, GDPR.
[61] Art. 17, GDPR.
[62] *Guidelines WP 251/rev01*, cit., p. 17-18.

conto delle finalità del trattamento, «l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa»[63].

In conclusione, rispetto ai procedimenti decisionali basati sulle inferenze prodotte dalla profilazione, il GDPR individua i requisiti che rendono lecito tale ricorso e le modalità di utilizzo, stabilendo doveri di informazioni *ex ante* e obblighi di rettifica a cancellazione.

6.9.3. La disciplina della decisione basata unicamente sulla profilazione

Nell'esempio discusso nel paragrafo precedente, la decisione (sulla concessione del credito) è assunta (da un dipendente della banca) anche sulla base di un profilo elaborato con mezzi automatizzati (*software*). Come noto, il GDPR contiene una normativa con riguardo a una distinta ipotesi, in cui la decisione è basata «unicamente» sulla profilazione (trattamento automatizzato di dati personali per valutare aspetti personali). Tale seconda disciplina – che si rinviene nell'art. 22 GDPR – va ad aggiungersi a quella esaminata nel paragrafo precedente.

Per comprendere bene l'ipotesi in cui la decisione è basata «unicamente» sulla profilazione, si immagini che stavolta rispetto alla richiesta di prestito formulata *on-line* l'istituto di credito preveda una procedura in cui la decisione sulla concessione del mutuo si fonda esclusivamente all'*output* elaborato da un *software* di intelligenza artificiale senza che vi sia spazio per altri elementi. Se nell'esempio precedente, l'*output* del *software* era valutato da un dipendente (persona fisica) della banca insieme ad altri fattori (es. colloquio), qui, invece, esso è il solo elemento su cui l'istituto di credito basa la sua decisione.

Nel rispondere alle tipiche domande del procedimento presuntivo (quando si può procedere per presunzioni? quali presunzioni si possono utilizzare? come?), la disciplina dettata a tale riguardo dall'art. 22 GDPR riveste un grande interesse teorico, giacché afferma due principi – quello della non esclusività e quello della conoscibilità – di sicura rilevanza per i *software* di intelligenza artificiale.

Il primo comma dell'art. 22 afferma il c.d. principio di non esclusività della decisione algoritmica, ossia il diritto di non essere sottoposto a una decisione che sia basata unicamente su un trattamento automatizzato (come appunto la profilazione) e che produca effetti giuridici che lo riguardano o incida in modo significativo sulla sua persona,

[63] Art. 16, GDPR.

quali il rifiuto automatico di una domanda di credito *online* o di pratiche di assunzione elettronica senza interventi umani[64]. In particolare, la norma prevede che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona»[65].

Le già citate *Guidelines WP 251/rev01* hanno chiarito i requisiti per il sorgere del diritto, ossia ciò che si deve intendere per decisione basata unicamente su un trattamento automatizzato e per decisione che produca effetti giuridici che riguardano l'interessato o che incida in modo analogo significativamente sulla sua persona. Il primo elemento concerne l'assenza di un fattore su cui basare la decisione diverso dal trattamento automatizzato dei dati[66]. Il secondo requisito, invece, va scomposto in due sub-elementi. Per un verso, rileva la idoneità della decisione assunta sulla base del trattamento interamente automatizzata a produrre effetti giuridici, il che vuole dire, ad esempio, la cancellazione di un contratto, la negazione della cittadinanza e così via. Per altro verso, per essere significativa sulla persona, la decisione, come si legge nelle *Guidelines WP 251/rev01*, deve essere in grado di incidere sulle scelte dell'interessato e sul suo comportamento, come può essere una decisione sull'accesso al credito, ai servizi sanitari o all'università[67].

Le medesime *Guidelines WP 251/rev01* chiariscono altresì che il termine «diritto» non deve essere inteso immaginando che la non esclusività si applichi solo a seguito di un qualche esercizio del titolare. Ciò sta a significare che l'articolo 22, para. 1, GDPR stabilisce un divieto generale, vigente a prescindere dall'attività dell'interessato[68]. *Mutatis mutandis*, esso va inteso alla stregua del secondo comma dell'art. 2729 c.c. (a mente del quale, «le presunzioni non si possono ammettere nei casi in cui la legge esclude la prova per testimoni») e ciò in quanto anche l'art. 22 para. 1, GDPR indica quando il ricorrere a delle

[64] Cons. 71, GDPR.

[65] Art. 22, para. 1, GDPR.

[66] *Guidelines WP 251/rev01*, cit., p. 20-21. Nella letteratura, sull'art. 22 para 1. si veda in particolare G. MALGIERI-G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *Intern. Data Priv. Law*, 2017, p. 251.

[67] *Guidelines WP 251/rev01*, cit., p. 21-22.

[68] *Guidelines WP 251/rev01*, cit., p. 20.

presunzioni (=profilazione) non è possibile (esclusività del trattamento automatizzato come fattore di decisione e rilevanza sul piano personale della decisione).

Si è prima osservato come il divieto di decisioni su base interamente automatizzata e significative per l'interessato sia analogo al divieto di cui al secondo comma dell'art. 2729 c.c. con riferimento alle presunzioni semplici in materia probatoria. In entrambi i casi si impedisce il ricorso a un meccanismo presuntivo. A differenza del divieto di ricorso a presunzioni semplici nei casi in cui la legge esclude la prova per testimoni (art. 2729, secondo comma c.c.), il divieto ex art. 22 GDPR para 1 ammette delle deroghe. Il paragrafo successivo, infatti, stabilisce le ipotesi in cui venga meno il diritto a non essere sottoposto a una decisione interamente automatizzata e significativa[69].

Questo divieto non si applica allorché la decisione basata esclusivamente su di un trattamento automatizzato (come, appunto, la profilazione) e significativa a livello personale *a*) sia necessaria per la conclusione o per l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; *b*) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; *c*) si basi sul consenso esplicito dell'interessato. Nelle eccezioni di cui all'art. 22, para 2, sub *a*) e *c*) non rientra il processo decisionale interamente automatizzato dei dati personali appartenenti a categorie particolari[70], il quale non è ammesso salvo che ricorra l'esplicito consenso dell'interessato, l'interesse pubblico al trattamento e che comunque siano in vigore misure adeguate alla tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato[71].

Per quanto sia affermato un generale divieto a decisioni interamente automatizzate che producono effetti giuridici significativi sulla persona[72], l'enorme estensione delle deroghe[73] rende di grande importanza la disciplina prevista a proposito dell'utilizzo di queste presunzioni. Il GDPR, infatti, stabilisce un principio fondamentale rispetto a

[69] Art. 22, para. 2, GDPR. Per una discussione delle misure adeguate che accompagnano l'utilizzo di decisioni interamente automatizzate, si v. E. FALLETTI, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in *Dir. informaz. informat.*, 2020, p. 169.

[70] Art. 9, para 1, GDPR.

[71] Art. 22, para. 4, GDPR.

[72] Art. 22, para. 1, GDPR.

[73] Art. 22, para. 2, GDPR.

due delle ipotesi, ossia quelle ex art. 22, para 2, lett. *a*) e *c*) (*i.e*. contratto e consenso), in cui è ammesso il ricorso a decisioni interamente automatizzate che producono effetti giuridici significativi sulla persona.

Nei casi in cui tale processo decisionale è così ammesso, il titolare deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, garantendogli, almeno, il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione[74]. Se il diritto di ottenere l'intervento umano sta a significare la possibilità di ripristinare il principio della non esclusività della decisione automatizzata (e quindi il diritto di cui all'art. 22, para. 1, GDPR), il diritto di esprimere la propria opinione e quello di contestare la decisione sono alla base del dibattito sul c.d. diritto alla spiegazione (*explainable artificial intelligence*, XAI) che, almeno secondo certi Autori, ne costituisce, per così dire, il presupposto logico e necessario per l'esercizio[75].

Ancorché l'esistenza di questo diritto alla spiegazione non sia riconosciuto da tutti gli Autori, le citate *Guidelines WP 251/rev01* dove si legge che l'art. 22, para. 3, GDPR riconoscono in capo al titolare del trattamento un obbligo di «*to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm*»[76]. L'informazione da fornire all'interessato *ex post* dovrà essere resa per iscritto, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro e in via tempestiva (ex art. 12, GDPR).

---

[74] Art. 22, para. 3, GDPR.

[75] Sul rapporto tra art. 22, para. 3, GDPR e il diritto alla spiegazione va osservato che la dottrina è divisa. A fronte di chi ritiene che la norma ex art. 22, para. 3, GDPR si sostanzia sia nel diritto a comprendere come la tecnologia funzioni sia nel definire chi debba dar conto per come essa funziona (in tal senso, *inter alia*, R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr*., 2019, p. 861; U. PAGALLO, *Algoritmi e conoscibilità*, cit., p. 96), altri negano tale diritto, osservando che dalla norma in esame si possa ricavare unicamente un dovere di rendere informazioni in merito alle generali funzionalità del *software* (così, S. WACHTER, B. MITTELSTADT, L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,* in *International Data Privacy Law*, 2017, p. 76). Una terza posizione, infine, afferma il c.d. diritto alla leggibilità, con ciò intendendo la pretesa del singolo a poter comprendere in via autonoma il processo decisionale automatizzato (G. MALGIERI-G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists*, cit., p. 256).

[76] *Guidelines WP 251/rev01*, cit., p. 25.

In sintesi, l'art. 22, terzo comma GDPR offre una risposta alla domanda sull'utilizzo (eccezionale) dell'*output* generato dal trattamento personalmente significativo e interamente automatizzato di dati personali nel senso di prevedere un insieme di diritti per l'interessato e obblighi per il responsabile del trattamento che consentono il rispetto dell'obiettivo fondamentale del GDPR, ossia il controllo sui propri dati personali[77]. Tra questi diritti/obblighi spicca quello, di natura informativa, teso a rendere disponibili, *ex post* e secondo una modalità «sufficientemente comprensiva», i dati che spiegano "*the logic involved*".

6.10. Conclusioni

Anche rispetto alla rivoluzione tecnologica in essere il diritto civile assolve il suo compito di regolare la convivenza secondo giustizia e non forza[78], così da "indirizzare l'intelligenza artificiale verso il bene degli individui e della società"[79]. Tale sforzo passa per l'affermazione di principi nuovi, che, come visto, si affermano nella società, quindi nelle aule dei tribunali e infine circolano tra ordinamenti e sistemi diversi. Di questo sforzo, la ricerca scientifica deve essere partecipe: "*There are all too many people who, in some great period of social change, fail to achieve the new mental outlooks that the new situation demands. There is nothing more tragic than to sleep through a revolution*"[80].

La strada è lunga.

---

[77] Cons. 71, GDPR.

[78] R. Nicolò, *Diritto civile*, in *Enc. dir.*, XII, Milano, Giuffré, 1964, p. 904.

[79] G. Sartor, *Introduzione*, in *Riv. fil. dir.*, 2020, p. 69.

[80] Martin Luther King, *Commencement Address for Oberlin College*, 1965 (testo disponible in https://www2.oberlin.edu).

7. La tutela giuridica del *software*: il caso *Top System* tra diritto di decompilazione e esigenze di conformità

Enzo Maria Incutti (Università di Roma La Sapienza)

7.1. Premessa: il caso *Top System*

Il presente studio prende spunto da una pronuncia della Corte di Giustizia dell'Unione Europea, che rappresenta l'occasione per riflettere sulla adeguatezza della tutela autoriale concessa al *software*, sui confini della autonomia privata e sulle potenziali prospettive evolutive della disciplina.

Il 6 ottobre 2021 la Quinta Sezione della Corte di Giustizia ha deciso sulla domanda di rinvio pregiudiziale promossa dalla *Cour d'appel de Bruxelles*, nell'ambito del procedimento *Top System SA* vs. *État belge* (C-13/20)[1], avente ad oggetto l'interpretazione dell'articolo 5, paragrafo 1[2], della direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore.

La controversia vedeva contrapporsi, da un lato, *Top System SA*, società di diritto belga che sviluppa programmi per elaboratore e fornisce prestazioni di servizi informatici e, dall'altro, *Selor*, l'ente pubblico belga responsabile della selezione e dell'orientamento dei collaboratori della pubblica amministrazione.

Su richiesta di *Selor*, *Top System* aveva sviluppato diverse specifiche applicazioni. Il 6 febbraio 2008 *Selor* e *Top System* avevano concluso un contratto avente ad oggetto l'installazione e la configurazione di un nuovo ambiente informatico di produzione, che, però, presentava

[1] Corte di giustizia dell'Unione Europea, 06 ottobre 2021, (causa C-13/20).

[2] «Salvo disposizioni contrattuali specifiche, non sono soggetti all'autorizzazione del titolare del diritto gli atti indicati nell'articolo 4, lettere a) e b), allorché tali atti sono necessari per un uso del programma per elaboratore conforme alla sua destinazione, da parte del legittimo acquirente, nonché per la correzione di errori».

subito dei difetti di funzionamento. Si noti a tal riguardo che Selor deteneva (e tutt'ora detiene) una licenza d'uso su tutti i programmi appositamente creati da Top System.
Il 6 luglio 2009 la Top System aveva proposto ricorso contro *Selor* e lo Stato belga dinanzi al *Tribunal de commerce de Bruxelles*, contestando l'illegittima attività di decompilazione effettuata da Selor sul programma per elaboratore e richiedendo il risarcimento dei danni per la decompilazione così effettuata.

Il 26 novembre 2009 la causa era stata rinviata dinanzi al *Tribunal de première instance de Bruxelles* che, il 19 marzo 2013, aveva dichiarato la domanda così proposta come infondata.

La *Top System* aveva, quindi, impugnato la sentenza di primo grado dinanzi al giudice del rinvio, la *Cour d'appel de Bruxelles*, sostenendo che la decompilazione possa essere effettuata solo in forza di un'autorizzazione dell'autore, o del suo avente diritto, o ancora a fini della c.d. interoperabilità - ovvero, l'interconnessione e l'interazione funzionale tra *software*.

Per contro, sulla base dell'interpretazione dell'art. 6 della Legge del 30 giugno 1994, che ha recepito nell'ordinamento belga la direttiva 91/250/CEE, *Selor* riteneva di essere legittimato a procedere alla decompilazione per correggere alcuni errori di funzionamento che rendevano impossibile un uso conforme alla destinazione del *software* e ad osservare, studiare e sperimentare il funzionamento del programma allo scopo di determinare le idee alla base delle funzionalità con l'obiettivo di prevenire le future interruzioni determinate da simili errori.

Alla luce dei presenti elementi di fatto ed avendo accertato l'avvenuta decompilazione da parte di *Selor*, la Corte d'Appello Belga aveva proposto, quindi, due differenti questioni pregiudiziali all'attenzione della Corte di Giustizia.

7.2. Alcune necessarie precisazioni in tema di decompilazione del *software*

Risulta opportuno ai fini di una corretta comprensione del fenomeno oggetto della controversia e, più in generale, del mondo informatico interessato dalla presente analisi, compiere alcune necessarie premesse.

In ambito informatico, per *software* si intende l'insieme composito del "sistema operativo" e di tutti i programmi in esso presenti[3], mentre il programma per elaboratore è una sequenza di istruzioni[4], espresse in linguaggio informatico[5] che, per effetto del caricamento in un elaboratore[6], interagendo con il sistema operativo di quest'ultimo comporta lo svolgimento di determinate attività[7].

L'altro elemento determinante è il c.d. *hardware*, ovvero l'insieme dei dispositivi fisici costituenti un sistema elaborativo e/o operativo.

Il programma per elaboratore è di regola scritto dall'uomo nel c.d. codice sorgente per essere successivamente tradotto dall'elaboratore in una sequenza di *bit*[8] che compongono il c.d. codice oggetto[9].

Per poter essere intellegibile da parte dell'elaboratore, il codice sorgente (scritto in linguaggio «umano») deve essere tradotto nel c.d. codice oggetto, un linguaggio traducibile da parte della sola macchina.

In questa fase, quindi, le istruzioni di un programma scritto in un linguaggio di programmazione (sorgente) vengono trasformate in un codice oggetto (detto anche eseguibile) suscettibile di essere caricato ed eseguito da un elaboratore e dal relativo sistema operativo.

Entrando nel merito del processo informatico interessato dal presente giudizio, è essenziale delimitare i confini del processo di decompilazione.

La c.d. decompilazione va intesa come quella attività di *reverse engineering* che consiste nella ricostruzione di un prodotto già esistente,

---

[3] Entità, quindi, ben più complessa rispetto al semplice programma che ne rappresenta solo una componente.

[4] L'istruzione è una proposizione espressa sotto forma di codice diretta ad ordinare ad un elaboratore lo svolgimento di una determinata funzione o attività.

[5] Il linguaggio è il sistema codificato di proposizioni che vengono espresse in forma di istruzioni

[6] Il c.d. caricamento, consiste in quell'attività di inserimento di un programma nella memoria di un elaboratore.

[7] Questa chiara distinzione tecnica non sembra, però, essere stata colta dal legislatore italiano che parla genericamente di programma per elaboratore, aprendo la porta a potenziali interpretazioni restrittive della disciplina. È indubbio che l'impropria restrizione terminologica non sia sinonimica di una concreta limitazione dell'ambito applicativo della normativa destinata ai *software*.

[8] Sequenza che viene espressa in forma binaria di 0 e 1.

[9] Dunque, il codice sorgente è scritto in un linguaggio di programmazione complesso ma comprensibile all'uomo (e non alla macchina); esso, infatti, deve essere tradotto dal compilatore in un linguaggio tecnico (il c.d. codice oggetto) attraverso la codificazione delle istruzioni in forma binaria.

in questo caso di un *software*. Il prodotto viene destrutturato per comprenderne l'architettura ed il suo funzionamento.

Lo scopo del *reverse engineering* in ambito *software* è quello di riprodurre il codice sorgente partendo dal codice oggetto di un programma esistente[10]. In questo modo è possibile ottimizzare il *software* correggendone gli errori di funzionamento, analizzare i programmi della concorrenza o sviluppare nuovi prodotti.

La ricostruzione di un *software* può riguardare diverse tipologie di attività, quali, a titolo esemplificativo, il recupero del codice sorgente del *software*; la comprensione delle regole di un protocollo di comunicazione; la creazione di un modello informatico; la ricerca dei c.d. *bug* nel programma; il miglioramento della compatibilità di un *software* con piattaforme e programmi di terze parti ed, anche, l'utilizzo di funzioni di piattaforme non documentate.

La decompilazione del *software* avviene di regola attraverso due specifiche modalità: a) attraverso la tradizionale decompilazione (c.d. *white box analysis*) del *software*; b) attraverso la tecnica della c.d. *black box analysis*, operazione consistente nell'osservazione del funzionamento del programma[11].

7.3.La tutela autoriale del *software*

L'esigenza di predisporre un'adeguata cornice di tutela per il *software* emerge nei primi anni '70 del secolo scorso, parallelamente all'evoluzione tecnico-informatica, trainata dai paesi occidentali [12].

[10] «La decompilazione consente, in genere, non di ottenere il codice sorgente originale, bensì una terza versione del programma di cui trattasi, denominata "quasi-codice sorgente", che potrà a sua volta essere compilata in un codice oggetto che consenta a tale programma di funzionare», così *Conclusioni Avvocato Generale, par. 41, Top System SA* vs. *État belge* (C-13/20).

[11] Molto spesso ciò avviene attraverso l'inserimento di *input* al fine di comprendere i corrispondenti *output* del programma. Questa distinzione informatica e procedurale risulta molto determinante sul piano normativo, come si vedrà più nel dettaglio successivamente.

[12] Sul punto, per un approfondimento v. L. MARTINAT e L. BOSSOTTI, *Tutela giuridica del software,* in S. VITRÒ (a cura di), *La tutela giuridica del software,* Key editore, 2022. p. 135 ss.

La ricerca di un corretto apparato normativo di tutela è stata, sin da subito, la principale e dirimente questione in materia [13]. Le due vie percorribili ma tra loro alternative – per approccio e per conseguenze - sono state individuate l'una nella tutela secondo il diritto d'autore e l'altra in quella brevettuale[14].

A prevalere con nettezza è stata la prima opzione; pertanto, la tutela del *software* è tradizionalmente inserita nella disciplina del diritto d'autore.

Le ragioni giustificative di questa scelta risiedevano nella considerazione del *software* come creazione intellettuale e erano sorrette dal timore di vedere arrestato il processo tecnologico dalle restrizioni della tutela brevettuale.

Difatti, l'applicazione della disciplina brevettuale al *software*, in qualità di invenzione tecnica, avrebbe limitato notevolmente il progresso tecnico[15] del mercato e avrebbe reso anche più complesse la commercializzazione e la diffusione dei programmi informatici a causa della rigidità del sistema dei brevetti.

Il diritto d'autore, invece, forniva - e fornisce tutt'ora - una soluzione più agevole sotto molteplici profili. Innanzitutto, si concede tutela sulla base della sola creazione del *software*, senza complesse procedure di "autorizzazione", e si agevolano così i canali distributivi e commerciali connessi ai *software*.

Con il diritto d'autore, dunque, trovano tutela sia il codice sorgente nel particolare linguaggio con cui è stato scritto dal suo autore, e nello stesso modo è tutelato anche il codice oggetto ed il relativo materiale preparatorio[16].

Non viene, invece, protetta l'idea che è alla base della creazione del *software*, permettendo di fatto che essa possa essere riutilizzata in un

---

[13] Cfr. E. AREZZO, *Tutela brevettuale e autoriale dei programmi per elaboratore. Profili e critica di una dicotomia normativa*, Giuffrè, Milano 2012; A.M. GAMBINO, *L'innovazione informatica tra brevettazione e diritto d'autore*, in *Dir. ind.*, 2010, II, p. 147 ss.; L. SCHIUMA, *Il software tra brevetto e diritto d'autore*, in *Riv. dir. civ.*, 2007, p. 683 ss.; G. DE SANTIS, *La tutela giuridica del software tra brevetto e diritto d'autore*, Giuffrè, Milano, 2000.

[14] Per una dettagliata analisi e ricostruzione storico-giuridica, v. R. PARDOLESI e M. GRANIERI, *Il software*, in *AIDA*, 2007, p. 288-312, ed anche, G. NOTO LA DIEGA, *Le idee e il muro del suono. I programmi per elaboratore nella più recente giurisprudenza europea*, in, *Europa e dir. priv.*, 2, 2013, p. 543 e ss.

[15] Si tenga in considerazione la durata ventennale della tutela brevettuale con tutte le sue correlative limitazioni e restrizioni.

[16] L. MARTINAT e L. BOSSOTTI, *op. cit.*, spec. p. 136.

numero indefinito di applicazioni a patto che venga diversamente espressa attraverso un autonomo codice sorgente[17].

Nella prospettiva del sistema brevettuale avrebbero trovato tutela anche le idee e i principi che hanno dato origine all'invenzione informatica. Ciò che, invece, rileva ai fini della disciplina autoriale è l'espressione dell'idea, resa attraverso uno specifico programma informatico[18].

Da un punto di vista legislativo, il primo intervento in questa direzione è ascrivibile al *Computer Software Copyright Act* statunitense[19] del 1980[20].

In seguito, in Europa, è stata accolta la medesima impostazione, offrendo tutela autoriale per i *software* attraverso la Direttiva 91/250/CEE[21] recepita, nel nostro ordinamento, dal D. Lgs. n. 518 del 1992.

In Italia quindi, a norma dell'art. 2, co. 1, n. 8 della legge sul diritto d'autore[22], sono protetti «i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore». Coerentemente alla *ratio* della disciplina autoriale,

---

[17] Sul punto, in giurisprudenza, v. Trib. Bari Sez. IV, 14-3-2007, in *Dir. internet*, 2007, p. 447 ss., con nota di E. PELINO.

[18] Come si legge in una importante pronuncia della Corte di Giustizia dell'UE, «[…] il vantaggio principale della tutela dei programmi per elaboratore mediante il diritto d'autore risiede nel fatto che essa concerne soltanto l'espressione individuale dell'opera e offre quindi uno spazio sufficiente a permettere ad altri autori di creare programmi simili, o perfino identici, purché essi si astengano dal copiare […]» (cfr. Corte eur. giust. grande sez., C-406/10 del 2 maggio 2012, § 41).

[19] *Computer Software Copyright Act*, L. n. 96-517, 94 Stat. 3015, 3028 (1980). Sul punto per una revisione critica, RICHARD H. STERN, *Another Look At Copyright Protection of Software: Did the 1980 Act Do Anything For Object Code?*, in *Computer L.J.*, 3, 1, 1981.

[20] Attualmente, negli Stati Uniti d'America la decompilazione dei software è fatta rientrare nella c.d. *fair use exception*, sulla base del Paragrafo 107 del Copyright Act. Si ritiene infatti, che l'utilizzo delle copie intermedie ai fini di *reverse engineering* sia pienamente legittimo anche in assenza di preventiva autorizzazione. Questa linea interpretativa sembra confermata dalla sentenza della Corte Suprema n. 18–956 del 5 aprile 2021, nel caso *Oracle* vs. *Google*.

[21] Direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore. A conferma del paradigma autoriale di tutela messo precedentemente in evidenza, il secondo paragrafo dell'art. 1 recita: «la tutela ai sensi della presente direttiva si applica a qualsiasi forma di espressione di un programma per elaboratore. Le idee e i principi alla base di qualsiasi elemento di un programma per elaboratore, compresi quelli alla base delle sue interfacce, non sono tutelati dal diritto d'autore a norma della presente direttiva».

[22] Legge, 22/04/1941 n. 633 (nel corso del presente studio, in via di semplificazione, anche l.d.a.)

restano, invece, esclusi dalla tutela accordata ai *software*, le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. È, invece, compreso nel termine «programma per elaboratore» il materiale preparatorio per la progettazione del software.

Come si vedrà in dettaglio successivamente, anche all'autore del programma per elaboratore vengono concessi diritti di utilizzazione economica (artt. 64-*bis* e ss. l.d.a.).

Sul piano internazionale, si conferma questo paradigma di tutela, come si evince dall'Accordo TRIPS[23] in aderenza a quanto già disposto dalla Convenzione di Berna.

Nello specifico, l'art. 10 sancisce, al primo paragrafo, che «i programmi per elaboratore, in codice sorgente o in codice oggetto, sono protetti come opere letterarie ai sensi della Convenzione di Berna (1971)»[24].

Anche il Trattato OMPI sul diritto d'autore (WCT)[25] si inserisce in questa linea regolatoria, affermando, all'art. 4, che i programmi per elaboratore sono tutelati secondo il diritto d'autore[26].

È utile ricordare, ai fini del presente discorso, che con il DPCM n. 244 del 3 gennaio 1994 sono state stabilite le modalità di registrazione all'interno del Registro pubblico speciale dei programmi per elaboratore, tenuto dalla S.I.A.E., tramite cui l'autore del programma può attestarne la paternità. Si tenga conto, però, il deposito all'interno del Registro non vale a costituire il momento inziale della tutela autoriale, in quanto esso coincide con la creazione stessa dell'opera informatica. Esso rileva, pertanto, ai soli fini probatori, nell'ipotesi in cui dovessero

[23] Accordo TRIPs (*Trade Related Aspects of Intellectual Property Rights*), adottato a Marrakech 15 aprile 1994 – "*Accordo relativo agli aspetti dei diritti di proprietà intellettuale attinenti al commercio*" ratificato dall'Italia con legge 29 dicembre 1994, n. 747.

[24] Al secondo paragrafo, si specifica che «le compilazioni di dati o altro materiale, in forma leggibile da una macchina o in altra forma, che a causa della selezione o della disposizione del loro contenuto costituiscono creazioni intellettuali sono protette come tali. La protezione, che non copre i dati o il materiale stesso, non pregiudica diritti d'autore eventualmente esistenti sui dati o sul materiale».

[25] Anche, più comunemente, *World Copyright Act,* adottato a Ginevra il 20 dicembre 1996.

[26] «I programmi per elaboratore sono protetti in quanto opere letterarie ai sensi dell'articolo 2 della Convenzione di Berna. Tale protezione si applica a qualsiasi modo o forma di espressione di un programma per elaboratore».

essere rivendicatati diritti di paternità sull'opera[27] o se dovessero essere presentate richieste di risarcimento per plagio.

Focalizzandosi sulla tutela autoriale, i programmi per elaboratore sono tutelati in qualsiasi forma siano espressi a condizione che siano una originale creazione intellettuale dell'autore. Come si evince dall'art. 1, co. 1, n.8 della l.d.a., la tutela predisposta per i *software* comprende anche il materiale preparatorio utile alla progettazione del programma informatico[28].

Il requisito dell'originalità per i *software*, al pari di ogni altra opera dell'ingegno, richiede che l'opera sia frutto dell'espressione creativa ed originale dell'autore, anche qualora essa sia frutto della rielaborazione di idee e concetti diffusamente condivisi nel settore di riferimento. Questo ultimo aspetto è particolarmente rilevante nell'ambito *software* in quanto la condivisione di principi informatici è fondamentale per lo sviluppo di nuovi programmi e per il progresso del mercato[29]. Laddove, invece, si dovesse applicare la disciplina brevettuale, anche le idee e i principi alla base della invenzione sarebbero protetti e, quindi, non accessibili agli altri operatori del mercato[30].

Si deve mettere in evidenza, inoltre, che al fianco dei diritti di utilizzazione economica l'autore acquisisce anche diritti morali, tra cui,

---

[27] «La registrazione, dunque, è una forma di pubblicità notizia che non produce un effetto suo proprio e autonomo ma si somma e si sovrappone a quello già prodotto dall'atto della creazione», così L. MARTINAT e L. BOSSOTTI, *op. cit.*, spec. p. 144.

[28] In tal senso, «[…] per dissipare ogni dubbio, occorre precisare che solo l'espressione di un programma per elaboratore è oggetto di tutela e che le idee e i principi alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce, non sono tutelati dal diritto d'autore a norma della presente direttiva. Conformemente a detto principio del diritto d'autore, le idee e i principi che sono alla base della logica, degli algoritmi e dei linguaggi di programmazione non sono tutelati a norma della presente direttiva. […]» (*cfr. Considerando 11, Direttiva 2009/24/CE*).

[29] Sulla tutelabilità della funzionalità di un programma per elaboratore, del linguaggio di programmazione e del formato dei file di dati utilizzati, v., in giurisprudenza, CGUE, Grande sez., C-406/10, cit.. In dottrina, v. A. GERACI, *Copia di un software e violazione del diritto d'autore: la Corte di giustizia sul caso SAS c. WP*, Dir. ind., 2012, V, 457 ss.; G. NOTO LA DIEGA, *op. cit.*

[30] In merito al requisito dell'originalità del *software*, «[…] sono tutelati dal diritto d'autore, quale risultato di creazione intellettuale, i programmi per elaboratore elettronico, intesi come un complesso di informazioni o istruzioni idonee a far eseguire al sistema informatico determinate operazioni, che siano completamente nuovi o forniscano un apporto innovativo nel settore, esprimendo soluzioni migliori o diverse da quelle preesistenti», cfr. Cass. pen., III, 16 marzo 2018, n. 30047, in *Repertorio Foro Italiano,* 2018, *Diritti d'autore*, n.° 67; in *Ced. Cass. pen*., rv. 273757 (m).

su tutti, il diritto al riconoscimento della paternità dell'opera da lui creata[31].

Volgendo, infine, lo sguardo verso il sistema brevettuale, è possibile notare che la scelta a favore di una disciplina di diritto d'autore per i *software* sembra essere confermata dalle disposizioni della Convenzione sul brevetto europeo[32] e, specificatamente, dai limiti imposti alle invenzioni brevettabili *ex* art. 52.

È importante chiarire, però, che la Direttiva 2009/24/CE[33] non ha escluso l'applicazione di altre disposizioni, anche in tema brevettuale, a patto che ciò non comporti la violazione dei diritti dell'autore del programma per elaboratore così come sanciti dal quadro normativo, nazionale ed europeo, in tema di diritto d'autore[34].

Questa netta presa di posizione del legislatore europeo lascia, per certi versi, aperto l'interrogativo sull'adeguatezza del sistema autoriale di tutela per programmi informatici così complessi ed in così notevole evoluzione. Dopotutto, l'agevole paradigma di disciplina imposto per i programmi per elaboratore, favorisce correttivi, modifiche e riutilizzazioni che se inclini ad un progresso tecnico-scientifico e rispondenti ad esigenze concorrenziali di mercato, risultano essere, parimenti, occasione di controversie circa la titolarità dei diritti di utilizzazione economica ed il loro legittimo esercizio.

Non a caso, unitamente alla disciplina sulle banche dati, la tutela del *software* è stata saggiamente definita come «la «più dirompente espressione dello "sconfinamento" del diritto d'autore contemporaneo»[35].

---

[31] Questi sono diritti inalienabili, imprescrittibili e irrinunciabili che si acquistano in modo automatico con la creazione dell'opera dell'ingegno.

[32] Conclusa a Monaco il 5 ottobre 1973 e riveduta a Monaco il 29 novembre 2000.

[33] Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009 relativa alla tutela giuridica dei programmi per elaboratore.

[34] Al considerando 16 della Direttiva si legge, infatti, che «la tutela dei programmi per elaboratore a norma delle leggi sul diritto d'autore non deve pregiudicare l'applicazione, in casi opportuni, di altre forme di tutela; tuttavia qualsiasi disposizione contrattuale non conforme alle disposizioni della presente direttiva riguardanti la decompilazione o alle eccezioni di cui alla presente direttiva relative alla possibilità di fare una copia di riserva o all'osservazione, studio o sperimentazione del funzionamento di un programma dovrebbe essere considerata nulla». Come ribadito, inoltre, dall'art. 8 della Direttiva, «le disposizioni della presente direttiva non ostano all'applicazione di altre eventuali disposizioni giuridiche come quelle in materia di diritti brevettuali […]».

[35] G. GHIDINI, *Profili evolutivi del diritto industriale. Innovazione - Concorrenza – Benessere dei consumatori - Accesso alle informazioni*, II ed., Giuffrè, Milano, 2008, spec. p. 193.

7.4. Il diritto di decompilazione

Come anticipato ed in modo speculare alle altre ipotesi di opere dell'ingegno, anche nel caso del *software*, l'autore diviene titolare di specifici diritti di utilizzazione economica[36].

In virtù dell'art. 64-*bis* della l.d.a., all'autore del *software* spettano i diritti di: a) riproduzione, permanente o temporanea, totale o parziale, con qualsiasi mezzo o in qualsiasi forma; b) traduzione, adattamento, trasformazione, modificazione nonché il diritto di riproduzione dell'opera, senza che ciò arrechi pregiudizio dei diritti di chi modifica il programma; c) distribuzione, in qualsiasi forma.

Al fianco, però, dell'autore del programma per elaboratore esistono diversi soggetti che possono legittimamente disporre di una copia del *software*, solitamente a seguito della conclusione di specifici contratti di cessione o di licenza d'uso[37].

---

[36] Tutelati, da un punto di vista processuale, dagli artt. 156 e ss. della l.d.a.

[37] Con il contratto di cessione di *software*, l'acquirente diviene titolare di tutti i diritti patrimoniali connessi al programma (e quindi, anche del codice sorgente), mentre nel caso di contratto di licenza d'uso, l'autore del *software* rimane titolare dei diritti di utilizzazione economica ma concede al licenziatario di poterne godere nei limiti delle condizioni contrattuali. Le licenze sono contratti atipici che possono assumere diverse connotazioni a seconda della tipologia del *software* e dei soggetti coinvolti. A titolo esemplificativo, esse possono comprendere tutti i diritti economici o soltanto una parte di esse, possono essere limitate territorialmente o possono essere concesse in esclusiva. Una delle licenze più diffuse nel mercato digitale, è la c.d. *End-User License Agreement* (EULA), con cui l'utente finale ha la possibilità di esercitare il diritto d'uso del *software* nei limiti espressi dalla licenza. Essa può essere perpetua, dietro il pagamento di una somma unica, o a durata, in cui è previsto il versamento di un canone periodico. Sul punto, v. L. MARTINAT e L. BOSSOTTI, *op. cit.*, p. 160 e ss. Altra ipotesi particolare è quella della licenza c.d. *click-through* che non consente all'utente di accettare i termini della licenza prima dell'accesso al *software*. A tal proposito, bisogna ricordare che per fronteggiare l'improprio utilizzo delle suddette licenze, spesso lesive dei diritti dell'utente, negli Stati Uniti sin dal 1998, con il *Digital Millenium Copyright Act* (DMCA), si è cercato di porre un argine legislativo e limitare il fenomeno. Per una primissima disamina sul punto, v. G. L. FOUNDS, *Shrinkwrap and Clickwrap Agreements: 2B or Not 2B*?, in *Federal Communications Law Journal*, vol. 52, 1, 1999, p. 99 e ss. Come ricordato anche in giurisprudenza, « accanto al modello di licenza tradizionale, che prevede il pagamento di un corrispettivo a fronte della concessione del diritto d'uso, si sono imposti, nel mondo dell'informatica, schemi negoziali alternativi, i quali consentono all'utilizzatore del programma di avere una disponibilità completa sul codice sorgente e d'impiegare il software anche senza corrispettivo», così Corte cost., 26 marzo 2010, in *Foro it*., n. 122, 2010, 1, X, p. 2650 ss.

Le disposizioni contrattuali, diversamente formulate, redistribuiscono, dunque, i diritti di utilizzazione economica così come predisposti dalla l.d.a. In questo, si erge la funzione "riequilibratrice" della autonomia privata che rappresenta il principale strumento tramite cui modellare le esigenze concorrenziali del mercato e gli interessi degli operatori coinvolti al paradigma normativo costruito sulle trame della l.d.a.

Nell'ambito della cornice legislativa ora in analisi ed a norma del primo comma dell'art. 64-*ter* l.d.a., l'utente legittimo ha il diritto di riprodurre, tradurre, adattare e modificare il *software*, «allorché tali attività sono necessarie per l'uso del programma per elaboratore conformemente alla sua destinazione da parte del legittimo acquirente, inclusa la correzione degli errori».

Il secondo comma, invece, concede all'utente legittimo di «effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso». Non è ammessa la possibilità di pattuizioni contrarie, a pena di nullità, diversamente da quanto sancito nel primo comma, in cui, invece, non si escludono le eventuali differenti previsioni contrattuali.

La copia di riserva non legittima l'utente a realizzare più copie private del programma, ma semplicemente ad utilizzare una copia di riserva in caso di malfunzionamento o di errori procedurali. La copia privata, ovviamente, deve rimanere nella disponibilità dell'autore del programma per elaboratore e non può essere venduta a terzi.

Ai fini del presente studio, estremamente rilevante risulta essere quanto previsto dal comma terzo dell'art. 64-*ter* l.d.a.

Infatti, l'utente legittimo può, anche senza l'autorizzazione del titolare dei diritti, «osservare, studiare o sottoporre a prova il funzionamento del programma, allo scopo di determinare le idee ed i princìpi su cui è basato ogni elemento del programma stesso».

Questa attività di decompilazione, la c.d. *black box analysis*, è ammessa qualora venga compiuta nell'ambito di operazioni di caricamento, visualizzazione, esecuzione, trasmissione o memorizzazione[38].

[38] In merito, v. G. NOTO LA DIEGA, *op. cit.* spec. p. 543 e ss. L'Autore correttamente mette in evidenza che «occorre precisare che: a) non è vietato il reverse engineering, ma solo quella sua *species* nota come decompilazione; b) non si tratta di un divieto, ma di un'attività consentita a determinate condizioni; c) quelli in discorso sono limiti imposti dal fondamento stesso della c.d. proprietà intellettuale, cioè dalla necessità di compensare gli investimenti, in pari tempo incentivando l'innovazione».

Al pari del secondo comma, le clausole contrattuali pattuite in violazione di quanto disposto nel terzo comma sono nulle.

In via generale, quindi, l'attività di decompilazione non è sempre ammessa, se non nei limiti previsti dalla legge e limitatamente alla tipologia della c.d. *black-box analysis.*

La previsione di nullità è volta a rafforzare il progresso tecnologico in ambito *software*, conformemente all'idea di fondo della tutela autoriale: proteggere l'espressione creativa ed originale ma non le idee ed i principi ad essa correlati [39].

Si tenga, infine, conto che l'attività di decompilazione, oltre alle limitazioni legislative e contrattuali, incontra anche notevoli costi e complesse operazioni tecniche che, di fatto, attribuiscono un livello ulteriore ed implicito di tutela per il codice sorgente [40].

7.5. Le soluzioni proposte dalla Corte di Giustizia nel caso *Top System*

Ritornando sulle tracce della pronuncia in esame, è utile ripercorre le argomentazioni a sostegno delle soluzioni proposte, al fine di vagliarne l'adeguatezza nell'ottica di una più generale ricalibrazione della tutela del *software*.

In merito alla prima questione, ci si domanda se l'articolo 5, paragrafo 1, della direttiva 91/250 (*Deroghe relative alle attività riservate*)[41]

[39] Sul punto, v. L. MARTINAT e L. BOSSOTTI, *op. cit.,* p. 154-155.

[40] In questi termini, v. R. PARDOLESI e M. GRANIERI, *op. cit.,* spec. p. 303 (cfr. «[…] il codice diviene inespugnabile, sia fisicamente, sia dal punto di vista economico, nella misura in cui il reverse engineering sui circuiti e la decompilazione divengono attività dispendiose e con non adeguate percuentuali di successo»).

[41] «Salvo disposizioni contrattuali specifiche, non sono soggetti all'autorizzazione del titolare del diritto gli atti indicati nell'articolo 4, lettere a) e b), allorché tali atti sono necessari per un uso del programma per elaboratore conforme alla sua destinazione, da parte del legittimo acquirente, nonché per la correzione di errori».

Le attività dell'articolo 4 che vengono richiamate sono «a) la riproduzione, permanente o temporanea, totale o parziale di un programma per elaboratore con qualsivoglia mezzo, in qualsivoglia forma. Nella misura in cui operazioni come il caricamento, la visualizzazione, l'esecuzione, la trasmissione o la memorizzazione del programma per elaboratore richiedono una riproduzione, tali operazioni devono essere sottoposte ad autorizzazione da parte del titolare del diritto ; b) la traduzione, l'adattamento, l'adeguamento e ogni altra modifica di un programma per elaboratore e la riproduzione

debba essere interpretato nel senso che il legittimo acquirente di un programma per elaboratore ha il diritto di procedere alla decompilazione di tutto o parte di esso al fine di correggere errori che incidono sul funzionamento di tale programma, anche quando la correzione consista nel disattivare una funzione che pregiudica il buon funzionamento dell'applicazione di cui fa parte detto programma.

A tal riguardo, la Corte ricorda che la decompilazione di un *software* è una attività di *reverse engineering* che consiste nella ricostruzione del codice sorgente partendo da un codice oggetto di un programma esistente. Attraverso la decompilazione, di regola, si ottiene un "quasi codice sorgente", non perfettamente corrispondente al codice sorgente originale. L'attività di *reverse engineering* rappresenta il contraltare, in ambito *software*, della c.d. compilazione, attività che attiene, invece, al processo di creazione del codice oggetto sulla base delle istruzioni contenute nel codice sorgente[42].

Siccome la decompilazione non è testualmente ricompresa tra gli atti disciplinati dall'art. 4 lett. a) e b) della direttiva, ai quali fa riferimento l'art. 5 par. 1, la Corte, nelle sue ricostruzioni, pone l'interrogativo sulla possibilità di estendere tale disciplina anche agli atti di decompilazione.

La decompilazione costituisce un'operazione di trasformazione della forma del codice di un programma che implica una riproduzione, almeno parziale e provvisoria, di tale codice, nonché una traduzione della forma di quest'ultimo.

A tal riguardo, la Corte sostiene che il legittimo acquirente di un programma non solo ha il diritto di decompilazione ai fini di interoperabilità a norma dell'art. 6 della direttiva, ma ha anche il diritto di decompilazione nel caso in cui ciò sia necessario per risolvere errori che incidono sul buon funzionamento del *software*, come previsto dall'art. 5, par. 1[43].

---

del programma che ne risulti, fatti salvi i diritti della persona che modifica il programma».

[42] «[…] la «decompilazione» è diretta a ricostituire il codice sorgente di un programma a partire dal suo codice oggetto. La decompilazione è effettuata mediante un programma denominato «decompilatore», cfr. CGUE, C-13/20, cit., § 37.

[43] La Corte ribadisce che sia il codice sorgente sia il codice oggetto trovano tutela autoriale, come peraltro già dichiarato in un'altra sentenza (Terza Sezione) del 22 dicembre 2010, *Bezpečnostní softwarová asociace - Svaz softwarové ochrany* contro *Ministerstvo kultury* (C-393/09).

Queste due ultime disposizioni hanno, però, finalità differenti, in quanto, mentre l'art. 6[44] riguarda gli atti necessari a garantire l'interoperabilità di programmi creati autonomamente, l'art. 5, par. 1 mira a consentire al legittimo acquirente di un programma di farne un uso conforme alla sua destinazione.

Dunque, l'articolo 5, paragrafo 1 della direttiva 91/250 deve essere interpretato nel senso che il legittimo acquirente di un programma per elaboratore ha il diritto di procedere alla decompilazione di tutto o parte di esso al fine di correggere errori che incidono sul funzionamento di tale programma, anche quando la correzione consiste nel disattivare una funzione che pregiudica il buon funzionamento dell'applicazione di cui fa parte detto programma.

In merito, invece, alla seconda questione (ovvero, se il legittimo acquirente di un programma per elaboratore che intenda procedere alla decompilazione al fine di correggere gli errori che incidono sul suo funzionamento debba soddisfare i requisiti previsti all'articolo 6 della direttiva), la Corte chiarisce i confini ed i presupposti dell'attività di decompilazione *ex* art. 5.

Nella ricostruzione della Corte, il compimento degli atti di decompilazione di un programma è soggetto a determinati requisiti, a norma dell'art. 5, par. 1.

La decompilazione, infatti, deve essere necessaria per la correzione di errori e per consentire al legittimo acquirente un uso conforme alla destinazione del programma. Inoltre, la rettifica degli errori secondo il modello dell'art. 5 deve rispettare le specifiche previsioni contrattuali che non possono in ogni modo vietare simili atti di correzione. Infine il legittimo acquirente non può utilizzare il risultato della decompilazione per fini diversi dalla correzione di errori di funzionamento.

Pertanto, come si legge nella sentenza, il legittimo acquirente che intenda procedere alla decompilazione al fine di correggere errori di funzionamento del *software* potrà agire soltanto nella misura necessaria a tale correzione e nel rispetto, se del caso, delle condizioni contrattualmente previste con il titolare del diritto d'autore su detto

[44] «Per gli atti di riproduzione del codice e di traduzione della sua forma ai sensi dell'articolo 4, lettere a) e b), non è necessaria l'autorizzazione del titolare dei diritti qualora ,l'esecuzione di tali atti al fine di modificare la forma del codice sia indispensabile per ottenere le informazioni necessarie per conseguire l'interoperabilità con altri programmi di un programma per elaboratore creato autonomamente», nel rispetto di specifiche condizioni dettate nell'art. 6 della direttiva.

programma, non dovendo, però rispettare i requisiti dettati dall'art. 6 della direttiva.

Nella prima e, soprattutto, nella seconda soluzione interpretativa emerge quale elemento di valutazione il giudizio di "conformità dell'uso" alla destinazione economica del programma[45].

Infatti, l'attività di decompilazione deve essere funzionale ad un uso conforme e legittimo del codice in analisi, nel rispetto di quanto previsto contrattualmente.

Il confine della legittimità di una specifica attività sembrerebbe, quindi, essere segnato dalla conformità di quell'atto al regolamento contrattuale ed alla destinazione economica ivi esplicitata.

In questo, si evince la centralità dell'autonomia privata che, di fatto, può estendere o restringere le maglie di accesso alle idee ed ai funzionamenti di base dei programmi per elaboratore, ricalibrando notevolmente l'assetto della tutela autoriale.

Parallelamente a ciò, dalla lettura della presente pronuncia, sembra emergere una chiara tendenza della CGUE favorevole alla condivisione delle idee e incline a realizzare un mercato europeo dei *software* aperto, accessibile e altamente concorrenziale[46].

7.6. Il *software* come "bene immateriale": quale tutela più adeguata?

L'annosa – e forse mai risolta - questione dell'individuazione della più adeguata tutela per i *software* ritorna con vigore alla luce delle grandi trasformazioni del mercato digitale.

---

[45] Riecheggia, indirettamente, la formulazione, in tema di usufrutto, dell'art. 981 cod. civ., laddove si prescrive «l'obbligo di non mutare la destinazione economica» in capo all'usufruttario. Continuando in questo tentativo di assimilazione si dovrebbe immaginare, allora, che il mancato rispetto della destinazione economica del *software*, farebbe venir meno il diritto dell'utente legittimo di compiere attività di decompilazione, nel rispetto della l.d.a.

[46] Sulla tendenza a proteggere un nucleo centrale di idee e principi non soggetti ad atti appropriativi o a diritti proprietari, v. su tutti, C. HESS e E. OSTROM (a cura di), *Understanding Knowledge as a Commons*. *From Theory to Practice*, MIT press, Cambridge, 2007; ma anche, G. RESTA, G. RESTA, *The Case against the Privatization of Knowledge: Some Thoughts on the Myriad Genetics Controversy, Biotech Innovations and Fundamental Right,* in *Biotech Innovations and Fundamental Rights*, a cura di R. Bin, S. Lorenzon e N. Lucchi, Springer, 2012, p. 11-36

Aspetto centrale della questione è l'evidente disallineamento tra la natura dell'oggetto di tutela (il *software,* quale invenzione informatica priva di materialità) e la disciplina autoriale di riferimento[47].

Questa distanza tra l'immaterialità del bene e la circoscrizione della tutela all'espressione creativa, sembrerebbe essere rimarcata laddove si dovesse ritenere esistente l'esigenza che il programma protetto fornisca soluzioni concrete e migliorative dello stato della tecnica[48].

Nell'attuale conformazione della tutela del *software* un conto è l'idea, altro è la sua espressione. Solo la seconda trova tutela nella l.d.a., mentre la prima rimane liberamente accessibile, rappresentando di fatto lo strumento tramite cui migliorare ed adattare il processo informatico.

Il binomio idea – espressione rispecchia la tradizionale distinzione *corpus mysticum* e *corpus mechanicum* che nel mondo virtuale e dei beni immateriali tende a scomparire [49]. Difatti, il *software,* seppur operante su sistemi materiali come gli *hardware,* rimane una creazione tecnico-informatica priva di un supporto fisico[50] che esteriorizzi l'espressione di quella idea.

Non bisogna, però, cadere nell'errore di una graduale assimilazione dei due concetti[51] poiché, in questo caso, il rischio sarebbe quello di vedere eccessivamente ampliato l'ambito applicativo della disciplina [52] , tutelando aspetti ed elementi che andrebbero, piuttosto,

---

[47] Cfr. G. NOTO LA DIEGA, *op. cit.* p. 560 e ss.

[48] «[…] l'evocata riemersione della natura è tangibile là dove si richiama la necessità che i programmi costituiscano soluzioni in grado di migliorare lo stato della tecnica, principio proprio della tradizione brevettuale, ma il cui richiamo in sede autoriale è, se non altro, inusitato», *ivi,* p. 3 e ss.

[49] Si rimanda alla tradizionale distinzione tra una creazione intellettuale in quanto idea (il c.d. *corpus mysticum*) e una opera dell'ingegno che si estrinseca in un supporto materiale (il c.d. *corpus mechanicum*). La digitalizzazione ha, difatti, spezzato il legame tra la dimensione immateriale e quella materiale dell'opera dell'ingegno: da un lato, infatti, può essere facilmente trasferita su qualsiasi supporto fisico, dall'altro, non necessita più, ai fini della sua circolazione del *corpus mechanicum*, potendo essere distribuita attraverso gli strumenti del Web che ne aumentano la capacità di fruizione simultanea.

[50] A meno che esso non venga caricato su un CD-rom o su altro dispositivo mobile.

[51] A favore di questa posizione, v. P. A. FRASSI, *Creazioni utili e diritto d'autore. Programmi per elaboratore e raccolte di dati*, Giuffrè, Milano, 1997.

[52] Sui delicati limiti del concetto di originalità del software in relazione al binomio ide e espressione, v. V. MOSCON, *Diritto d'autore e protezione del software: l'irrisolta questione dell'originalità*, in *Dir. internet*, IV, 2007, p. 350 ss.

inseriti in quel «*retroterra non proprietario*» [53], ovvero quel vasto patrimonio di idee, conoscenze e informazioni liberamente accessibili e sottratte a qualsivoglia forma di personale appropriazione, in quanto condizione essenziale per la creatività futura dell'intera collettività.

Si deve, inoltre, considerare che tassello centrale in questo complesso puzzle è costituito dalla tradizionale predisposizione del mondo digitale ed informatico a favore di processi accessibili e di dati liberamente condivisi[54]. Non a caso lo spazio lasciato all'autonomia privata dalla l.d.a. è abbastanza ampio, con il limite invalicabile del divieto di monopolizzazione delle idee e dei principi[55].

Ed allora, tra la via autoriale, che pone tuttora gli interrogativi anzidetti[56], e la scelta altamente protezionistica e restrittiva del brevetto, potrebbe stagliarsi una terza soluzione intermedia[57]. Si potrebbe, difatti, valutare l'opportunità di una ulteriore e più approfondita ricalibrazione della disciplina autoriale del *software,* implementando regole che aderiscano maggiormente alla natura immateriale del bene ed alle tendenze del mercato dei programmi per elaboratore.

---

[53] Stefano Rodotà elabora questa espressione particolarmente colorita e significativa, nel contesto di una più generale rivalutazione del rapporto beni pubblici-beni privati, in *Il terribile diritto. Studi sulla proprietà privata*, II ed., Il Mulino, Bologna, 1990.

[54] Si pensi al ruolo dei c.d. *open-source software* che rappresentano una soluzione comune in materia e sarebbero del tutto estranei ad una disciplina protezionistica come quella brevettuale. Sul punto, v. F. MARABINI, *La tutela giuridica del "software" e l'"open source"*, in *Ciberspazio e diritto*, 2017, 2, p. 405-422; C. PIANA e S. ALIPRANDI, *Il Free and Open Source software nell'ordinamento italiano: principali problematiche giuridiche*, in *Informatica e diritto*, 2012, 1, p. 79-96; A. ROSSATO, *Diritto e architettura nello spazio digitale. Il ruolo del software libero*, Padova, CEDAM, 2006; E. LOFFREDO, *Open source e appartenenza del software*, in *AIDA*, 2004, 67.

[55] «[…] l'autonomia privata incontra limiti stringenti imposti dalla esigenza di evitare che possano essere monopolizzate le idee», così G. NOTO LA DIEGA, *op. cit.,* spec. p. 559 e ss.

[56] «D'altro canto, il diritto d'autore come strumento di protezione del software continua a mostrare il fianco alle debolezze tipiche di quella forma di protezione e alla pericolosità insita nel riconoscimento automatico della protezione», così R. PARDOLESI e M. GRANIERI, *op. cit.,* spec. p. 303.

[57] Come già si metteva in evidenza in dottrina, circa la soluzione regolatoria più opportuna, bisogna «o denervare, a tutto campo e sino in fondo, quel che resta della già scossa matrice del diritto d'autore. Oppure ricavare al suo interno regole specificamente conformate alla natura adespota del software: opzione, quest'ultima, resa nella sostanza indisponibile dall'isteresi di scelte internazionali difficilmente riplasmabili nel breve periodo». così R. PARDOLESI, *«Software», property rights» e diritto d'autore: il ritorno dal paese delle meraviglie*, in *Foro it*., 1987, 3, II, p. 289 e ss, spec. p. 300.

In campo software, si enfatizza la tensione tra le spinte verso l'innovazione e il modello privatistico di tutela dei diritti di proprietà intellettuale[58].

In questa tensione, sembra poter essere leso «quell'equilibrio originario tra le prospettive di breve periodo (riguardanti appunto la protezione accordata agli inventori ed ai creatori) e quelle di lungo periodo (in termini di incentivo al progresso e alla promozione della cultura a beneficio dell'umanità) che, in definitiva, è alla base dell'*intellectual property*»[59].

Una disciplina speciale per un bene (immateriale) speciale sembra poter essere una – valida - soluzione di compromesso tra le contrapposte istanze.

7.7. L'esigenza di conformità tra progresso scientifico ed esigenze contrattuali: riflessioni conclusive

La pronuncia qui in esame ha messo in evidenza peculiari aspetti della tutela giuridica del software.

È evidente che, data la specificità del bene tutelato, la disciplina autoriale subisca – anche involontariamente – un riadattamento che fa leva sulla funzione di equilibrio dell'autonomia privata.

Infatti, nel caso di specie, l'esigenza di conformità dell'uso del programma alla sua destinazione economica riflette l'incidenza delle clausole contrattuali sulle necessità tecniche di studio e di analisi.

Per questa ragione, interviene la l.d.a. sanzionando con la nullità i patti che impediscano legittime attività di decompilazione dell'utente legittimo, al fine di studiare il funzionamento del *software* e di correggere eventuali errori.

Dunque, da un lato esigenze contrattuali, dall'altro istanze di tipo tecnico-informatico e di progresso scientifico.

---

[58] Sul tema dell'accesso a dati ed informazioni comuni in ambito digitale, v. *ex multis,* G. GHIDINI, *Evoluzioni del diritto d'autore e promozione di informazione e cultura. Nuove luci e nuove ombre,* in *Scenari e prospettive del del diritto d'autore*, a cura di A.M. Gambino e V. Falce, Art ,Roma, 2009.

[59] A. IANNARELLI, *"Proprietà", "immateriale", "atipicità": i nuovi scenari di tutela,* in G. RESTA (a cura di), Diritti esclusivi e nuovi beni immateriali, Utet, 2011, spec. p. 166.

Il diritto, per sua stessa attitudine, ricerca costantemente nuove vie da percorrere, per trovare le soluzioni più adeguate alla realtà da regolare.

Il diritto d'autore, in particolare, ha da sempre risentito dello sviluppo delle nuove tecnologie. Il fenomeno nel suo complesso ha originato nuovi interrogativi, dovuti alla difficoltà di recepire il cambiamento e di porre un limite al dilagare delle ipotesi di elusione o violazione del sistema di diritto d'autore nel contesto virtuale.

Si è, dunque, imposta una politica legislativa europea orientata ad un sistema uniforme, attraverso la creazione di un mercato unico digitale che possa permettere un più alto tasso di efficienza ed adeguatezza delle regole ed un rilevante grado concorrenziale.

Allo stesso tempo, però, il diritto d'autore avrebbe il dovere rispondere alla sua seconda indole intrinseca, ovvero la sua tendenza a promuovere lo sviluppo culturale e scientifico, attraverso la creazione di un sistema il più possibilmente inclusivo che sia capace di cogliere appieno le nuove forme di business e le innovative attività del mondo digitale.

Il modello strettamente patrimonialista e volontaristico di concedere tutela all'opere del proprio ingegno, soprattutto in relazione alla sua utilizzazione economica, sembra non rispondere più perfettamente alle mutate caratteristiche della realtà digitale.[60]

Alla luce di queste considerazioni, appare ancor più complesso considerare come appetibile la scelta brevettuale di tutela per il *software*. Essa, infatti, rappresenterebbe un "aggravamento" delle restrizioni ad ora previste, impedendo al mercato dei programmi per elaboratore di evolversi liberamente, costituendo monopoli sulle idee e i principi informatici.

Di certo, ciò non significa che la soluzione di diritto d'autore non possa essere corretta ed integrata. L'esistenza di una soluzione più restrittiva ed inadatta non legittima il legislatore ad una statica e passiva ricerca di alternative migliorative.

---

[60] Si discute ampiamente su forme di remunerazione alternative, su base strettamente morale e fondata sui rapporti interpersonali tra i soggetti del mondo digitale. (cfr. A. MUSSO, *Grounds of Protection: How Far Does The Incentive Paradigm Carry?,* in A.OHLY (a cura di), *Common Principles of European Intellectual Property Law,* Tübingen : Mohr Siebeck, 2012, spec. p. 33 e ss).

8. *Platform economy* e responsabilità delle piattaforme di intermediazione

Silvia Martinelli (Università di Torino)

8.1. Introduzione

Informatica e Internet hanno profondamente mutato i modi in cui nella nostra società sono create, trasmesse e conservate le informazioni. Trasformazione digitale e rivoluzione dell'informazione[1] sono espressioni ormai di uso comune che descrivono il cambiamento in atto.

Dopo una prima fase nella quale le interazioni online riguardavano essenzialmente la trasmissione di conoscenza tra piccole comunità di persone e la pubblicazione di informazioni su siti web personali, hanno iniziato a diffondersi alcune grandi piattaforme in grado di radunare utenti in quantità molto elevate traendo da essi valore economico. Mediante modelli di business differenti queste piattaforme riescono a estrarre valore dalle informazioni che gli utenti pubblicano e dalle interazioni che tra di essi si svolgono all'interno della piattaforma stessa.

Vengono definite "multi-sided platform", valorizzando una loro peculiare caratteristica: il favorire l'incontro e l'interazione tra due o più categorie di utenti. Nel presente scritto ci si concentrerà, in particolare, sulle piattaforme di intermediazione, come meglio definite nel paragrafo seguente, ovvero quelle piattaforme che mettono in connessione almeno due gruppi di utenti affinché essi scambino beni o servizi tra di loro.

Tali piattaforme presentano caratteristiche comuni ai social network, consentendo di creare profili individuali, di creare connessioni

[1] Floridi, *The Fourth Revolution. On the Impact of Information and Communication Technologies*.

tra i profili e di cercare nuove connessioni, che la piattaforma traccia e gestisce[2].

Sono modelli di business che si fondano sulla creazione della connessione e dello scambio. Geoffrey G. Parket, Marshall W. Van Alstyne e Sangeet Paul Choudary[3], descrivono la piattaforma come un "business based on enabling value-creating interactions", un nuovo modello di business che utilizza la tecnologia per connettere persone, organizzazioni e risorse "in a interactive ecosystem in which amazing amount of value can be created and exchanged". Differenti gruppi di utenti entrano in connessione grazie alle possibilità offerte dalla piattaforma "into a variable set of relationship": "some of them are producers, some of them are consumers, and some of them may play both roles at various times" e, nel processo, scambiano, consumano e talvolta creano "something of value".

Si tratta di modelli che abilitano nuove forme di comunicazione e interazione, in tal modo anche cambiando le forme organizzative della produzione e dello scambio. Viene eliminata la catena di produzione lineare per sostituirla con un modello più flessibile, in cui i *traditional gatekeepers* sono sostituiti dai segnali provenienti direttamente dai consumatori, mediante gli acquisti e i feedback. La piattaforma, inoltre, in genere non possiede i "physical asset", ma si limita ad organizzarli: "Airbnb doesn't own any rooms".

La piattaforma non si limita al coordinamento di un'attività di distribuzione, ma sposta il focus del business dalle attività interne a quelle esterne, organizzando persone, risorse e funzioni che esistono al di fuori di essa: "platform invert the firm", "managing external assets the firm doesn't direct control"[4]. Al contempo, sfruttando i network effects e agendo come "network orchestrator", la piattaforma trasforma "the value of communities into the value of a firm", ovvero estrae valore dalla comunità di utenti per sé stessa, trasformando gli utenti in una fondamentale risorsa.

Al centro del modello di business vi è quella che Parket, Van Alstyne e Choudary definiscono "core interaction" (ad esempio, per Facebook l'aggiornamento dello stato, su Youtube il caricamento di video, etc.), che è caratterizzata da tre componenti: participants, value

[2] Cfr. Katz, *Regulating the Sharing Economy*.

[3] Parker, Van Alstyne, e Choudary, *Platform Revolution. How networked markets are transforming the economy and how to make them work for you*.

[4] Ibidem.

unit (il valore che si crea con l'interazione), filter (ovvero l'algoritmo). La combinazione di più forme di interazione attrae più utenti nella medesima piattaforma e la partecipazione di più utenti consente di incrementare l'utilità del servizio complessivo, del valore creato, dei dati raccolti e, quindi, anche il miglioramento dell'algoritmo, del match e del modello di business stesso.

La nuova forma organizzativa è abilitata dalla tecnologia e dall'utilizzo di un'infrastruttura tecnologica nella quale gli utenti sono messi in relazione sfruttando dati e algoritmi. Ming Zeng[5], nel descrivere il modello di business di Alibaba, denomina come "smart business" questi nuovi modi di organizzazione produttiva e di creazione di valore, evidenziandone due elementi che li caratterizzano: la "network coordination" e la "data intelligence". Con la prima, si riferisce alla "scomposizione di complesse attività di business in modo che gruppi di persone o aziende possano eseguirle con più efficacia", ovvero alla possibilità, tramite la tecnologia, di coordinare in modo più facile, attraverso le connessioni online, funzioni che storicamente erano isolate in strutture integrate verticalmente o in rigide filiere. Per "data intelligence", intende la combinazione di dati, algoritmi e servizi flessibili, ovvero la capacità di gestire efficacemente prodotti e servizi in base alle attività e alla risposta dei consumatori, mediante analisi con *machine learning* di un costante flusso di dati derivante da interazioni e processi online in tempo reale. La struttura lineare tradizionale viene sostituita da una rete coordinata in modo decentrato, i cui imperativi fondamentali sono: scalabilità, costi, velocità e personalizzazione.

Il nuovo mezzo comunicativo e la nuova forma organizzativa da esso abilitata modificano, quindi, lo scambio e la produzione di beni e servizi, ma al contempo modificano anche i beni e servizi stessi.

Porter e Heppelmann[6] individuano tre stadi della rivoluzione digitale: il primo ha portato all'automazione delle attività e dei processi di business standardizzati, il secondo ha riguardato le catene di approvvigionamento, mentre il terzo ha investito lo stesso prodotto. Lo "smart product" è definito come il prodotto che coinvolge una parte fisica, una parte "smart", composta di dati e software, e la connettività e necessità di una "piattaforma" per lo scambio di dati e il loro utilizzo. I dati raccolti consentono di monitorare, controllare e ottimizzare il

[5] Zeng, *Smart Business. I segreti del successo di Alibaba*.

[6] Porter e Heppelmann, *How Smart, Connected Products Are Transforming Competition*; Porter e Heppelmann, *How Smart, Connected Products Are Transforming Companies*.

prodotto, anche in modo autonomo, e sono, quindi, essi il fulcro della trasformazione, che dal prodotto va ad investire anche la creazione di valore, la "value chain" e le "companies".

Le caratteristiche evidenziate sottolineano le peculiarità e l'innovatività di questi nuovi modelli e suggeriscono una più approfondita analisi sui ruoli e le funzioni che tali soggetti svolgono, per poi delineare le responsabilità ad esse attribuibili, in prospettiva *de iure condito* e *de iure condendo*.

8.2. *Sharing economy, platform economy, collaborative economy*: aspetti definitori

Sharing economy, economia della condivisione, collaborative economy, platform economy, *gig economy*, piattaforme, intermediari online, sono espressioni che capita sempre più frequentemente di sentire e che vengono variamente usate nel tentativo di descrivere e inquadrare il fenomeno che si sta diffondendo.

Ai fini dell'analisi occorre, in primo luogo, intendersi su cosa si intenda per "piattaforme di intermediazione" e "platform economy", per circoscrivere l'ambito di indagine e di analisi. Tra le molte espressioni utilizzate per definire le piattaforme che svolgono la funzione di favorire l'incontro di domanda e offerta di beni o servizi, si ritiene preferibile utilizzare l'espressione "piattaforme di intermediazione", intendendo per tali le piattaforme volte allo scambio di beni o servizi tra gli utenti[7].

Le piattaforme di intermediazione rientrano nella più ampia categoria delle cosiddette "online platform", che ricomprende le piattaforme di intermediazione, i *social networks*, ma anche tutte le piattaforme, create per i fini più vari, che si rivolgono a un singolo ed omogeneo gruppo di utenti, come ad esempio le comuni piattaforme di e-commerce[8].

---

[7] Non saranno oggetto della presente analisi attività quali i servizi di mero advertisement offerti dai social network, bensì soltanto quelle attività volte alla conclusione dello scambio tra utente e utente. Nel caso dei servizi pubblicitari, infatti, generalmente i due gruppi di utenti sono entrambi fruitori di un servizio fornito dalla piattaforma e non vengono messi nella condizione di concludere, tra loro, accordi. Saranno, inoltre, escluse, ai fini del presente lavoro, le piattaforme volte alle interazioni tra utenti che non sono volte alla modificazione di rapporti giuridici patrimoniali.

[8] In senso contrario la definizione utilizzata dalla Commissione europea ai fini dell'indagine pubblica sulle "online platform", nella quale è stata fornita una definizione che

L'espressione "online platforms" o "piattaforme online" è stata adottata dalla Commissione europea in alcune sue comunicazioni e proposte. In particolare, nella Comunicazione "Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa"[9] la Commissione, pur senza fornire una definizione, le esemplifica come segue: "piattaforme pubblicitarie online, mercati, motori di ricerca, social media e punti vendita di contenuti creativi, piattaforme di distribuzione di applicazioni, servizi di comunicazione, sistemi di pagamento e piattaforme per l'economia collaborativa". Sebbene si tratti di attività tra loro molto diverse, esse presentano caratteristiche comuni, che paiono fondare la trattazione congiunta come "online platform":

"— possono creare e formare nuovi mercati, fare concorrenza a quelli tradizionali e organizzare nuove forme di partecipazione o di esercizio di attività economiche basate sulla raccolta, sul trattamento e sulla modifica di grandi quantità di dati;

— operano all'interno di mercati multilaterali, ma con gradi di controllo variabili sulle interazioni dirette tra gruppi di utenti;

— beneficiano degli "effetti di rete", in virtù dei quali, generalmente, il valore del servizio aumenta con l'aumentare degli utenti;

— spesso si basano sulle tecnologie dell'informazione e della comunicazione per raggiungere i propri utenti in modo istantaneo e con facilità;

— svolgono un ruolo chiave nella creazione di valore digitale, in particolare intercettando tale valore in modo rilevante (anche attraverso l'accumulo di dati), agevolando nuove iniziative imprenditoriali e creando nuove dipendenze strategiche".

Nella nuova proposta di Regolamento europeo per la regolamentazione delle piattaforme, cosiddetto "Digital Services Act"[10], la "piattaforma online" è definita come il provider di un servizio di hosting che, su richiesta di un destinatario del servizio, memorizza e diffonde al pubblico informazioni, a meno che tale attività non sia una caratteristica minore e puramente accessoria di un altro servizio e, per ragioni

---

le limita alle two or multi-sided market platform, per la quale si chiedeva ai partecipanti alla consultazione se la ritenevano adatta o se avessero suggerimenti al riguardo. Cfr. European Commission, *Regulatory environment for platforms , online intermediaries, data and cloud computing and the collaborative economy*.

[9] Commissione Europea, *Le piattaforme online e il mercato unico digitale. Opportunità e sfide per l'Europa*.

[10] EU Commission, *Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act)*.

oggettive e tecniche, non possa essere utilizzata senza quell'altro servizio, cosicché l'integrazione del servizio rappresenta solo un mezzo per aggirare l'applicabilità del Regolamento.

Le piattaforme di intermediazione possono essere, quindi, considerate come appartenenti alla più ampia categoria delle "online platform"[11], costituendone un sottoinsieme.

Si ritiene che la parola "intermediazione" sia la più appropriata per descrivere ed inquadrare la tipologia di piattaforme analizzate, sebbene un po' riduttiva rispetto al ruolo che la piattaforma in concreto svolge, in quanto solitamente utilizzata per indicare un soggetto in ogni caso terzo rispetto al rapporto instaurato tra i soggetti il cui incontro favorisce[12]. Rispetto al suo utilizzo dovranno, inoltre, essere operate le opportune precisazioni, in particolare escludendo, o per lo meno separando, i casi nei quali la piattaforma diviene vero e proprio fornitore del servizio sottostante, intervenendo nel rapporto di scambio tra gli utenti in modo tanto invasivo, ed esercitando sugli utenti e sugli scambi un così alto grado di controllo[13], da non potersi più sostenere ch'essa svolga un mero ruolo di intermediazione[14].

---

[11] Con riguardo a tale più ampia categoria la Commissione europea ha recentemente nominato un gruppo di esperti per analizzare le problematiche esistenti e monitorare le evoluzioni del mercato in vista di futuri interventi. Cfr. *Expert group to the EU Observatory on the Online Platform Economy | Digital Single Market*.

[12] Per definire con maggior dettaglio cosa si debba intendere con "favorendo l'incontro e facilitando gli scambi" ci si può riferire all'art. 1, secondo comma, delle Model Rules on Online Platform , ove si afferma che le disposizioni sono pensate per essere applicate alle piattaforme che: a) consentano ai clienti di stipulare contratti per la fornitura di beni, servizi o contenuti digitali con i suppliers all'interno di un ambiente digitale controllato dal gestore della piattaforma; b) consentano ai fornitori di inserire annunci pubblicitari in un ambiente digitale controllato dall'operatore della piattaforma che può essere consultato dai clienti per contattare i fornitori e concludere un contratto al di fuori della piattaforma; c) offrano confronti o altri servizi di consulenza ai clienti che identificano i suppliers di beni, servizi o contenuti digitali e che indirizzano i clienti ai siti Web di tali fornitori o forniscono dettagli di contatto; oppure d) consentano agli utenti della piattaforma di fornire recensioni su fornitori, clienti, beni, servizi o contenuti digitali offerti dai fornitori, attraverso un sistema di reputazione. Cfr. EUROPEAN LAW INSTITUTE, *Model Rules on Online Platforms*, disponibile al seguente link https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf.

[13] Katz, *Regulating the Sharing Economy*.

[14] L'espressione "online intermediation services" o "servizio di intermediazione online" può essere anch'essa utilizzata, sebbene non preferita ai fini del presente lavoro, in quanto "piattaforme di intermediazione", in ragione del riferimento alla "piattaforma" rende più immediata la comprensione delle tipologie di servizi che possano esservi ricomprese e, in particolare, appare più idonea rispetto alle specifiche

Al fine di definire il fenomeno nel suo complesso, invece, all'espressione "sharing economy"[15], più conosciuta e inflazionata, si preferisce l'espressione "platform economy".

L'espressione "sharing economy" viene comunemente utilizzata per indicare alcune piattaforme, tra le quali, ad esempio, Uber e Airbnb, che, sviluppatesi dopo la diffusione dei *marketplaces* per la vendita al dettaglio, come Ebay e Amazon, connettono tra loro utenti ai fini della conclusione di scambi aventi ad oggetto questa volta non la vendita di beni, bensì la fornitura di servizi.

Non esistendo una definizione univoca, l'espressione potrebbe esser utilizzata anche per descrivere piattaforme molto diverse, che tuttavia operano favorendo l'incontro tra gli utenti; tuttavia vi è chi ritiene che il termine debba essere utilizzato solo al fine di descrivere quelle attività che comportano effettivamente una qualche forma di condivisione. La condivisione, componente importante del legame sociale, secondo alcuni studiosi[16], dovrebbe essere considerata come una

piattaforme che saranno oggetto di analisi (Uber, Airbnb, Amazon, Ebay). L'espressione "online intermediation services" o "servizi di intermediazione online" è, in particolare, utilizzata dalla Commissione europea nel Regolamento 1150/2019 "che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online", nell'ambito del quale è utilizzato per definire i servizi della società dell'informazione che consentono a business users di offrire beni o servizi a consumatori, facilitando la transazione tra questi (indipendentemente da dove queste transazioni siano alla fine concluse), purché sussista un rapporto contrattuale ovvero purché siano forniti in base a rapporti contrattuali tra il fornitore di tali servizi e gli utenti professionali che offrono beni e servizi ai consumatori. Nella legislazione europea si rinviene anche il diverso termine "marketplace" o "mercato online", definito come "un servizio che utilizza un software, compresi siti web, parte di siti web o un'applicazione, gestito da o per conto del professionista, che permette ai consumatori di concludere contratti a distanza con altri professionisti o consumatori". Cfr. art. 4 della Direttiva 2161/2019, che modifica la Direttiva 83/2011, introducendo all'art. 2, lett. e, n. 17 la nuova definizione.

[15] Tra i tanti termini comunemente utilizzati, ma non soddisfacenti per un corretto inquadramento del fenomeno: "the disaggregated economy", "the peer-to-peer economy", "the human-to-human economy", "the community marketplace" "the on-demand economy", "the App economy", "the access economy", "the mesh economy", "the gig economy", "the Uberization of everything". Cfr. ORLY LOBEL, *The Law of the Platform*, «Minnesota Law Review» (2016), 101, 1, pp. 87–166, il quale li elenca al fine di definire il fenomeno della "digital platform revolution" ovvero della trasformazione di ogni cosa in risorsa disponibile (servizi, spazi, prodotti, connessioni, sapere) tramite le tecnologie.

[16] MATTEO ARIA, ADRIANO FAVOLE, *La condivisione non è un dono*, in *L'arte della condivisione*, Milano, Utet, 2015

"terza logica", da affiancarsi al dono[17] e all'interesse individuale, che non implica l'obbligo di ricambiare e "caratterizza tutte quelle situazioni in cui gli 'io' si dissolvono in un 'noi'"[18]. Russel Belk, nei suoi studi sulla condivisione, ha evidenziato come esso si distingua sia dallo scambio che dal dono e l'ha definita come "l'atto e il processo di distribuzione di ciò che è nostro agli altri per il loro uso e/o l'atto e il processo di ricevere o prendere qualcosa dagli altri per il nostro uso"[19]. Esempio quasi archetipico è la condivisione degli oggetti in una casa tra i membri del gruppo familiare, dove la condivisione non è una forma di scambio, ma è connessa sia ad un aspetto affettivo sia a una visione di comunità. È una sfera in cui il noi è tanto diffuso che non permane nemmeno quel "grazie" che opera nel dono[20].

Se questo è, dunque, il corretto significato da attribuire alla parola "sharing" o "condivisione", il fenomeno che verrà descritto e che coinvolge la gran parte delle piattaforme si trova da esso molto lontano. Nelle parole di Alec Ross, "la puoi chiamare economia della condivisione, ma non dimenticare la carta di credito"[21] si tratta piuttosto di "un modo per fare mercato di qualsiasi cosa e per fare di chiunque un microimprenditore"[22], di far entrare nel mercato anche ciò che non era sfruttato[23].

Sicuramente l'utilizzo di queste piattaforme, degli algoritmi e dei *big data* può consentire una migliore allocazione delle risorse, permettendo un maggiore sfruttamento delle risorse sottoutilizzate, siano esse beni o persone. Si pensi ad Airbnb e agli immobili prima non pienamente utilizzati ed ora rientrati nel mercato o alle persone che grazie a questi mezzi riescono a trovare un secondo o terzo lavoro, offrendo le proprie capacità.

Inoltre, la possibilità di consentire l'utilizzo temporaneo di una risorsa, in tempi e con costi ridotti, determina una maggior flessibilità nel rapporto con le risorse stesse. Si pensi, ad esempio, ai nuovi servizi come Netflix o Spotify che consentono di accedere a contenuti audiovisivi e musica senza più acquistare il bene, ma mediante un

---

[17] Da intendersi secondo la nozione elaborata e descritta da Mauss, *Saggio sul dono*.

[18] MATTEO ARIA, ADRIANO FAVOLE, *La condivisione non è un dono*, in *L'arte della condivisione*, Milano, Utet, 2015, p. 23.

[19] Belk, *Sharing*.

[20] Aria e Favole, *La condivisione non è un dono*.

[21] Ross, *Il nostro futuro*, p.121.

[22] Ibidem., p. 120.

[23] Lobel, *The Law of the Platform*.

abbonamento che consente l'accesso a molteplici prodotti sotto forma di un servizio.

Sebbene ciò realizzi una diversa e migliore allocazione delle risorse e una maggior flessibilità e dinamicità nel rapporto tra individui e beni, ad avviso di chi scrive, il termine condivisione non è il più indicato, proprio perché richiamante quella sfera di comunità e unione, che generalmente, nonostante l'inflazionato uso del termine "comunità", non si rinviene nelle piattaforme online. Preferibile è, invece, il termine "platform economy"[24], che maggiormente evidenzia la presenza della piattaforma e il ruolo centrale che essa svolge.

La Commissione europea, nella sua Comunicazione del giugno 2016[25], ha preferito utilizzare una nuova terminologia, coniando il termine "economia collaborativa" e riferendolo ai "modelli imprenditoriali in cui le attività sono facilitate da piattaforme di collaborazione che creano un mercato aperto per l'uso temporaneo di beni o servizi spesso forniti da privati". Viene specificato che l'economia collaborativa coinvolge tre categorie di soggetti: i) i prestatori di servizi che condividono beni, risorse, tempo e/o competenze e possono essere sia privati che offrono servizi su base occasionale ("pari") sia prestatori di servizi nell'ambito della loro capacità professionale ("prestatori di servizi professionali"); ii) gli utenti di tali servizi; e iii) gli intermediari che mettono in comunicazione — attraverso una piattaforma online — i prestatori e utenti e che agevolano le transazioni tra di essi ("piattaforme di collaborazione"). È precisato, infine, che "le transazioni dell'economia collaborativa generalmente non comportano un trasferimento di proprietà e possono essere effettuate a scopo di lucro o senza scopo di lucro".

Anche tale espressione, ad avviso di chi scrive, presenta alcune problematiche, e non sarà utilizzata ai fini della presente analisi. In primo luogo, la parola collaborazione riporta nuovamente, sebbene in forma più sfumata, ad un'unione comunitaria di persone, non del tutto adatta per la descrizione del fenomeno, che più che delinearlo

[24] Assolombarda, *Platform economy : definizioni e prospettive*.

[25] COMMISSIONE EUROPEA, *Un'agenda europea per l'economia collaborativa*, «Com(2016) 356» (2016). Cfr. Cauffman, *The Commission's European Agenda for the Collaborative Economy – (Too) Platform and Service Provider Friendly?*; Cauffman e Smits, The Sharing Economy and the Law. *Food for European Lawyers*; Sundararajan e Parlamento Europeo, *The Collaborative Economy: Socioeconomic, Regulatory and Policy Issues*; Petropoulos e Parlamento Europeo, *An economic review on the Collaborative Economy*; Hatzopoulos, *The collaborative economy and EU law*..

oggettivamente intende suggerire un'impressione positiva dello stesso[26]. Inoltre, al fine di definire l'"economia collaborativa", la Commissione utilizza nuovamente il termine condivisione. In secondo luogo, non convince la limitazione "all'uso temporaneo di beni o servizi", ancor più se coordinato con l'affermazione che le transazioni "generalmente non comportano un trasferimento di proprietà", affermazione che non corrisponde a una distinzione chiara[27] e sembrerebbe mettere in dubbio anche la distinzione tra diritti reali e obbligatori[28].

Ci si chiede, infatti, se la temporaneità dell'utilizzo di beni o servizi possa essere rilevante ai fini della definizione e regolazione del fenomeno e quali siano i limiti che tale temporaneità dovrebbe rispettare. Sebbene, infatti, si registri più spesso la configurazione di diritti meramente obbligatori e di contratti di servizi, rispetto che di transazioni che comportino il trasferimento di diritti reali e in particolare della vendita, non è affatto chiaro se dall'ambito che si intende definire, ed eventualmente regolare, si ritiene realmente di escludere i trasferimenti di diritti reali e in particolare della proprietà o se, invece, si vuole limitare la definizione ai soli contratti ad effetti obbligatori. Si potrebbe distinguere tra piattaforme "marketplace" tradizionali, quali Amazon e Ebay, dove si concludono contratti di compravendita e piattaforme della nuova "sharing economy", quali Airbnb e Uber, attraverso le quali sono conclusi contratti di servizi[29]. La Commissione inquadra coloro che offrono i servizi della "sharing economy" come prestatori di servizi, definiti nella Direttiva 2006/123/CE relativa ai servizi nel

[26] Cfr. Cécile Remeur, *Collaborative economy and taxation*. che sottolinea come i termini più ampiamente utilizzati per descrivere il fenomeno non lo descrivano pienamente, ma enfatizzino alcuni aspetti utilizzando parole che contribuiscano a generare una percezione positiva.

[27] Cfr. Ibidem. ove, invece, si esclude in modo espresso il trasferimento della proprietà dalla definizione di "collaborative economy". Si veda anche Hatzopoulos, *The collaborative economy and EU law*., p. 4, il quale ritiene che il termine "collaborative economy" debba essere riferito ai modelli economici che s'incentrano sul fornire accesso a prodotti e servizi, mediante noleggio, trading o condivisione, anziché attraverso il trasferimento di proprietà.

[28] Cfr. anche *Conclusioni dell'Avvocato Generale Szpunar nella causa C-434/15 («caso Uber»)*. che, con riferimento alla nozione di economia collaborativa afferma, alla nota 13, che si tratta "di una definizione talmente ampia che vi è motivo di dubitare della sua utilità al fine di individuare una tipologia di attività sufficientemente differenziata che giustificherebbe l'assoggettamento della stessa a un trattamento giuridico specifico".

[29] Bamberger e Lobel, *Platform Market Power*.

mercato interno, come "qualsiasi attività economica non salariata di cui all'articolo 50 del trattato fornita normalmente dietro retribuzione"[30].

La definizione di economia collaborativa fornita dalla Commissione europea ricomprende sia le attività svolte con scopro di lucro che le attività che perseguono altri scopi. La scelta di ricomprendere entrambe non ha, in sé, nulla di sbagliato; tuttavia, con riguardo al tema che ci occupa, la disciplina più adeguata rispetto alla responsabilità per le piattaforme non potrà non tener conto della diversità degli scopi delle diverse piattaforme, anche sociali, politici, culturali o filantropici, al fine di evitare che misure pensate sul modello della piattaforma che opera con fine di lucro possano estendersi senza limiti anche a realtà così differenti, che potrebbero non essere in grado di sostenere i rischi e i costi connessi. Si pensi, ad esempio, al noto caso di Wikipedia, piattaforma con contenuti generati dagli utenti al fine di condividere il sapere, creata e gestita dalla Wikimedia Foundation Inc., fondazione creata nel 2003 senza fini di lucro[31].

Elemento fondamentale per circoscrivere il fenomeno che s'intende analizzare è, invece, la presenza di (almeno) tre categorie di soggetti, elemento che caratterizza anche la definizione della Commissione europea di economia collaborativa.

In alcuni studi recenti[32], l'economia collaborativa è, infatti, definita privilegiando tale ultimo aspetto, descritto come "a new trinity": "'users-providers-platforms' that does not match with traditional consumer, business and intermediary concepts", e l'economia collaborativa è descritta come "giving, sharing or swapping services via a platform, for a fee or for free".

La "nuova trinità" è posta in luce in modo peculiare da una differente definizione, fornita dalle scienze economiche: "multi-sided market platform". Il termine è utilizzato per definire le piattaforme che servono distinti gruppi di utenti che in qualche modo hanno bisogno l'uno dell'altro, dove il *core business* della piattaforma consiste nel

---

[30] Articolo 4 della citata Direttiva. Cfr. anche Corte di Giustizia, C-291-13 nel caso Papasavvas v. Fileleftheros, punto 30.

[31] Wikimedia è stata peraltro promotrice di alcune campagne per la difesa della sua attività e, più in generale, della libertà di espressione online. Recentemente, in particolare, con riguardo alla riforma della disciplina in materia di diritto d'autore nel mercato unico digitale. Cfr. Wikimedia Italia, *La comunità di Wikipedia si attiva per difendere la libertà di espressione sul web*..

[32] Cécile Remeur, *Collaborative economy and taxation*.

consentire l'incontro e facilitare le interazioni tra i distinti gruppi di utenti[33]. Vi sono, quindi, almeno due diversi gruppi di utenti, che vengono messi in grado di incontrarsi e dialogare grazie alla piattaforma, che riduce i costi informativi e di transazione[34]. Senza la piattaforma questi incontri non si sarebbero realizzati e per tale motivo la piattaforma viene anche definita "catalizzatore"[35].

Nella definizione di *multi-sided market platform* possono rientrare piattaforme anche molto differenti tra loro ma accomunate dagli aspetti sopra evidenziati. Sono *multi-sided market platform* i *social networks*[36], nei quali la piattaforma s'interfaccia con un primo gruppo di utenti, quelli che vengono comunemente definiti "user" - che generano profili, contenuti ed interagiscono tra loro - ed un secondo gruppo di utenti che si relaziona con la piattaforma in modo differente denominati "advertiser", ai quali la piattaforma offre servizi pubblicitari[37]. Sono certamente *multi-sided market platforms* anche le piattaforme di intermediazione analizzate (Ebay, Amazon, Uber, Airbnb), le quali possono infatti essere definite anche come *multi-sided market platforms* che favoriscono l'incontro tra domanda e offerta di beni e servizi. Rientrano, quindi, in tale definizione Airbnb, Uber e Ebay, ma anche Amazon, quando non opera come venditore ma svolge una funzione di "intermediazione", favorendo lo scambio tra due soggetti.

Si tratta, quindi, di una definizione che pone in evidenza la "nuova trinità" e le peculiarità ch'essa comporta, ma nell'ambito della quale

---

[33] DAVID S. EVANS, RICHARD SCHMALENSEE, MICHAEL D. NOEL, HOWARD H. CHANG, DANIEL D. GARCIA-SWARTZ, *Platform economics: Essays on multi-sided businesses*, «Competition Policy International» (2011), pp. 459.; JONAS SEVERIN FRANK, *Competition Concerns in Multi-Sided Markets in Mobile Communication*, in *Competition on the Internet*, a cura di RUPPRECHT PODSZUN, JOSEF DREXL, RETO M. HILTY, JOSEPH STRAUS, Springer, 2014

[34] Tali costi includono i costi informativi e di ricerca concernenti con chi e quale tipo di accordo s'intende concludere, i costi di contrattazione e decisione, i costi di esecuzione e vigilanza. Con riguardo ad ognuno di tali aspetti la piattaforma fornisce informazioni che riducono i costi. Cfr. Lobel, *The Law of the Platform*.

[35] Evans et al., *Platform economics: Essays on multi-sided businesses*.

[36] I social network possono essere definiti come servizi online che consentono agli individui di (1) costruire un profilo pubblico o semi-pubblico all'interno di un sistema delimitato, (2) articolare una lista di altri utenti con i quali si condivide una connessione, e (3) vedere e attraversare la propria lista di connessioni e quelle create dagli altri utenti all'interno del sistema. Cfr. Boyd e Ellison, *Social network sites: Definition, history, and scholarship*.

[37] Stucker e Grunes, *Big Data and Competition Policy*.

rientrano anche soggetti diversi da quelli che si ritiene di fare oggetto della presente analisi.

Per quanto concerne la precisazione della definizione da un punto di vista tecnologico, si ritiene preferibile evitare di definire la piattaforma da un punto di vista tecnico, con riguardo alla tecnologie utilizzate, analizzando piuttosto le funzioni ch'essa svolge e le dinamiche che in tali contesti si realizzano e sono poste in essere. Mentre l'individuazione di alcuni esempi - nel caso di specie sono stati analizzati Ebay, Amazon, Uber e Airbnb - sia necessaria per dare concretezza all'analisi, una definizione incentrata sulle caratteristiche tecnologiche sarebbe di scarsa utilità e avrebbe poca fortuna, poiché si tratta di realtà in costante evoluzione.

Nella definizione di "Internet intermediaries" dell'OECD sopra citata, infatti, il riferimento è ai "soggetti che forniscono tramite Internet un'infrastruttura o piattaforma che consente comunicazioni e transazioni tra terze parti e fornisce applicazioni e servizi". Gli elementi ivi indicati come necessari sono, quindi, Internet e questa "infrastruttura o piattaforma".

Si consideri, però, che anche la presenza di Internet non è, in realtà, necessaria, potendo essere sostituita da reti private. Forse sarebbe meglio, allora, dire che ciò che è necessario è una connessione. Alla connessione, essenziale, deve aggiungersi la presenza di quella infrastruttura, che si è scelto nel presente lavoro di denominare piattaforma, in particolare in ragione dei modelli di riferimento considerati, ma che in futuro potrà anche trovare nuove forme e denominazioni.

Si consideri, in particolare, l'evoluzione in atto con la diffusione dell' "Internet of Things" o "Internet of Everythings", ovvero della sempre maggiore diffusione di oggetti dotati di software e sensori in grado di raccogliere, trasmettere ed elaborare dati. Questi oggetti comunicano, su rete Internet o tramite reti private, mediante infrastrutture tecnologiche, che, che le si chiami piattaforme o meno, svolgono una funzione in parte analoga a quanto descritto, di facilitatore dell'interazione e di aggregatore di più oggetti e servizi, nonché dei dati da essi tratti, al fine di offrire ulteriori servizi a valore aggiunto[38]. Sebbene dissimili dalle piattaforme considerate, identificabili in un sito web in Internet al quale gli utenti accedono, anch'essi costituiscono "terze

[38] European Commission, *Advancing the Internet of Things in Europe*; Commissione Europea, *Digitalizzazione dell'industria europea. Cogliere appieno i vantaggi di un mercato unico digitale*.

parti" che, tramite un'infrastruttura tecnologica, vengono a svolgere nuove funzioni di aggregatore e facilitatore. Sebbene ancora in fase di sviluppo e non ancora oggetto di approfondite analisi, queste nuove terze parti emergenti nell'ambito dell'Internet of Things evidenziano sia come la tecnologia in sé sia continuamente soggetta ad evoluzioni, sia come la diffusione di nuovi soggetti intermediatori, aggregatori e facilitatori costituisca un trend in crescita, rispondente alla necessità di aggregare grandi quantità di dati e, sfruttando questi e la tecnologia, re-intermediare in modo innovativo l'offerta di beni e servizi.

La tecnologia utilizzata incide profondamente sui modi nei quali le persone e, quindi, anche i soggetti del mercato interagiscono, divenendo abilitante di nuove strutture relazionali e nuovi mercati e modelli di business. Ciò nonostante, ogni definizione strettamente connessa ad una tecnologia particolare, anziché alla funzione da essa abilitata, tenderà a divenire obsoleta velocemente.

8.3. Ruolo, funzioni e natura della piattaforma

Le piattaforme svolgono un ruolo di governance dell'ecosistema che creano, abilitando e regolando le interazioni tra gli utenti.

Tutte le attività che si svolgono all'interno della piattaforma sono sottoposte alla regolamentazione contrattuale che essa predispone per i propri utenti. Viene creato un "ambiente chiuso" [39] ove gli utenti entrano in relazione mediante le possibilità di comunicazione tecnicamente offerte dalla piattaforma e sottostando alle regole ch'essa predispone nell'esercizio della sua autonomia privata.

La piattaforma costruisce tale ambiente, ne detta le regole, vigila sulla loro osservanza, assume decisioni sanzionatorie in caso di violazione ed esegue le decisioni. Si pensi, ad esempio, alla cancellazione di contenuti che violino i termini di servizio, alla sospensione dell'account o anche alla attribuzione o diminuzione di privilegi relativa agli "status utente" premiali sulla base delle recensioni.

L'insieme della struttura tecnica della piattaforma (infrastruttura, dati e algoritmi), delle norme che la regolano e del controllo ch'essa effettua, unitamente ai suoi utenti e ai loro dati, fanno della piattaforma ciò che è, distinguendola dalle altre, determinandone il successo

[39] Rodriguez de las Heras Ballell, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU*.

o l'insuccesso, costituendo il servizio ch'essa offre. Sono tali aspetti che rendono la piattaforma attraente ed efficiente.

Le piattaforme di intermediazione rendono possibile un incontro tra domanda e offerta di beni e servizi che era impensabile prima della loro diffusione, consentendo anche a soggetti non professionali, che non sarebbero stati in grado di sostenere i costi di ingresso sul mercato, di offrire beni o servizi. Ciò avviene grazie ai servizi che la piattaforma offre, molto variabili in relazione alla piattaforma considerata. Tra questi vi è, in primo luogo, l'incontro mirato, reso possibile anche grazie all'utilizzo di big data, algoritmi e geolocalizzazione, al quale si affiancano la gestione delle comunicazioni, la riduzione dei costi informativi, la gestione dei metodi di pagamento, la creazione di una cornice di regolazione privata entro la quale le relazioni tra gli utenti si svolgono, la gestione delle controversie, le verifiche sulle informazioni e servizi forniti dagli utenti, etc.

Le piattaforme si pongono anche quali risolutori delle controversie insorte tra utenti, decidendo sui reclami dei customers, ponendo altresì in essere direttamente, a seguito della decisione, i trasferimenti monetari conseguenti, grazie alle pre-autorizzazioni fornite dagli utenti al momento della conclusione del contratto.

Dall'analisi dei contratti di Ebay, Amazon, Uber e Airbnb emerge che: il servizio svolto dagli utenti costituisce il fulcro dell'attività economica della piattaforma; le piattaforme, attraverso la definizione di standard di qualità, determinano (seppur in misura diversa) la tipologia e la qualità dei servizi offerti; le performance sono valutate dalla piattaforma, con possibilità di risoluzione dei contratti, sospensione degli account o riduzione dei privilegi laddove non siano mantenuti gli standard di qualità.

Da ultimo, interviene dunque anche un controllo ex post sull'adempimento della prestazione.

Ebay, ad esempio, si riserva il diritto di risolvere il contratto per inadempimento, previa diffida ad adempiere con termine di 15 giorni, nonché di limitare, sospendere, terminare i suoi servizi e l'account degli utenti[40], senza alcun preavviso, in una serie di casi, tra i quali

[40] Più precisamente "limitare, sospendere, terminare i suoi Servizi e l'account degli utenti, limitare o altrimenti limitare la visibilità delle inserzioni, nonché proibire l'accesso e le attività degli utenti relative ai Servizi, cancellare le offerte e rimuovere le inserzioni e gli altri contenuti ospitati, nonché ogni stato associato all'account, e adotterà ogni provvedimento tecnico e legale per impedire all'utente di utilizzare i Servizi". Cfr. "Abuso di eBay e risoluzione del contratto" dell'"Accordo per gli utenti".

compaiono: il caso in cui l'utente "abbia gli standard minimi della performance del venditore al di sotto dei minimi previsti dalle regole sullo Standard della performance del venditore o sugli Standard Internazionali della performance dei venditori"; "abbia ricevuto un numero totale di feedback negativi e/o neutri tale da compromettere la sua affidabilità"; "abbia ricevuto un numero di controversie per oggetto non pagato o per oggetto non conforme alla descrizione ai sensi delle relative regole tale da compromettere la sua affidabilità"; ovvero il caso (invero già da solo generico e difficilmente circoscrivibile) in cui "tali provvedimenti possano migliorare la sicurezza della comunità di eBay o ridurre l'esposizione a responsabilità finanziarie di eBay o di altri utenti"; o anche il caso in cui l'utente "abbia concluso transazioni al di fuori del sito".

Gli "Standard della performance del venditore" costituiscono un documento separato e dettagliato, che esordisce con "eBay si aspetta che i venditori forniscano sempre un servizio eccellente agli acquirenti". La prima obbligazione prevista è quella di "risolvere velocemente i problemi degli acquirenti" e si indica come "standard minimo" la garanzia che non più del 2% delle transazioni presentino uno o più difetti "nel periodo di valutazione più recente", al qual fine sarà valutato anche il numero di controversie "chiuse senza risoluzione del venditore" ovvero le controversie che il venditore "non riesce a risolvere con l'acquirente prima che questi chieda a eBay di intervenire o prima che la controversia venga inoltrata a PayPal e che eBay o PayPal determini che il venditore è responsabile".

In Airbnb, l'Host è tenuto a fornire informazioni complete e accurate[41], immagini (della qualità e quantità richiesta), scegliere il prezzo (sebbene ve ne sia uno suggerito), indicare i dati necessari ai fini della gestione dei pagamenti da parte di Airbnb, nonché fornire il servizio offerto mantenendo determinati standard qualitativi.

[41] Cfr. 7.1.1. dei Termini del Servizio. In particolare, "l'utente deve (i) fornire informazioni complete e accurate riguardo al proprio Servizio dell'Host (tra cui, ad esempio, la descrizione dell'annuncio, l'ubicazione e la disponibilità di calendario), (ii) indicare eventuali carenze, restrizioni (ad es. regole della casa) e requisiti che si applicano (ad es. qualsiasi età minima, competenza o requisito di idoneità fisica per un'Esperienza) e (iii) fornire qualsiasi altra informazione pertinente richiesta da Airbnb". Inoltre, è responsabile di "mantenere aggiornate in ogni momento" le informazioni dell'annuncio, compresa la disponibilità di calendario.

Gli "standard qualitativi" si compongono dei termini e delle politiche di Airbnb[42], suddivise in varie sezioni, tra le quali vi sono gli Standard della Community[43], le Linee Guida sul contenuto[44], i Requisiti di base per gli Host[45], le politiche per le cancellazioni[46], ma risultano anche da documenti peculiari quali le politiche di non-discriminazione[47] o contro l'"estorsione"[48], quest'ultimo concernente casi quali la minaccia di recensioni negative.

Limitandosi in questa sede ai "Requisiti di base degli host", essi sono elencati come segue:

"Offrire i servizi essenziali: questa categoria comprende carta igienica, sapone, lenzuola e almeno un asciugamano e un cuscino per ospite.

Essere reattivi: mantieni un tasso di risposta elevato, replicando alle domande e alla richieste di prenotazione entro 24 ore.

Accettare le richieste di prenotazione: fai sentire benvenuti gli ospiti, accettando le loro richieste quando sei disponibile.

Evitare le cancellazioni: prendiamo molto sul serio le cancellazioni delle prenotazioni e chiediamo a tutti i nostri host di evitarle poiché possono rovinare i programmi di viaggio degli ospiti.

Mantenere delle valutazioni elevate: agli ospiti piace sapere che possono aspettarsi un certo livello di qualità, indipendentemente da dove prenotano".

Si tratta di requisiti considerati "di base", eppure molto incisivi, che definiscono la prestazione che gli Host sono tenuti ad offrire. Quest'ultima è, inoltre, anche verificata attraverso le valutazioni date nei *reputational feedback systems*, nonché in relazione alle "controversie" che la piattaforma ha dovuto gestire.

Le piattaforme utilizzano tali "standard qualitativi" nella valutazione delle "condotte" degli utenti che offrono beni o servizi. Tali condotte non son altro che le "prestazioni finali" che vengono offerte agli utenti-clienti e vengono valutate in base a quanto previsto nella disciplina contrattuale e nelle linee guida delle comunità, facendo riferimento anche ai reputational feedback system, stabilendo valori minimi

[42] Airbnb, *Termini e politiche Airbnb*.
[43] Airbnb, *Standard della Community*.
[44] Airbnb, *Linee guida sul contenuto*.
[45] Airbnb, *Requisiti di base degli Host*.
[46] Airbnb, *Politiche cancellazioni*.
[47] Airbnb, *Politiche di non discriminazione*.
[48] Airbnb, *Normative sull'estorsione di Airbnb*.

al di sotto dei quali la piattaforma potrà procedere alla risoluzione del contratto, alla sospensione del servizio o di alcune sue parti, alla diminuzione delle funzionalità e dei privilegi.

Gli standard qualitativi vanno così a determinare le caratteristiche e la qualità della "prestazione finale" offerta agli utenti-clienti, anche in modo dettagliato, includendo il mantenimento di determinati livelli di soddisfazione del cliente valutati attraverso i reputational feedback system, nonché l'assenza di reclami e controversie.

La piattaforma è, quindi, un soggetto che crea nuove forme di interazione estraendo da queste valore. La sua presenza facilita le interazioni e gli scambi, abilitandone di nuovi, riduce i costi di transazione e, al contempo, aumenta la fiducia, riduce i rischi e le incertezze e aumenta la prevedibilità. Svolge non solo un ruolo organizzativo, ma anche di governance rispetto a tutte le relazioni che al suo interno sono poste in essere, compresa l'esecuzione della prestazione.

Ci si interroga, quindi, su come possa essere qualificata la piattaforma nel nuovo scenario, quale forma di organizzazione di risorse produttive che presenta similitudini sia con l'impresa che con il mercato, distinguendosi tuttavia da entrambe[49]. Vi è, infatti, un'organizzazione di risorse per la fornitura di un servizio a un cliente finale, ma con un controllo delle risorse mediato dalla tecnologia e senza acquisizione degli asset organizzati.

Ronald Coase ha evidenziato che l'impresa nasce al fine di ridurre i costi transattivi: sebbene si possa produrre anche in modo decentrato, con singole transazioni, l'impresa emerge, organizzando al suo interno un insieme di relazioni, per ridurre i costi transattivi[50]. L'impresa consente di organizzare le risorse, sotto l'autorità dell'imprenditore, evitando il "meccanismo dei prezzi" e riducendo i costi di produzione e il numero di contratti. Tuttavia, essa richiede un grosso investimento di capitale e l'assunzione del rischio relativo alle decisioni assunte nel management: che una transazione venga organizzata all'interno dell'impresa o che venga conclusa sul mercato da contraenti indipendenti "dipende anche da un confronto tra i costi di conclusione di

[49] Busch, *Self-Regulation and Regulatory Intermediation in the Platform Economy*; Acquier, *Uberization Meets Organizational Theory: Platform Capitalism and the Rebirth of the Putting-out System*; Constantiou, Marton, e Tuunainen, *Four Models of Sharing Economy Platforms*..

[50] Coase, *Impresa, mercato e diritto*.

queste transazioni di mercato con i costi di conclusione di queste transazioni all'interno di un'organizzazione, l'impresa"[51].

Coase si chiedeva anche perché una sola grande impresa non realizzi tutta la produzione, rinvenendo la ragione nei rendimenti decrescenti dell'attività di management e, al contempo, sottolineando che "cambiamenti come il telefono e il telegrafo, che tendono a ridurre il costo di organizzazione nello spazio, tendono ad aumentare la dimensione dell'impresa", e che tutti i cambiamenti che migliorano le tecniche del management tendono ad aumentare le dimensioni dell'impresa"[52].

Se già il telegrafo e il telefono potevano essere considerati elementi rilevanti e dirompenti, possiamo ora immaginare quanto possano esserlo l'utilizzo di connettività, dati e algoritmi per la produzione di beni e servizi.

Il carattere innovativo della piattaforma quale modello organizzativo deriva, quindi, direttamente dalle nuove possibilità che la tecnologia offre per la comunicazione, l'analisi e la gestione delle informazioni. Le nuove tecnologie abilitano nuove forme di organizzazione e management più efficienti, flessibili, personalizzate; la piattaforma consente di gestire anche risorse esterne, senza investimento di capitali e assunzione del rischio; divengono più profittevoli organizzazioni dalle dimensioni più ampie (e ciò è incrementato dai *network effects* e, in particolare, dal *data network effect*).

Evidenziata l'innovatività del modello, nonché la tipologia di piattaforme sulla quale ci si vuole concentrare, occorre riflettere sulle peculiari problematiche che tali piattaforme sollevano e sulle possibilità di regolamentazione di tali nuovi soggetti.

8.4. Problematiche e responsabilità

Tra le problematiche che tali nuovi modelli sollevano si possono evidenziare, in particolare, i problemi relativi alla tutela della concorrenza, alla tutela dei soggetti deboli in ambito contrattuale, all'applicabilità dei requisiti di accesso al mercato elaborati per i modelli di business tradizionali, al tema della gestione dei dati; ma è al più ampio problema delle responsabilità attribuibili a tali soggetti che la nostra analisi si concentrerà.

---

[51] Ibidem. p. 116.

[52] Ibidem., p. 86.

I problemi relativi alla concorrenza sono dovuti alle peculiari concentrazioni del potere di mercato nelle mani di pochi soggetti in ragione dei *network effects*[53] e all'efficientamento dei mezzi comunicativi che permette la gestione profittevole di organizzazioni di dimensioni più grandi, come evidenziato da Coase; tali problemi sono oggetto di una nuova proposta normativa europea denominata "Digital Market Act"[54], che introduce la definizione di piattaforma "gatekeeper" alla quale applicare, in ragione del ruolo nel mercato, obblighi, divieti e un quadro di vigilanza a tutela della concorrenza e del mercato.

La tutela dei soggetti deboli deve essere rivisitata alla luce dell'utilizzo dei nuovi mezzi tecnologici, con riferimento soprattutto alla profilazione e all'utilizzo di algoritmi, come evidente nel caso dei *reputational feedback system*, ma nel senso di un'estensione dei soggetti protetti, potendosi ravvisare una posizione di debolezza anche dei business users, rispetto ai quali il nuovo Regolamento europeo 1150/2019 introduce alcune prime forme di tutela[55], fino a giungere alla posizione di debolezza di chi offre un servizio sulla piattaforma, come i riders o i drivers, rispetto ai quali si sollevano interrogativi in merito al corretto inquadramento contrattuale nell'ambito dei rapporti di lavoro.

Con riguardo ai requisiti di accesso al mercato sorgono interrogativi sull'applicazione delle normative settoriali ai nuovi modelli di business, come evidente nel caso di Uber e delle controversie diffusesi in tutto il globo sui requisiti di tale servizio e le normative ad esso applicabili[56].

---

[53] Cfr. Bambergert e Lobel, *Platform Market Power*; Stucker e Grunes, *Big Data and Competition Policy*; Evans et al., *Platform economics: Essays on multi-sided businesses*; OECD, *Rethinking Antitrust Tools for Multi-Sided Platforms*; Colangelo e Zeno-Zencovich, *Online Platforms, Competition Rules and Consumer Protection in Travel Industry*; Katz e Sallet, *Multisided platforms and antitrust enforcement*.

[54] Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector, Digital Markets Act, COM (2020)842

[55] Cfr. European Commission, *Study on contractual relationships between online platforms and their professional users*; Palmieri, *Profili giuridici delle piattaforme digitali. La tutela degli utenti commerciali e dei titolari di siti web aziendali*; Cauffman, *New EU rules on business-to-consumer and platform-to-business relationships*; Twigg-Flesner, *The EU's Proposals for Regulating B2B Relationships on online platforms – Transparency, Fairness and Beyond*; Martinelli, *The vulnerable business user: the asymmetric relationship between the business user and the platform -*.

[56] Cfr. De Franceschi, *Uber Spain and the "Identity Crisis" of Online Platforms*; De Franceschi, *The adequacy of Italian law for the platform economy*; Resta, *Uber di fronte alle corti europee*; Ruotolo e Vaira, *Il caso Uber nel mercato unico digitale*; Turci, *Sulla natura dei servizi offerti dalle piattaforme digitali: il caso Uber*; Pollicino e Lubello, *Un monito*

Infine, rispetto ai dati, sussistono le più ampie problematiche concernenti non solo la protezione dei dati personali, ma anche quelle relative ai diritti sui dati non personali e alle possibilità di accesso, di utilizzo e riutilizzo[57].

Questo saggio vuole concentrarsi, in ogni caso, sui problemi connessi alla responsabilità della piattaforma stessa, alla luce dei ruoli che essa ricopre nei modelli sopradescritti.

Tale problema è tradizionalmente analizzato sotto il profilo della cosiddetta "responsabilità del provider", o "secondary liability", ovvero della responsabilità della piattaforma per i contenuti immessi in essa dagli utenti, disciplinata dalla Direttiva 31/2000, cosiddetta Direttiva sul commercio elettronico.

Da tempo ci si interroga, infatti, sulla responsabilità di quei soggetti che offrono agli utenti uno spazio nel quale memorizzare le informazioni, e dunque in altre parole che offrono il "contenitore" rispetto alle informazioni memorizzate ma caricate da altri.

I medesimi problemi si pongono non soltanto per le piattaforme di intermediazione, ma per tutte le "online platform" che consentono agli utenti di pubblicare contenuti, riguardando tutti i casi in cui i contenuti sono caricati direttamente dagli utenti su uno spazio gestito da un altro soggetto, ma si complicano ulteriormente nelle piattaforme di intermediazione, ove la funzione della piattaforma non è più soltanto quella di ospitare contenuti, bensì quella di favorire la conclusione di contratti tra gli utenti.

La disciplina della "secondary liability" muove dall'assenza di un obbligo di sorveglianza da parte della piattaforma sui contenuti immessi dagli utenti, in mancanza del quale probabilmente le piattaforme sarebbero oggi molto diverse da come le conosciamo. Viene stabilito una sorta di "safe harbor" per le piattaforme, ritenute non responsabili rispetto ai contenuti, indipendentemente dalla tipologia di responsabilità considerata, salvo in casi determinati e purché la Direttiva sia applicabile alla specifica piattaforma e attività considerata.

---

complesso ed una apertura al dibattito europeo rilevante: uber tra giudici e legislatori; Caruso, *Regolazione del trasporto pubblico non di linea e innovazione tecnologica. Il caso Uber*; Hatzopoulos, *After Uber Spain: the EU's approach on the sharing economy in need of review?*

[57] Graef, Wahyuningtyas, e Valcke, *Assessing data access issues in online platforms*; Martinelli, *Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and «Porting Rights»*; Prüfer, *Competition Policy and Data Sharing on Data-driven Markets*.

Tale disciplina è oggetto della nuova proposta normativa della Commissione europea, cosiddetto "Digital Services Act"[58]. Il Regolamento proposto mira a ridefinire la disciplina applicabile alle piattaforme *online*, modificando la Direttiva 31/2000 ed introducendo nuove disposizioni in materia di trasparenza, obblighi informativi e *accountability* per la moderazione dei contenuti. La proposta è parte del "Digital Services Act package", che ricomprende la "Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM(2020)825" e la "Proposal for a Regulation on Contestable and Fair Markets in the Digital Sector, Digital Markets Act, COM (2020)842".

All'interno di tale più ampio quadro, ci si vuole qui concentrare sulle piattaforme di intermediazione, volte allo scambio di beni e servizi, come meglio in precedenza definite, in quanto si ritiene che in tali casi la piattaforma riveste una funzione ulteriore rispetto a quello di mero contenitore di informazioni: un ruolo organizzativo, di governance e di intermediazione.

La tesi che si sostiene, in estrema sintesi, è che la piattaforma consenta forme di organizzazione e controllo inedite, che richiedono una nuova riflessione anche giuridica, in primo luogo con riguardo alla loro responsabilità.

La soluzione non potrà peraltro essere omogenea per tutte le piattaforme, necessitando di un'analisi e valutazione del potere direttivo, organizzativo e di controllo esercitato sugli utenti. Alti livelli di controllo porteranno all'inclusione delle attività degli utenti tra le attività controllate dalla piattaforma e rispetto alle quali, quindi, sorgerà una sua responsabilità; livelli di controllo più bassi potranno dar luogo a suddivisioni delle responsabilità tra piattaforma e utenti o addirittura l'assenza della responsabilità della piattaforma.

Sebbene relative ad altro profilo (quello dei requisiti di accesso), illuminanti appaiono a tal proposito le pronunce della Corte di Giustizia rese nei casi Uber e Airbnb.

Nell'analisi del caso Uber, causa C-434/15, la Corte di Giustizia ha affermato che il servizio deve essere considerato come an "overall service whose main component is a transport service". La Corte ha affermato che Uber esercita un'influenza determinante ("decisive influence") sulle condizioni in cui i servizi di trasporto erano forniti dai

[58] Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) and Amending Directive 2000/31/EC, COM(2020)825.

conducenti, esercitando un controllo attraverso la stessa applicazione (sulla qualità dei veicoli e dei loro conducenti, determinando la tariffa massima per il viaggio, etc). Alla luce di tale controllo, Uber è stata qualificata come "organizer of the general operation of the services that were not provided by electronic means".

Diversamente, nel caso Airbnb, causa C-390/18, la Corte di Giustizia non ha rilevato tale "decisive influence over the conditions for the provision of the accommodation services to which Airbnb intermediation service relates". In particolare, la Corte ha affermato che la piattaforma "is intended to connect, for remuneration, potential guests with professional or non-professional hosts offering short-term accommodation services, while also providing a certain number of services ancillary to that intermediation service".

La Commissione europea, già nella Comunicazione "Un'agenda europea per l'economia collaborativa", individuava un elenco di criteri, "fattuali e giuridici", per la valutazione del "livello di controllo e di influenza che la piattaforma di collaborazione può esercitare sul prestatore di tali servizi", ritenuto "in genere il fattore determinante": determinazione del prezzo; di altre condizioni contrattuali fondamentali che definiscono la relazione contrattuale tra il prestatore dei servizi sottostanti e l'utente; proprietà dei beni essenziali; assunzione del rischio e sostenimento delle spese; esistenza di un rapporto di lavoro subordinato tra la piattaforma di collaborazione e la persona che ha prestato il servizio sottostante in questione. Tali elementi sono però qualificati come "indizi": non sono ritenuti determinanti, ma "potrebbero indicare che la piattaforma di collaborazione esercita un livello di controllo e di influenza elevato sulla prestazione del servizio sottostante"[59].

Tali pronunce e considerazioni, suggeriscono di indagare se, nei casi di *decisive influence*, il prestatore del servizio sulla piattaforma (es. il driver) possa essere ritenuto un ausiliario della piattaforma stessa; ausiliario in senso stretto ove realizzi l'adempimento e in senso ampio ove cooperi con il debitore per l'esecuzione della prestazione. Ove sussistessero i requisiti, in Italia si potrebbe applicare l'art. 1228 c.c., ove prevede che "salva diversa volontà delle parti, il debitore che nell'adempimento dell'obbligazione si vale dell'opera dei terzi, risponde anche dei fatti dolosi o colposi di costoro".

[59] European Commission, *A European agenda for the collaborative economy*.

Analogamente, con riguardo alla responsabilità civile extracontrattuale, la natura del rapporto tra la piattaforma e il "prestatore del servizio" assume un rilievo determinante, in quanto la piattaforma potrebbe essere ritenuta responsabile per l'operato degli utenti-prestatori del servizio, ai sensi dell'art. 2049 c.c., ovvero per i fatti illeciti compiuti dai suoi preposti nell'esercizio delle incombenze loro affidate. La responsabilità ex art. 2049 c.c., infatti, è applicabile in presenza di un potere di direzione e vigilanza del preponente, anche se temporaneo o occasionale.

Le nozioni civilistiche di ausiliario o soggetto preposto sono più ampie e indipendenti dalla qualificazione giuslavoristica, e potrebbero trovare applicazione anche al di là della qualificazione del rapporto come di lavoro subordinato, in relazione a quei rapporti tra piattaforma e prestatori del servizio che, pur non essendo qualificabili come lavoro subordinato, presentino le caratteristiche della preposizione.

L'attribuzione alla piattaforma di responsabilità, contrattuali o extracontrattuali, derivanti dalle condotte dei "suppliers" potrà, quindi, avvenire, secondo i principi civilistici, in tutti i casi nei quali l'agente è qualificabile come preposto della piattaforma.

Il problema che si pone, in conclusione, è che, nelle piattaforme considerate, si realizzano forme di direzione, coordinamento e controllo inedite e poste in essere in differente grado, nelle quali però si vuol porre il rischio a carico del prestatore del servizio. Diviene, quindi, fondamentale stabilire ed identificare il limite entro il quale l'esercizio di tali poteri da parte della piattaforma, e dunque l'influenza posta in essere, siano tali da attribuire alla piattaforma i rischi connessi. Ove si possano ravvisare il controllo e la direzione dell'attività in capo alla piattaforma, necessariamente anche le responsabilità contrattuali ed extracontrattuali dovranno esserle imputate.

Guardando, invece, a una prospettiva *de iure condendo*, interessante sul punto è la proposta delineata nel "Discussion Draft of a Directive on Online Intermediary Platforms" [60]. Si tratta di un documento elaborato dal Research group on the Law of Digital Services al fine di sollecitare il dibattito, pubblicato nel 2016, che propone una bozza di direttiva che regoli l'attività delle piattaforme di intermediazione. A tale

[60] Research group on the Law of Digital Services, *Discussion Draft of a Directive on Online Intermediary Platforms*; Christoph et al., *Discussion Draft of a Directive on Online Intermediary Platforms. Commentary*; Busch et al., *The Rise of the Platform Economy: A New Challenge for EU Consumer Law?*

documento hanno fatto seguito le Model Rules on Online Intermediary Platform[61], che hanno recepito stimoli e commenti, proponendo un insieme di disposizioni volte a regolare la *platform economy*, non più nella forma della Direttiva ma come *model rules* che possano fungere da modello per legislatori nazionali, europei e internazionali, o da fonte d'ispirazione per l'autoregolamentazione e la standardizzazione. Tra le proposte ivi presenti vi è l'introduzione di una nozione di "predominant influence", diversa dalla "decisive influence" prima citata, che può essere utilizzata per descrivere e regolare una nuova categoria; si tratterebbe di un primo passo verso il riconoscimento dell'esistenza di un soggetto che assume un ruolo diverso da quelli che conosciamo, che è non una semplice impresa che racchiude tutti i servizi complessivi e sottostanti, ma nemmeno un mero intermediario, in nessun senso in cui oggi si intende "intermediario".

Per questa categoria intermedia di piattaforme è prevista, nella proposta, l'introduzione di una responsabilità solidale con il fornitore, sia per l'inadempimento dei fornitori che per la responsabilità da prodotto. L'article 20 prevede: "If the customer can reasonably rely on the platform operator having a predominant influence over the supplier, the customer can exercise the rights and remedies for the non-performance available against the supplier under the supplier-customer contract also against the platform operator". La proposta prevede che la piattaforma con predominant influence sia "jointly-liable for failure to perform the service", assuma quindi un ruolo di garanzia rispetto all'adempimento, configurandosi come garante con responsabilità senza colpa. La disposizione dovrebbe applicarsi non solo ai consumatori, ma a tutti i clienti.

I criteri da considerare per determinare se sussista tale predominant influence sarebbero: a) il contratto *supplier-customer* è concluso esclusivamente mediante facilities fornite dalla piattaforma; b) la piattaforma può trattenere il pagamento eseguito dal customer in esecuzione del contratto *supplier-customer*; c) i termini del contratto *supplier-customer* sono determinati principalmente dalla piattaforma; d) il prezzo pagato dal *customer* è determinato dalla piattaforma; e) la piattaforma fornisce un'immagine unitaria dei *suppliers* o un marchio; f) il marketing è realizzato incentrandosi sulla piattaforma e non sui

[61] European Law Institute, «Model Rules on Online Platforms»., disponibile al seguente link https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf.

suppliers; g) la piattaforma promette di monitorare le condotte dei *suppliers*[62].

Si porrebbe in essere così un'ulteriore categoria di piattaforme, rispetto a quelle delineate nei casi Uber e Airbnb, a cui applicare una disciplina differente, in particolare attribuendo un ruolo di garanzia.

8.5. La piattaforma come intermediario

Nelle piattaforme di intermediazione l'interazione principale tra gli utenti consiste in uno scambio, che prevede la conclusione e quindi l'esecuzione di un contratto.

Per definire ulteriormente quale ruolo svolgano tali piattaforme e quali responsabilità possano essergli attribuite, occorre indagare più approfonditamente anche quale sia il ruolo della piattaforma in relazione al contratto concluso tra gli utenti.

Guardando al mandato, all'agenzia, alla mediazione e all'intermediazione si possono trarre alcune conclusioni *de iure condito* e *de iure condendo*.

Allo schema del mandato o del contratto di commissione si potrebbe pensare, ad esempio, rispetto ad Amazon, ove, come si è visto, la piattaforma si occupa della gestione di molti degli aspetti relativi alla vendita dei beni. Tuttavia, non sussiste alcun obbligo, per Amazon, di concludere contratti, non vi è rappresentanza e gli effetti del contratto si producono in capo al prestatore del servizio.

Per ritenere applicabile la disciplina del mandato, si potrebbe affermare che il prestatore del servizio agisce per conto della piattaforma o viceversa, ma ciò non appare aderente alla realtà, in quanto tutti e tre i soggetti coinvolti agiscono autonomamente e per sé stessi, realizzando però un'operazione negoziale complessa che presenta un collegamento funzionale in senso lato, essendo l'intera operazione volta all'esecuzione delle "prestazioni finali", ma manchevole dello scopo comune in senso stretto. Salvo nei casi in cui si giunga a considerare la piattaforma come prestatore di un servizio complessivo, comprensivo del "servizio sottostante", i tentativi di qualificare l'intero rapporto bilateralmente sembrano nascondere la natura "multi-sided" di queste piattaforme. D'altra parte, anche nell'ambito di "servizi complessivi" come descritti nel paragrafo precedente, l'attività posta in essere dal

[62] Cfr. Ibidem.

supplier sembrerebbe un'attività materiale posta in essere per l'adempimento dell'obbligazione della piattaforma e non, invece, l'adempimento di un mandato ad agire contrattualmente per suo conto, qualificandosi pertanto il *supplier* come ausiliario della piattaforma e non come suo mandatario.

Con riguardo al contratto di agenzia, che ai sensi dell'art. 1742 è il contratto mediante il quale "una parte assume stabilmente l'incarico di promuovere, per conto dell'altra, verso retribuzione, la conclusione di contratti in una zona determinata", le similitudini rispetto al caso della piattaforma si rinvengono nell'attività di "promozione" e convincimento del cliente, nonché nella stabilità del rapporto, non episodico.

Il contratto di agenzia non pare, in astratto, lontano dai rapporti analizzati e sembrerebbe possibile una qualificazione della piattaforma come agente. Tuttavia, la disciplina codicistica è interamente volta alla tutela dell'agente quale parte debole del rapporto, mentre nel caso della piattaforma di intermediazione è tipicamente la parte contrattualmente più forte.

La posizione terza della piattaforma sopra descritta induce a ritenere ancor più significativi i punti di contatto con la mediazione, caratterizzata dall'intervento di un terzo estraneo alle parti che le mette in relazione per provocare o agevolare la conclusione di un affare, senza obbligo di conclusione né per il mediatore, né per le parti che gli abbiano conferito l'incarico, anche con possibilità di impegno generico del mediatore di favorire la conclusione di contratti cercando di procurare il consenso di un altro soggetto.

Sulla mediazione la dottrina è divisa con riguardo alla sua natura contrattuale, non essendovi l'obbligo di concludere il contratto mediato: secondo si tratterebbe di una fattispecie progressiva nella quale alcuni effetti sarebbero riconducibili alla messa in relazione, mentre sarebbero legati alla successiva conclusione dell'affare.

Ai sensi del codice civile, il mediatore è tenuto a comportarsi secondo correttezza, secondo il criterio della diligenza media professionale di cui all'art. 1176, secondo comma c.c., nonché ad alcuni obblighi di informazione e di garanzia; in particolare, l'art. 1759, primo comma, impone al mediatore l'obbligo di "comunicare alle parti le circostanze a lui note, relative alla valutazione della sicurezza dell'affare, che possano influire sulla conclusione di esso".

Particolarmente interessante è la disposizione di cui all'articolo 1762 c.c. ("Contraente non nominato"), che prevede che "il mediatore che non manifesti a un contraente il nome dell'altro risponde dell'esecuzione del contratto e, quando lo ha eseguito, subentra nei diritti verso il contraente non nominato", nonché, al secondo comma, che "se dopo la conclusione del contratto il contraente non nominato si manifesta all'altre parte o è nominato dal mediatore, ciascuno dei contraenti può agire direttamente l'uno contro l'altro, ferma restando la responsabilità del mediatore".

I contratti delle piattaforme di intermediazione potrebbero, quindi, essere ritenuti contratti di mediazione, sebbene diversi dalle ipotesi più tradizionali, e si potrebbe allora prospettare l'applicazione degli artt. 1762 e 1759: il primo consentirebbe di attribuire alla piattaforma la responsabilità relativa all'adempimento della prestazione per il caso in cui il supplier non sia identificabile; il secondo, che prevede in capo al mediatore l'obbligo di "comunicare alle parti le circostanze a lui note, relative alla valutazione della sicurezza dell'affare, che possano influire sulla conclusione di esso", legittimerebbe l'imputazione alla piattaforma di tutte le responsabilità relative all'affare concluso tra gli utenti, ove essa sia stata manchevole, secondo la diligenza professionale, di fornire agli utenti le adeguate informazioni.

Oltre alla figura del mediatore, rispetto al quale le specifiche discipline prevedono obblighi di trasparenza, professionalità e imparzialità, esistono altre figure di "intermediari", regolati con riguardo ad alcune specifiche attività. Il termine viene utilizzato in modo aspecifico per indicare attività, professionalità e contratti molto diversi, tra i quali il mandato, il contratto di agenzia e la mediazione. Sebbene tali discipline non possano essere ritenute direttamente applicabili, se non eventualmente per analogia, alle piattaforme di intermediazione, da esse possono trarsi alcuni spunti per meglio comprenderne natura e funzione, nonché in vista di futuri interventi regolatori.

Tra gli intermediari di assicurazione o riassicurazione, definiti dall'art. 1, lett. cc-quinquies del Codice delle Assicurazioni come "qualsiasi persona fisica o giuridica, diversa da un'impresa di assicurazione o riassicurazione o da un dipendente della stessa e diversa da un intermediario assicurativo a titolo accessorio, che avvii o svolga a titolo oneroso l'attività di distribuzione assicurativa[63], si ritrovano due

[63] Cfr. art. 1 del Codice delle Assicurazioni Private, D.lgs. 209/2005, ove sono altresì definite le figure dell'intermediario riassicurativo (cc-sexies: "qualsiasi persona fisica o

figure: gli agenti e i mediatori, iscritti in due distinte sezioni. Agenti di assicurazione sono coloro che "agiscono in nome o per conto di una o più imprese di assicurazione o di riassicurazione"; i mediatori di assicurazione o di riassicurazione, denominati anche "broker", "agiscono su incarico del cliente e senza poteri di rappresentanza di imprese di assicurazione o di riassicurazione"[64].

La figura del broker presenta alcune affinità rispetto alle piattaforme analizzate, ovvero un'attività di intermediazione in assenza di mandato definita con il termine "mediazione", sebbene il mediatore agisca "su incarico del cliente"[65], mentre la piattaforma di intermediazione instaura relazioni contrattuali con entrambi i soggetti, seppur dimostrando chiaramente un favor verso il *customer*. Ulteriore elemento di distinzione è la molteplicità dei contratti che saranno conclusi e dei soggetti con i quali i contratti potranno essere posti in essere.

All'art. 107, terzo comma, del Codice delle assicurazioni si specifica che non costituisce attività di intermediazione "la mera fornitura a potenziali assicurati di informazioni su prodotti assicurativi o riassicurativi, su un intermediario assicurativo o riassicurativo, su un'impresa di assicurazione o riassicurazione, se il fornitore non intraprende ulteriori iniziative di assistenza nella conclusione del contratto". La distinzione tra un intermediario e un soggetto che si limita a fornire informazioni viene rinvenuta, quindi, nelle "ulteriori iniziative di assistenza nella conclusione".

Il medesimo principio potrebbe essere applicato alla piattaforma di intermediazione, quest'ultima certamente fornisce informazioni su

giuridica, diversa da un'impresa di assicurazione o di riassicurazione o da un dipendente di essa, che avvii o svolga a titolo oneroso l'attività di distribuzione riassicurativa") e dell' intermediario assicurativo a titolo accessorio (cc-*septies*: "qualsiasi persona fisica o giuridica, diversa da uno dei soggetti di cui alla lettera d), comma 2, dell'articolo 109, che avvii o svolga a titolo oneroso l'attività di distribuzione assicurativa a titolo accessorio").

[64] Cfr. art. 109, secondo comma, del Codice delle Assicurazioni Private.

[65] La legge 792/1984, art. 1, definiva, invece, il mediatore, come "chi esercita professionalmente attività rivolta a mettere in diretta relazione con imprese di assicurazione e riassicurazione, alle quali non sia vincolato da impegni di sorta, soggetti che intendano provvedere con la sua collaborazione alla copertura dei rischi, assistendoli nella determinazione del contenuto dei relativi contratti e collaborando eventualmente alla loro gestione ed esecuzione". L'agire "su incarico del cliente" ha risollevato dubbi sulla natura della mediazione assicurativa, che comporta sia l'attività di mediazione che un'attività di consulenza professionale all'assicurando. La giurisprudenza, pur riconoscendo i connotati intellettuali, ha affermato la prevalenza della mediazione. Cfr. Cass. 6874/2003.

prodotti, servizi e prestatori del servizio, ma a tale attività informativa si affiancano tutte le ulteriori attività che la piattaforma pone in essere tra le quali la fornitura del canale di comunicazione, i *reputational feedback systems*, ma anche le possibilità di proporre reclamo e di avvalersi di strumenti di risoluzione delle controversie, attinenti invece a fasi successive rispetto alla conclusione. Ci si chiede, quindi, se e quando, tali attività, considerate caso per caso e complessivamente, possano essere considerate intermediazione.

Il mediatore creditizio, ai sensi degli artt. 128-sexies e ss. del T.U.B., è "il soggetto che mette in relazione, anche attraverso attività di consulenza, banche o intermediari finanziari previsti dal Titolo V con la potenziale clientela per la concessione di finanziamenti sotto qualsiasi forma". Deve svolgere esclusivamente tale attività ed è tenuto a svolgerla "senza essere legato ad alcuna delle parti da rapporti che ne possano compromettere l'indipendenza"[66]. Deve essere iscritto negli appositi elenchi, può essere soggetto a ispezioni dell'Organismo di cui all'art. 128-undecies, per il tramite della Guardia di Finanza. Risponde in solido dei danni causati nell'esercizio dell'attività dai dipendenti e collaboratori di cui si avvale, anche in relazione a condotte penalmente sanzionate[67].

Sono, inoltre, applicabili le norme del Titolo VI per garantire trasparenza e correttezza nei rapporti con la clientela. Tra le disposizioni ivi previste, di particolare interesse ai nostri fini sono quelle sulla pubblicità delle condizioni economiche relative alle operazioni e ai servizi offerti e degli indicatori che assicurano la trasparenza informativa alla clientela, nonché sulla possibilità di degli organi di vigilanza di determinare criteri e parametri per determinare le commissioni massime e elementi essenziali da indicare negli annunci pubblicitari (art. 116). Vi sono, inoltre, ulteriori disposizioni alle quali si potrebbe guardare *de iure condendo* relative alla forma dei contratti (art. 117), alla modifica unilaterale delle condizioni contrattuali (art. 118), alle comunicazioni periodiche alla clientela (art. 119) , al recesso (120-bis), alla portabilità (120-quater).

Si tratta, quindi, di una figura che presta attività consulenziale, ma con i caratteri dell'indipendenza. Viene definito come "un consulente qualificato la cui indipendenza dalle parti e l'adeguata capacità reddituale gli consentono di avere un potere contrattuale tale da

[66] Cfr. art. 128-sexies, quarto comma, del T.U.B.
[67] Cfr. art. 128-nonies, quarto comma, del T.U.B.

permettergli di ottenere condizioni più favorevoli al cliente nella contrattazione con l'intermediario finanziario"[68].

La piattaforma presenta caratteristiche analoghe: sia la terzietà rispetto alle parti, sia il potere contrattuale, esercitato con un favor verso il *customer*. Tuttavia, nel caso della piattaforma, il *supplier* non può considerarsi normalmente un contraente forte.

Le norme in materia di mediazione creditizia rimangono peculiari, specifiche per l'attività considerata; tuttavia si rinvengono disposizioni volte a rispondere ad esigenze di tutela dell'indipendenza e della trasparenza, che si estendono anche alle piattaforme di intermediazione. Le disposizioni di cui al Titolo VI regolano, infatti, aspetti che sollevano problematiche anche nella *platform economy*.

Con riguardo all'intermediazione finanziaria è possibile qualche riflessione ulteriore, di più ampio respiro, essendo l'attività finanziaria l'ambito nel quale l'intermediazione si è ad oggi maggiormente sviluppata.

La teoria economica degli intermediari finanziari rinviene le cause della necessità di un'intermediazione nella divergenza delle preferenze degli scambisti (propensione al rischio e alla liquidità), nella razionalità limitata (decisioni non puramente razionali e informazione eccessiva rispetto alle capacità) e nei costi di transazione (di ricerca, selezione, valutazione etc., influenzati dalla dimensione e dalla frequenza dello scambio).

Un ulteriore aspetto che caratterizza tali mercati e che si vuole sottolineare è che con riguardo ai prodotti finanziari l'informazione relativa a prodotti e servizi è già da tempo gestita attraverso sistemi computazionali connessi.

Le caratteristiche sopra descritte e che valgono per i mercati finanziari si rinvengono anche nell'offerta di beni e servizi al consumo: rilevanza delle preferenze, razionalità limitata e costi di transazione alti rispetto a piccoli scambi. La digitalizzazione e la possibilità di raccogliere dati consentono di accedere al patrimonio informazionale che, a sua volta, permette, tramite gli algoritmi, di identificare le preferenze. La piattaforma appare, quindi, come l'interprete del patrimonio informazionale relativo a prodotti e servizi che oggi possono essere digitalizzati, e dunque un nuovo intermediario. Tuttavia, l'analogia funziona fino a che non si considerino i poteri organizzativi e di direzione che la piattaforma esercita sugli utenti, che la qualificano come

[68] Ciani, *Agenti in attività finanziaria, mediatori creditizi, ed altri intermediari del credito*.

qualcosa di ulteriore, non già realmente terza rispetto al rapporto. Di nuovo, è l'influenza che determina il grado di somiglianza rispetto al modello offerto dall'intermediazione finanziaria: solo ove questa sia ridotta, potrà ravvisarsi una forma analoga di intermediazione.

La contrattualistica in materia di intermediazione finanziaria è caratterizzata dalla presenza di contratti "cornice", cui seguono singoli ordini, dei quali la dottrina ha dato differenti interpretazioni, ricostruite dalla dottrina[69] come segue: 1) contratto normativo in cui il primo contratto ha per oggetto la disciplina dei futuri singoli contratti; 2) fattispecie a formazione progressiva dove il primo livello sarebbe rappresentato dal contratto quadro e il secondo dai singoli ordini; 3) "contratto quadro come un obbligo, ovvero una sorta di mandato conferito all'intermediario finanziario, affinché costui esegua gli incarichi di volta in volta conferitogli dall'investitore". Come noto, rispetto a tali contratti centrale era il problema della validità degli ordini in presenza di patologie del contratto quadro.

Nelle piattaforme ritroviamo la presenza di "contratti quadro" e di "singoli ordini", ma in un contesto in cui i due soggetti da intermediare vengono messi in contatto attraverso la piattaforma cosicché la manifestazione della volontà di concludere il contratto viene mediata attraverso lo strumento informatico, ma resa direttamente tra i "mediati". Nell'intermediazione finanziaria il cliente impartisce ordini e istruzioni all'intermediario, nella piattaforma utilizza il servizio da questa offerto per individuare le possibili controparti contrattuali.

Similmente a quanto avviene nell'intermediazione finanziaria, l'intermediario è in possesso di un patrimonio informazionale al quale l'utente non ha accesso e al quale si affida, tuttavia tali informazioni sono raccolte dalla piattaforma attraverso gli spazi e i *tools* che mette a disposizione, ma fornite e inserite dagli utenti: i *providers* forniscono le informazioni relative al bene o prodotto, i *customers* i *feedback* tramite le recensioni e i sistemi di valutazione. La piattaforma, sfruttando i dati da questi forniti e gli ulteriori raccolti dall'utilizzo del servizio da parte degli utenti, offre le informazioni e il canale di comunicazione.

In conclusione, le piattaforme di intermediazione, al di fuori dell'ipotesi della piattaforma che regoli e controlli anche il servizio sottostante sopradescritta, introducono una nuova forma di intermediazione, svolta attraverso un'infrastruttura IT.

---

[69] Iudica, *La responsabilità degli intermediari finanziari*.

Potrebbe essere introdotta una nuova normativa, riferita ad un contratto di mediazione caratterizzato dall'elevato utilizzo della tecnologia e dalla fornitura di servizi "come prodotto".

La disciplina inoltre potrebbe essere divisa in due, come avviene nel Codice delle Assicurazioni, con una doppia opzione tra mediazione e contratto di agenzia (seppur con le peculiarità evidenziate e legate al diverso equilibrio di forza contrattuale).

Escludendo il caso in cui la piattaforma possa essere considerata un fornitore di un servizio complessivo, compreso il servizio offerto dai *suppliers*, le nuove forme di intermediazione descritte richiedono nuove normative con riguardo a tali aspetti. Il livello di controllo esercitato dalla piattaforma sugli utenti e sull'ecosistema creato, suggeriscono la necessità di ulteriori misure e la nuova disciplina può essere ispirata dalla regolamentazione dei servizi di mediazione, intermediazione bancaria e intermediazione assicurativa, tenendo conto però delle peculiarità dei nuovi modelli.

Le attività di intermediazione, mediazione o agenzia è posta in essere attraverso un'infrastruttura informatica, ma nonostante la peculiarità, anche la piattaforma abilita e governa rapporti contrattuali, influenzando le relazioni tra gli utenti.

Le nuove proposte normative europee, Digital Services Act e Digital Markets Act, introducono nuove nozioni e disposizioni per introdurre regimi di responsabilità più severi ma non tengono, tuttavia, conto dei livelli di controllo della piattaforma rispetto agli utenti e agli scambi che questi pongono in essere.

9. *Neurorights*. Una prospettiva di analisi interdisciplinare tra diritto e neuroscienze

Anna Anita Mollo (Scuola Superiore Meridionale)

9.1. La vulnerabilità relazionale come sostrato etico-giuridico delle neurotecnologie

Le neuroscienze, intese come l'insieme delle discipline che studiano i vari aspetti funzionali del sistema nervoso[1], si avvalgono dell'apporto di numerose branche della ricerca biomedica ma presentano profili di enorme rilevanza anche per la ricerca etica e giuridica.

Il rapporto tra diritto e neuroscienze è tanto rilevante che ben due distinte aree di studio, che trovano oggi pieno riconoscimento scientifico, si sono sviluppate per approfondire tutte le implicazioni a tal fine rilevanti. A partire dagli anni novanta del secolo scorso, infatti, con il termine *neurolaw*[2] - o neurodiritto[3] – si fa riferimento ad un'ampia area di studio che si occupa delle questioni giuridiche connesse all'analisi del cervello umano mediante l'impiego di neurotecnologie, ovvero di

[1]Parla di "era Neurocentrica" per indicare la centralità degli studi neuroscientifici anche rispetto alle scelte governative e politiche in generale J.F. DUNAGAN, *Politics for Neurocentric Age*, in *Journal of Futures Studies*, 2010, 51-70.

[2] J.S. TAYLOR, J.A. HARP, T. ELLIOTT, *Neuropsychologists and neurolawyers*, in *Neuropsychology*, 1991, 293–305; F. X. SHEN, *Law and Neuroacience 2.0*, in *Arizona State Law Journal*, 2021, 1043-1086.

[3] Nella letteratura giuridica italiana sull'impiego del termine neurodiritto E. PICOZZA (a cura di), *Neurodiritto. Una introduzione*, 2011; A. LAVAZZA, L. SAMMICHELI, *Il delitto del cervello. La mente tra scienza e diritto*, 2012. Sul rapporto tra neuroscienze e diritto AA. VV., *Neuroscience and Law*, 2021; A. D'ALOIA, *Neuroscienze e diritto. Appunti preliminari*, in *Rivista di Biodiritto*, 2017, 1-6; L. TAFARO, *Neuroscienze e diritto civile: nuove prospettive*, in *Rivista di Biodiritto*, 2017, 251-275.

metodi e *devices* che consentono di stabilire una connessione diretta con il cervello umano e le relative attività neurali; più di recente con il termine neuroetica, utilizzato per la prima volta nei primi anni duemila[4], si indica l'ambito di riflessione scientifica attinente ai profili etici delle neuroscienze.

Le prime questioni analizzate hanno riguardato il possibile utilizzo delle acquisizioni delle neuroscienze nell'ambito del processo penale, in relazione a vari profili tra cui la responsabilità e la colpevolezza dell'imputato nonché la prevedibilità e controllabilità di comportamenti violenti; l'ammissibilità di prove neuroscientifiche (*brain imaging*) in sede dibattimentale[5]; i profili etici di ammissibilità del potenziamento cognitivo[6].

Negli ultimi anni, invece, un diverso e nuovo approccio si è andato sviluppando nell'ambito del neurodiritto e della neuroetica, attinente alla definizione di una serie di possibili principi etici e giuridici relativi alle situazioni giuridiche connesse all'impiego di neurotecnologie e, quindi, alla tutela del cervello e della mente umana.

Tale nuovo ambito di studio e di ricerca, quale sottocategoria della neuroetica e del neurodiritto e noto con il sintagma "*neurorights*" o neurodiritti, vuole indagare la possibilità di individuare un nuovo *framework* normativo in tema di diritti fondamentali degli individui come possibile regolamentazione delle neurotecnologie che, grazie allo sviluppo dell'intelligenza artificiale, ci consentono non più soltanto di acquisire il dato neurale ma anche di elaborarlo con scopi inferenziali e predittivi.

---

[4] Il termine 'neuroetica' è stato usato per la prima volta all'interno della conferenza '*Neuroethics: Mapping the Field*' del 2002, dal giornalista del *New York Times* William Safire, *Visions for a new field of" neuroethics.* Sul punto anche M. IENCA, K. IGNATIADIS, *Artificial Intelligence in clinical neuroscience: methodological and ethical challenges*, in *AJOB Neuroscience*, 2020, 77-87. Nella letteratura giuridica italiana G. PIZZETTI, *Ragione e sentimento tra etica, neuroscienze e diritto*, in *Biblioteca della Libertà*, 2021, 1-11.

[5] M.S. PARDO, D. PATTERSON, *Mind, Brains, and Law. The Conceptual Foundations of Law and Neuroscience*, in *Oxford University Press*, 2013, 179-207; S.J. MORSE, *New neuroscience, old problems*, in *Neuroscience and Law: Brain, Mind and the Scale of Justice*, 2004, 157-198; M.J. FARAH, *Emerging ethical issues in neuroscience* in *Nature neuroscience,* 2002, 1123-1129.

[6] M.J. FARAH, J. ILLES, R. COOK-DEEGAN, H. GARDNER, E. KANDEL, P. KING, P.R. WOLPE, *Neurocognitive enhancement: what can we do and what should we do?* in *Nature Reviews Neuroscience,* 2004, 421-425.

Tali riflessioni si inseriscono nel più ampio dibattito sulla definizione e regolamentazione del particolare rapporto tra soggetto e tecnologia nonché del concetto di *vulnerabilità* intesa come naturale condizione di fragilità di ogni essere umano.

Al riguardo, infatti, autorevole dottrina ha definito "soggetti vulnerabili"[7] tutti coloro che possano subire un pregiudizio dall'interazione con *devices* tecnologici, anche in assenza di quegli elementi della fattispecie (disabilità, incapacità – anche per minore età - anzianità) che il legislatore individua per destinare una maggior tutela a favore di determinati soggetti.

Rispetto a tali nuovi scenari creati dall'evoluzione tecnologica il sintagma "*vulnerabilità relazionale*"[8] sembra esprimere perfettamente una condizione/qualità astrattamente riferibile ad ogni individuo, sebbene transitoria e non permanente, riferita al periodo in cui opera in un ambiente tecnologico.

Una condizione di vulnerabilità che sembra duplicare l'esigenza di tutela laddove sia riferita alle persone con disabilità, ai minori o agli anziani, già destinatari di una maggior attenzione da parte dell'ordinamento giuridico. Una tutela che, al contrario, si qualifica come prima istanza di protezione per coloro che proprio dall'interazione con *devices* tecnologici possano subire un pregiudizio.

Queste due distinte ipotesi, entrambe connesse al tema dell'esigenza di tutela per soggetti che, in vario modo e per cause molteplici e/o diverse, si trovino in una condizione di vulnerabilità, rappresentano il sostrato etico-giuridico di riferimento su cui innestare una più ampia analisi sul tema delle neurotecnologie.

9.2. Le neurotecnologie: tipologie e ambiti applicativi

Qualsiasi riflessione sulle implicazioni etiche e giuridiche dell'impiego delle *neurotecnologie* impone una preventiva individuazione del

[7] L. GATT, *The vulnerability of the human being in a technological environment: the need for protective regulation,* in L. GATT (a cura di) *Social networks and multimedia habitats*, 2020, 1-53.

[8] I.A. CAGGIANO, *Minori d'età e GDPR*, in AA.VV., *Family law and Technology*, a cura di E. DE BELVIS, 2022, 189-214.

preciso significato da attribuire a tale termine. Con esso, infatti, è possibile indicare ogni tecnologia che consenta di creare un percorso di comunicazione diretto – variamente articolato nei termini che di qui a breve si andranno a specificare - con il cervello umano.

Una definizione quest'ultima che suggerisce l'ampia eterogeneità di un complesso di metodi e strumenti tecnologici che non sono riconducibili ad unità, richiedendo una classificazione diversificata degli stessi.

Pur avendo ben in mente tale diversità, una possibile distinzione che consenta una più agevole analisi da un punto di vista giuridico delle neurotecnologie è quella tra tecniche di *neuroimaging* da un lato e tecniche di *Brain Computer Interface* (BCI) dall'altro.

Le prime consentono l'osservazione scientifica del sistema nervoso centrale, cogliendo la presenza di eventuali strutture patologiche dall'analisi dell'immagine del cervello visualizzata[9]; le stesse sono, altresì, in grado di registrare determinate funzioni celebrali e di indicare a quale area del cervello sono riferibili[10]. Si tratta di tecniche ampiamente utilizzate in oncologia e nella diagnostica, per rilevare eventuali patologie di natura neurologica e le relative lesioni del sistema nervoso.

Le descritte tecniche di *neuroimaging* costituiscono, tuttavia, anche i principali strumenti per registrare l'attività celebrale e per consentire lo sviluppo ed il funzionamento delle interfacce Cervello-Computer o di *Brain Computer Interface* (in acronimo BCI)[11].

Queste ultime costituiscono le più recenti neurotecnologie che consentono non solo di accedere al cervello per studiarne la struttura ed il

---

[9] Questi si definiscono *metodi di visualizzazione strutturale* in quanto si limitano ad analizzare la struttura del cervello; vi rientra ad esempio la Risonanza magnetica nucleare (NMR).

[10] Si tratta di *metodi di visualizzazione funzionali* e consentono di studiare quali effetti sono prodotti su determinate aree celebrali da varie patologie neurologiche e psichiatriche. Si distinguono in *metodi di visualizzazione funzionale diretti*, che registrano il potenziale elettrico celebrale come l'Elettroencefalogramma multicanale (EEG); metodi di *visualizzazione funzionale indiretti* come la Tomografia ad emissione di positroni (PET) e la Risonanza magnetica funzionale (fMRI). I dati generati attraverso queste tecniche di *neuroimaging* possono essere utilizzati per identificare biomarcatori basati sull'immagine delle malattie cerebrali, ovvero biomarcatori di *neuroimaging*.

[11] N. LIV, *Neurolaw: Brain-Computer Interfaces*, in *Journal of Law and Public Policy*, 2021, 328-355.

funzionamento ma anche di collegarlo ad un *computer* esterno che traduce l'attività celebrale rilevata dell'utente in comandi per il controllo di un dispositivo esterno (*computer*, sintetizzatori vocali, neuroprotesi).

Le interfacce di BCI sono state originariamente progettate in relazione a quella grave condizione clinica nota come "*locked-in syndrome*" in cui il soggetto, pur essendo capace e cosciente in quanto in grado di comprendere quanto accade intorno a sé, non riesce ad esprimersi attraverso la comunicazione verbale e ad eseguire semplici movimenti del suo corpo, non avendone più il controllo.

Le neurotecnologie che utilizzano sistemi di BCI operano attraverso fasi determinate: dopo aver generato un *input* iniziale, ovvero un'attività celebrale da parte dell'utente in risposta ad uno stimolo, questa viene dapprima registrata e poi decodificata da parte dell'interfaccia; in tal modo, l'i*nput* iniziale viene da questa trasformato in un *output*, ovvero nell'esecuzione di una precisa funzione che il singolo riuscirà a svolgere in autonomia grazie al dispositivo di BCI (controllo di un arto robotico o di una sedie a rotelle elettronica; espressione delle propria volontà in piena autonomia grazie all'ausilio dell'interfaccia[12]).

Per meglio definire gli attuali sistemi di BCI occorre distinguerli in due categorie: invasivi e non invasivi, a seconda delle modalità con cui l'attività celebrale viene registrata. Le BCI non invasive utilizzano elettrodi non impiantati nel corpo ma posizionati sulla superficie dello scalpo; le BCI invasive richiedono l'impianto di microelettrodi direttamente nel sistema nervoso centrale attraverso un intervento chirurgico.

L'ultima evoluzione delle tecniche di BCI è rappresentata dalla neuromodulazione. In questo caso l'interfaccia non è solo in grado di registrare e trasformare l'attività celebrale in un *output* ma anche di incidere sulla stessa, ovvero di inviare segnali elettrici al cervello per modificarne il funzionamento. Tra le più note tecniche di neuromodulazione invasiva[13] si individua la *Deep Brain Stimulation* (DBS) che, grazie alla riscrittura dell'attività celebrale, è in grado di mitigare alcuni

[12] U. CHAUDARY et al., *Spelling interface using intracortical signals in a completely locked-in patient enabled via auditory neurofeedback training,* in *Nature Communications*, 2022, 1-9.

[13] Richiede l'impianto di fili sottili con elettrodi collegati a prolunghe che vengono incanalate sotto la pelle del paziente e lungo il collo. Tali prolunghe sono a loro volta collegate a un generatore di impulsi (un dispositivo simile a un *pacemaker* cardiaco) che il paziente può accendere o spegnere grazie ad un telecomando.

gravi sintomi di malattie come il Parkinson[14], consentendo di controllare ed eliminare/attenuare il tremore tipico di questa malattia. Si consideri, inoltre, che grazie allo sviluppo e all'applicazione dei meccanismi di *machine learning* alle tecniche di DBS, queste ultime sono state più di recente progettate in modo da automatizzare completamente il processo di stimolazione in base ai sintomi di ogni persona. Si tratta dei dispositivi di DBS c.d. *closed-loop*[15], ovvero ad anello chiuso, in cui è l'algoritmo a decidere i parametri della stimolazione.

Le descritte neurotecnologie sono state progettate e sviluppate per essere impiegate in ambito clinico, per la diagnosi e il trattamento di pazienti con malattie gravemente invalidanti e neurodegenerative, che consentono di recuperare funzioni motorie e cognitive altrimenti andate irrimediabilmente perdute. Tuttavia, negli ultimi anni si assiste ad una sempre più ampia diffusione di dispositivi che utilizzano tecniche neuroscientifiche per fini diversi dalla cura dei pazienti e dalla ricerca biomedica.

Un primo impiego di neurotecnologie per finalità non terapeutiche si è avuto in ambito militare[16]. Già da tempo, infatti, l'agenzia americana *DARPA*, interna al Pentagono, utilizza neurotecnologie per potenziare le capacità cognitive dei militari e renderli in grado di agire anche in condizioni di sonno o stanchezza[17]. Più in particolare, lo studio "*CCDC CBC-TR-1599, Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DOD*"[18] prevede che i progressi tecnologici attuali e prossimi consentiranno a breve e medio termine la creazione di combattenti potenziati con tecnologie aumentative oculari, uditive, muscolari e neurali. Al riguardo non sono ancora note le

[14] Grazie ad un recente studio condotto presso l'Università Sant'Anna di Pisa è stato possibile, applicando tecniche di DBS, identificare il comportamento dei neuroni che portano i pazienti a prendere decisioni rischiose https://www.santannapisa.it/it/news/parkinson-e-controllo-degli-impulsi-grazie-una-collaborazione-tra-li-stituto-di-biorobotica

[15] Il primo impianto in un essere umano di un sistema di DBS ad anello chiuso è stato realizzato presso l'Università di Oxford https://www.ox.ac.uk/news/2022-02-08-first-human-implant-closed-loop-bioelectronic-research-system

[16] A. KRISHNAM, *Military Neuroscience and the Coming Age of Neurowarfare*, 2017; M.B. RUSSO, M.C. STETZ, T.A STETZ TA, *Ethical considerations. Cogneuticals in the military*, in *Farah MJ, Chatterjee A (eds) Neuroethics in practice*, 2013. Nella dottrina italiana A. SALVATORE, *Neuroscienze e utilizzazione militare delle tecniche di potenziamento umano*, in *Etica & Politica*, 2014, 182-198.

[17] https://www.darpa.mil/program/our-research/darpa-and-the-brain-initiative.

[18] Lo studio è disponibile qui https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/300458

conseguenze sull'integrità psico-fisica dei soldati sottoposti a tali tecniche e del loro livello di reversibilità[19].

Sempre più ampia appare, inoltre, la progettazione ed immissione sul mercato di dispositivi che non hanno come destinatari persone con disabilità in un contesto clinico, bensì utilizzati come accessori indossabili per attività come il gioco – c.d. *neurogaming* – o la cura del proprio benessere individuale[20].

Si parla al riguardo di "*consumer* o *pervasive neurotechnologies*"[21] e gli investimenti al riguardo sono sempre più consistenti, specie se si considera che provengono dalle grandi aziende tecnologiche che dominano il mercato. Già nel 2017 *Facebook Reality Labs* (FRL) ha fondato il progetto *Brain-Computer Interface* (BCI) con l'obiettivo di sviluppare un'interfaccia neurale vocale silenziosa e non invasiva, che consenta alle persone di digitare semplicemente immaginando le parole che desiderano dire. *Facebook* ha di recente annunciato di voler investire su interfacce neurali consistenti in dispositivi basati sul polso alimentati dall'elettromiografia[22].

Microsoft ha investito nell'iniziativa di intelligenza artificiale di un noto imprenditore americano, che nel 2017 ha creato la società di

---

[19] L. PALAZZANI, *Il potenziamento umano. Tecnoscienza, etica e diritto*, 2015; M.B. RUSSO, M.C. STETZ, T.A. STETZ TA, *Ethical considerations. Cogneuticals in the military*, cit., 2013.

[20] Diversi dispositivi sono già presenti sul mercato e registrano l'attività elettrica del cervello; questi in alcuni casi sfruttano anche il canale della neuromodulazione rilasciando delle scariche elettriche a determinate aree del cervello con lo scopo di migliorare i processi di concentrazione o ridurre i livelli di *stress*. Ciò costituisce l'oggetto del lavoro di una *startup* americana, EMOTIV Inc., che ha messo sul mercato un *headset* indossabile chiamato *EMOTIV Insight* che, grazie ad una sorta di cuffia che utilizza tecniche proprie degli strumenti per l'elettroencefalografia impiegati nei laboratori di ricerca, riesce a registrare le emozioni, lo stress e il livello di attenzione di chi lo indossa. Tali dati sono poi analizzati da algoritmi per migliorare il livello di produttività. (https://www.emotiv.com/insight/). In dottrina con specifico riferimento all'impiego di tali tecniche al di fuori dell'ambito medicale M.D. TENNISON, J.D. MORENO, *Neuroscience, Ethics and National Security: the state of the art*, in *PLoS Biology*, 2012, 1-4.

[21] M. IENCA, *Neurodiritti: storia di un concetto e scenari futuri*, in *Atti del Convegno* "Privacy *e neurodiritti. La persona al tempo delle neuroscienze*, 2021, 35-54; M. IENCA, E. VAYENA, *Direct-to-Consumer Neurotechnology*: *What Is It and What Is It for?*, in *AJOB Neuroscience*, 2019, 149-151; A. WEXLER, P. B. REINER, *Oversight of direct-to consumer neurotechnologies*, in *Science*, 2019, 234-235; M. IENCA, P. HASELAGER, E. EMANUEL, *Brain leaks and consumer technology*, in *Nature*, 2018, 805-810.

[22] https://www.facebook.com/TechatMeta/videos/1146186389155473/?t=86

ricerca medica "*Neuralink*", con sede in California[23], che opera nel campo delle neurotecnologie invasive tramite impianti neurali[24].

Con specifico riferimento al commercio e ai *social network*, inoltre, è sempre più diffusa l'applicazione delle tecniche neuroscientifiche al *marketing*, tanto che la disciplina emergente nota con il termine *neuromarketing* si propone di analizzare i processi che avvengono nella mente del consumatore e che influiscono in maniera inconsapevole sulle decisioni di acquisto, così come il livello di coinvolgimento emotivo rispetto ad un certo *brand*[25].

Da ultimo, si considerino anche gli impieghi di natura coercitiva delle neurotecnologie. È il caso della Cina che ha imposto l'utilizzo di fasce indossabili per controllare il livello di attenzioni degli alunni in classe[26], nonché dispositivi di "*neuromonitoring*" installati in luoghi di lavoro per calibrare i flussi di produzione.

9.3. Dati neurali e dati mentali: il procedimento di inferenza inversa e le neurotecnologie di consumo

Il fenomeno sopra descritto del progressivo ampliamento dell'utilizzo delle neurotecnologie al di fuori dell'ambito clinico, rispetto al quale è stata utilizzata l'espressione "rivoluzione neurotecnologica" [27], non è il solo elemento che ha determinato la progressiva attenzione per le questioni etiche e giuridiche sollevate dalle neurotecnologie.

I recenti studi in materia, infatti, prendono in considerazione le implicazioni delle neurotecnologie come da ultimo potenziate grazie ai meccanismi di *machine learning* e *deep learning*. Lo sviluppo dell'intelligenza artificiale, infatti, ha consentito di ampliare notevolmente le

---

[23] https://neuralink.com/

[24] Ha fatto molto scalpore la notizia che la società di Helon Musk sia riuscita a far giocare una scimmia rilevandone i segnali celebrali https://www.youtube.com/watch?v=rsCul1sp4hQ.

[25] Per un ampio inquadramento del fenomeno L. CATTUBO, A. MENDOLA, *Le scelte "inconsapevoli" nelle nuove dinamiche d'acquisto. Il neuromarketing e la tutela del consumatore-follower*, 2022.

[26] https://www.theguardian.com/world/2019/nov/01/chinese-primary-school-halts-trial-of-device-that-monitors-pupils-brainwaves

[27] G. SCOTT, *The neurotechnology revolution has arrived* in *The Futurist*, 2013, 6-7.

funzionalità dei dispositivi in questione, profondamente innovati nella capacità di acquisizione del dato in maniera automatizzata.

Ciò impone una più ampia riflessione giuridica in merito alla necessità di tutelare il dominio della mente da intrusioni non autorizzate, partendo dall'analisi dei dati che le neurotecnologie sono in grado di rilevare attraverso la registrazione e decodificazione dall'attività celebrale dell'utente.

Si tratta, infatti, non soltanto di dati che attengono alla struttura e al funzionamento del cervello, ovvero di c.d. "*human brain data*"[28] o dati celebrali/neurali che rivelano informazioni sulla condizione clinica e, dunque, sulla salute di una persona, ma anche di dati ulteriori attinenti alla sfera più intima del soggetto, non altrimenti rilevabili dall'esterno (*mental data* o dati/stati mentali).

Grazie ad algoritmi intelligenti alla base delle più moderne neurotecnologie, queste possono essere in grado di rilevare anche informazioni ulteriori rispetto al dato clinico (dato neurale), informazioni (ovvero dati) che, grazie ad un procedimento di c.d."inferenza inversa"[29], rivelano *stati mentali*[30] inespressi (dato mentale).

In altre parole, dall'analisi dei dati neurali relativi ad una determinata attività celebrale registrata dai dispositivi neurotecnologici è possibile inferire che nel cervello dell'utente si sia attivato anche un

[28] M. Ienca, *Common Human rights challenges raised by different applications of neurotechnologies in the biomedical fields*, 2021, 1-82.

[29] R.A. Poldrack, *Inferring mental states from neuroimaging data: from reverse inference to large-scale decoding*, in *Neuron*, 2011, 692-697.

[30] Sulla definizione di *stato mentale* M. Ienca, G. Malgieri, *Mental data protection and the GDPR*, in *Journal of Law and the Biosciences*, 2022, 1-19, "*we define mental state' any conglom- eration of mental representations and propositional attitudes that corresponds to the experience of thinking, remembering, planning, perceiving, and feeling*".

diverso processo cognitivo corrispondente ad un discorso silenzioso (*inner speach*) [31], ad un ricordo[32], ad una intenzione nascosta[33].

Ciò che le neurotecnologie sono attualmente in grado di mostrarci non corrisponde al contenuto semantico di un pensiero o di un ricordo; tuttavia, queste consentono di stabilire una corrispondenza tra i correlati neurali di una certa attività celebrale e le informazioni su determinati stati mentali.

Occorre tenere ben presente, pertanto, la distinzione tra i dati neurali (attinenti alla struttura e al funzionamento del cervello) e i "*dati mentali*" (generati dai dati neurali grazie al procedimento di inferenza inversa), ovvero qualsiasi informazione che può essere organizzata ed elaborata per dedurre gli stati mentali di una persona, compresi i suoi stati cognitivi ed affettivi[34] come ricordi, emozioni[35] ed intenzioni.

La complessità del tema trattato rende evidente che una riflessione che si riferisca unicamente agli aspetti etici e giuridici rischierebbe di risultare parziale in quanto non in grado di ricomprendere tutti i profili di complessità che necessitano uno studio specifico.

---

[31] D.A. MOSES, M.K. LEONARD, J. G. MAKIN, E.F. CHANG, E. F., *Real-time decoding of question-and-answer speech dialogue using human cortical activity* in *Nature Communications,* 2019, 3096, in cui si può leggere che grazie a registrazioni EEG intracraniche si è rilevata l'attività celebrale legata al discorso interiore. Gli stessi risultati sono stati ottenuti grazie a scansioni fMRI e segnali elettrocorticografici ad alta densità.

[32] Sulla capacità di prevedere un ricordo J. CHEN, Y.C. LEONG, C.J. HONEY, C. H. YONG, K.A. NORMAN, U. HASSON, *Shared memories reveal shared structure in neural activity across individuals*, in *Nature neuroscience,* 2019, 115-125, studio in cui è stato possibile identificare dettagli sui ricordi delle persone coinvolte basandosi unicamente sui dati neurali decodificati dall'algoritmo.

[33] M. BLES, J.D. HAYNES, *Detecting concealed information using brain-imaging technology*, in *Neurocase,* 2008, 82-92, ricerca in cui ai partecipanti veniva richiesto di decidere se aggiungere o sottrarre due numeri e mantenere la loro intenzione segretamente nascosta per alcuni secondi. Tale intenzione nascosta è stata decodificata prima che i partecipanti la manifestassero (scegliendo di aggiungere o sottrarre). Sulla possibilità di decodificare in anticipo l'intenzione del soggetto prima che questi effettui la sua scelta C.S. SOON, A.H. HE, S. BODE, J.D. HAYNES, *Predicting free choices for abstract intentions* in *Proceedings of the National Academy of Sciences,* 2013 , 6217-6222.

[34] Così M IENCA, G. MALGIERI, *Mental data protection and the GDPR*, cit. 4, "*We define 'mental data' any data that can be organized and processed to infer the mental states of a person, including their cognitive, affective, and conative states*."

[35] Sul legame tra attività neurale ed emozioni, su come queste ultime siano in grado di influenzare nuove, non correlate, informazioni A. TAMBINI, U.RIMMELE, E. A PHELP, L. DAVACHI, *Emotional brain states carry over and enhance future memory formation,* in *Nature Neuroscience*, 2017, 271-278.

Si tratta di un tema che richiede un approccio interdisciplinare e che non può prescindere dalla preventiva analisi delle questioni tecniche e di analisi comportamentale che tali tecnologie pongono, che hanno immediate ricadute anche da un punto di vista etico e giuridico.

I profili di rischio da un punto di vista tecnico che occorre tenere presente attengono, in primo luogo, al possibile malfunzionamento dell'algoritmo che potrebbe determinare *bias cognitivi*, inducendo nell'utente scelte e/o azioni potenzialmente illecite, oltre che non volute dal soggetto agente[36]. In secondo luogo, come ogni strumento tecnologico, anche le interfacce connesse al cervello portano con sé il serio rischio che possano essere alterate, con evidenti problemi di *cyber sicurezza* e di riflessi negativi non solo dal punto di vista dell'accesso illecito e non autorizzato ai dati neurali e mentali rilevati dal dispositivo, ma anche della possibile e conseguente alterazione dell'attività celebrale dell'utente[37], che in questo caso risulterebbe negativamente incisa non a causa di un malfunzionamento ma da una volontaria manomissione del dispositivo, con diverse considerazioni in ordine alla responsabilità per i danni arrecati.

A ciò si aggiunga che diversi sono i profili di criticità che sono stati rilevati in seguito all'analisi comportamentale di pazienti sottoposti a sedute di terapia con *Deep Brain Stimulation*, in considerazione di disturbi insorti successivamente alla terapia ed ulteriori rispetto alla patologia inizialmente tratta[38].

Tutto quanto precede rileva in relazione a diversi livelli di analisi.

---

[36] D. Danks, A. London, *Algorithmic bias in autonomous systems*, in *Int. Joint Conf. Artif. Intell.* 2017, 4691–469 sostengono che non tutti i *bias* algoritmici sono da valutare negativamente in quanto alcuni potrebbero anche servire a mitigare gli effetti pregiudizievoli di altri *bias*.

[37] M. Ienca, *Common Human rights challenges raised by different applications of neurotechnologies in the biomedical fields*, cit.; P. Chaudhary, R. Agrawal, *Emerging threats to security and privacy in brain computer interface* in *International Journal of Advanced Studies of Scientific Research*, 2018, 340-344; M. Ienca, P. Haselager, *Hacking the brain: brain–computer interfacing technology and the ethics of neurosecurity* in *Ethics and Information Technology*, 2016, 117-129.

[38] D.D. Dougherty, A.R. Rezai, L.L. Carpenter, R.H. Howland, M.T. Bhati, J.P. O'Reardon, et al. *A randomized sham- controlled trial of deep brain stimulation of the ventral capsule/ventral striatum for chronic treatment-resistant depression*, in *Biol. Psychiatry, 2015* 240–248, B.D. Greenberg, L.A. Gabriels, D.A. Malone, A.R. Rezai, G.M. Friehs, M.S. Okun, et al., *Deep brain stimulation of the ventral internal capsule/ventral striatum for obsessive-compulsive disorder: worldwide experience*, in *Mol. Psychiatry*, 2010, 64–79.

La prima considerazione prende spunto dalla valutazione delle caratteristiche tecniche dei diversi dispostivi neurotecnologici. Laddove si tenga conto che esistono degli strumenti che sono in grado non solo di registrare e decodificare il dato neurale ma anche di riscrivere l'attività celebrale dell'utente, si pone una evidente questione di tutela del principio di autodeterminazione dell'individuo che potrebbe non essere più in grado di operare in piena autonomia, con evidenti riflessi, in primo luogo, sulla sua identità personale e, come logico corollario, sul regime di responsabilità per le azioni compiute.

In secondo luogo, l'accesso al dato mentale, sia esso collegato o meno ad una condizione clinica, impone di valutare quale sia la base giuridica del trattamento dei dati in tal modo rilevati. Vi è pertanto una chiara esigenza di salvaguardare un diritto fondamentale quale la *privacy* dei dati mentali, specie quando questi non siano qualificabili come dati sanitari[39].

Il punto in cui le riflessioni su entrambi i profili di rilevanza giuridica riferiti coincidono attiene alla mancanza di un *framework* normativo specifico che consenta di disciplinare le eterogenee e peculiari situazioni giuridiche connesse all'utilizzo delle neurotecnologie.

Occorre, pertanto, chiedersi quale siano i principi etici e le norme giuridiche applicabili a tali nuove fattispecie, ovvero interrogarsi se sia sufficiente ricercare nel sistema norme che in via analogica siano applicabili al di fuori delle ipotesi espressamente previste oppure se sia preferibile accogliere le istanze volte all'introduzione di un nuovo impianto normativo sul punto, che tenga conto della complessità e rilevanza degli interessi in gioco.

9.3.1. (segue) I profili di tutela dell'identità personale: tra principio di autodeterminazione e responsabilità del soggetto agente

Il concetto di *vulnerabilità relazionale* in precedenza menzionato sembra ben esprimere lo stato soggettivo di insita debolezza che riguarda le persone che si rapportano a *devices* neurotecnologici come da ultimo potenziati dai sistemi di intelligenza artificiale.

Appare di immediata percezione che alterare la capacità cognitiva di un soggetto comporti anche l'alterazione della sua identità personale[40]. Ciò in quanto la libera autodeterminazione del soggetto, ovvero la sua capacità di adottare scelte libere ed autonome rispetto alla sua sfera di interessi, è la principale manifestazione dell'identità personale del soggetto. Se tale autonomia decisionale viene ad essere limitata da strumenti tecnologici, sebbene progettati per migliorare le condizioni di vita di persone con gravi patologie, ciò pone una questione etica e giuridica di non poco conto. Occorre valutare, infatti, se nel normale bilanciamento di interessi che dovrebbe porsi a base di ogni disciplina normativa sia più rilevante consentire il recupero di determinate funzioni psichiche o motorie, piuttosto che apprestare adeguata tutela dell'identità del soggetto, che non può in ogni caso essere sminuita o celata da un'attività celebrale che non è più espressione del suo naturale funzionamento.

Quanto detto è tanto più rilevante se lo si riferisce alle neurotecnologie in ambito extra-clinico, in cui le limitazioni della identità personale del soggetto non trovano fondamento nella tutela di un diritto del pari fondamentale quale la salute, ma in mere logiche economiche e di mercato[41] che rafforzano la proposta di un quadro normativo chiaro e preciso sul punto, che eviti la mercificazione dei dati attinenti al dominio della mente.

Altro profilo di vulnerabilità connesso alla identità personale del soggetto attiene ai riflessi sul piano dell'azione e del relativo regime di responsabilità di chi utilizza *devices* neurotecnologici. In una condizione in cui l'identità personale risulta alterata dai pervasivi stimoli provenienti dall'esterno – dai dispositivi a base algoritmica – potrebbe risultare difficile, sul piano della qualificazione giuridica, definire con esattezza se il soggetto che ha agito lo ha fatto in maniera autonoma ovvero in una condizione di limitazione della sua capacità di autodeterminazione; occorre, in altre parole, verificare se il comportamento posto in essere dal soggetto sia a lui effettivamente imputabile da un

---

[40] F. Gilbert, M. Cook, T. O'Brien, T., J. Illes, *Embodiment and estrangement: Results from a first-in-human "intelligent BCI" trial*, in *Science and engineering ethics,* 2019, 83-96; F. Gilbert, E. Goddard, J.N.M. Viaña, A. Carter, A., M. Horne, *I miss being me: Phenomenological effects of deep brain stimulation* in *AJOB neuroscience,* 2017, 96-109.

[41] Si consideri il noto studio sul contagio emozionale condotto dal più grande *social network* al mondo quale Facebook. Sul punto A. D. I. Kramera, E. J. Guilloryb, and J. T. Hancockb, *Experimental evidence of massive-scale emotional contagion through social networks* , in PNAS, 2014.

punto di vista giuridico[42]. In quest'ultimo caso, laddove dal comportamento del soggetto agente ne derivino dei pregiudizi a carico di soggetti terzi, si pone in primo luogo il problema di rilevare il nesso di causalità tra l'azione – non liberamente determinata – e il danno prodotto. Inoltre, occorre stabilire chi sia il responsabile di un danno provocato da un'azione posta in essere da un soggetto la cui volontà probabilmente non si è formata in maniera autonoma.

In assenza di un quadro normativo sul punto, anche in questo caso il riferimento ai più importanti testi internazionali in materia di tutela dei diritti umani non consente di ritrovare un valido fondamento normativo per la tutela dell'identità personale in relazione alle neurotecnologie[43].

9.3.2. (segue) Le istanze di tutela del diritto alla *privacy* del dominio mentale

Discutere di tutela della *privacy* anche in relazione al dominio della mente significa interrogarsi in via preliminare sulla natura giuridica dei dati che le neurotecnologie sono in grado di rilevare.

A tal fine appare utile la distinzione prima riferita tra dati neurali e dati mentali.

I primi, riferendosi al funzionamento e alla struttura del cervello, consentono di identificare il soggetto cui si riferiscono suggerendo,

---

[42] P. HASELAGER, *Did I Do That? Brain–Computer Interfacing and the Sense of Agency*, in *Mind and Machines*, 2013, 405-418.

[43] In particolare, non vi è certezza che l'art. 3 della Convenzione dei Diritti Fondamentali dell'Unione Europea che disciplina il diritto all'integrità psichica possa ricomprendere anche la tutela delle possibili alterazioni del processo celebrale determinato dalle neurotecnologie. Sul punto S. FUSELLI, *Profili filosofico-giuridici di un mutamento in atto*, *in Journal of Ethics and Legal Technologies*, 2020, 2-30. Al riguardo, una primo approccio al tema suggerisce di operare una interpretazione evolutiva e tecnologicamente orientata non solo della norma innanzi citata, ma anche degli articoli 7 e 9 della Convenzione, nonché dell'art. 22 GDPR in relazione alla decisione algoritmica; così O. POLLICINO, *Costituzionalismo,* privacy *e neurodiritti*, in *Atti del Convegno "*Privacy *e neurodiritti. La persona al tempo delle neuroscienze*, 2021, 69-84. Per altro verso, vi è chi propone di adottare una "Dichiarazione Universale su Neuroscienze e Diritti Umani" al fine di stabilire principi giuridici e valori condivisi a livello internazionale. Così F.G. PIZZETTI, *Brain- Computer Interfaces and the Protection of the Fundamental Rights of the Vulnerable Persons*, in *Neuroscience and Law*, 2021, 291-318.

pertanto, una prima qualificazione giuridica dei dati neurali quali dati personali ai sensi dall'art. 4, paragrafo 1 del GDPR[44].

Tuttavia, in quanto tali, i dati neurali sono anche espressione di una condizione clinica dell'interessato, intesa quest'ultima non necessariamente come condizione di carattere patologico ma anche di benessere fisico e psichico[45].

Pertanto, i dati neurali non sono semplici dati personali identificativi ma "*dati relativi alla salute*" ai sensi dell'art. 4, paragrafo 15 GDPR[46]. Da ciò ne deriva che la base giuridica del trattamento deve essere quella stabilita per "*categoria particolari di dati personali*" di cui all'art. 9 GDPR, con una tutela rafforzata che si sostanzia nel "consenso esplicito" dell'interessato.

La qualificazione in termini di dato personale, invece, non è pacifica in relazione al dato mentale. Quest'ultimo, infatti, se collegato ad altri dati che consentano l'individuazione certa dell'interessato (come nel caso del dato neurale), può certamente qualificarsi come dato personale. Questa è la prima fattispecie che può essere oggetto di analisi e che pare riferirsi ai dati mentali generati in seguito alla registrazione e decodifica del dato neurale con i dispositivi neurotecnologici utilizzati in ambito clinico, come risultato dal procedimento di inferenza inversa, che potrebbe rilevare anche stati mentali come emozioni o ricordi e non solo la condizione clinica dell'interessato.

In questo primo caso, lo stretto collegamento tra il dato neurale ed il dato mentale suggerisce una qualificazione di quest'ultimo come dato personale, ciò in quanto la lettura congiunta con il dato neurale è in grado di consentire l'identificazione dell'interessato.

Il dubbio sulla qualificazione del dato mentale si pone con maggiore forza nelle ipotesi in cui esso sia acquisito al di fuori dell'ambito medico e, pertanto, del tutto svincolato dal dato neurale, come nel caso delle neurotecnologie di consumo, le quali potrebbero rilevare dati

---

[44] Sull'adeguatezza della disciplina contenuta nel GDPR rispetto ai dati ottenuti con le neurotecnologie S. Raiuney, K. McGillivray, S. Akintoye, T. Fothergrill, C. Bublitz, B. Stahl, *Is the European Data Protection Regulation sufficient to deal with emerging data concerns relating to neurotechnology?*, in *Journal of Law and Biosciences*, 2021, 1-19.

[45] "*La salute è il bene dell'interezza e sanità dell'organismo umano*" Così Bianca, *La norma giuridica e i soggetti*, in *Diritto Civile*, 2002, 162.

[46] S. Yang, F. Deravi, *On the Usability of Electroencephalographic Signals for Biometric Recognition: A Survey*, in *Trans. Hum.-Mach. Syst*., 2017, 958-969; K. Aloui, A. A Nait-Ali, M. Saber Naceur, *Using Brain Prints as New Biometric Feature for Human Recogni- tion*, in *Pattern Recogn*., 2017.

mentali pur non accedendo direttamente al funzionamento del cervello inteso come complesso biologico. In questo caso, un valido aiuto alla qualificazione giuridica pare potersi ritrovare nell'art. 4, 1 paragrafo GDPR che considera idonei all'identificazione del soggetto anche "*uno o più elementi caratteristici della sua identità psichica*" sebbene la medesima disposizione non chiarisca cosa debba intendersi per *identità psichica*. Pertanto, solo in via interpretativa possono allo stato qualificarsi i dati mentali come dati personali, ovvero laddove sia possibile ritenere che una emozione o un ricordo siano dati tali da consentire di identificare in maniera univoca un soggetto, anche senza fare riferimento ai suoi dati neurali.

Ma vi è un ulteriore livello di analisi che va approfondito in merito alla qualificazione giuridica dei dati relativi al dominio mentale e che non costituisce una mera specificazione di quanto detto in relazione alla definizione di dato personale, in quanto rileva sul piano ben più rilevante dell'individuazione della base giuridica del trattamento.

La fattispecie innanzi analizzata, delle neurotecnologie in ambito clinico, determina che il trattamento dei dati mentali presupponga la loro qualificazione come dati sanitari in quanto ulteriore espressione dell'integrità psicofisica dell'interessato (ovvero della sua salute), già ricavata in maniera diretta dall'analisi del dato neurale[47]. Pertanto, il vuoto normativo parrebbe, solo in questo caso, attenuato dalla possibile applicazione in via analogica dell'art. 9 GDPR.

La fattispecie diviene più complessa se si considerano le neurotecnologie di consumo che, sebbene siano in grado di rilevare dati mentali (es. emozioni), non rilevano la condizione di salute dell'interessato perché non rilevano il dato neurale.

Pertanto, considerare la salute come il bene dell'interezza e sanità dell'organismo umano induce a qualificare i dati mentali come dati sanitari solo quando siano associati a dati neurali. Diversamente, non poter accedere al dato neurale implica che i dati mentali, in sé e per sé considerati, non possano essere qualificati come dati sanitari, in quanto non riescono da soli a mostrare lo stato di salute (sebbene fisiologico e non patologico) dell'interessato.

---

[47] M. IENCA, G. MALGIERI, *Mental data protection and the GDPR*, cit., 9 ss. i quali propendono per la qualificazione del dato mentale come dato personale relativo alla salute intesa in senso ampio ed estensivo, per ricomprendere anche gli stati mentali affettivi e cognitivi indicatori di una condizione clinica non patologica.

In una prospettiva comparatistica, con specifico riferimento alle tecniche di identificazione biometrica di tipo comportamentale, si consideri che secondo l'ICO (*Information Commissioner's Office*)[48], organismo indipendente del Regno Unito istituito per sostenere i diritti di informazione e con specifiche competenze anche in tema di *Data Protection*, i dispositivi che sono in grado di operare un'analisi dello sguardo (c.d. *eye-tracking*) registrano dati di tipo biometrico così come definiti dagli articolo 4 e 9 e dal considerando 51 del UK GDPR[49]; pertanto, se un *devices* è in tal modo in grado di registrare emozioni o altri dati mentali che sono qualificabili come dati biometrici, per gli stessi risulterà applicabile la relativa normativa sul punto.

Tale ultima fattispecie (dati mentali che non siano allo stesso tempo anche dati neurali e, dunque, qualificabili come dati sanitari) non è prevista nel nostro GDPR, che si caratterizza per una evidente lacuna, laddove non definisce e non disciplina i dati mentali[50]. Residuerebbe, pertanto, la possibilità di poter accedere alla maggior tutela di cui all'articolo 9 GDPR soltanto laddove i dati mentali siano in grado di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'orientamento sessuale di una persona.

---

[48] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

[49] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (*United Kingdom General Data Protection Regulation*) disponible qui https://www.legislation.gov.uk/eur/2016/679/article/9.

[50] Sul punto gli autori che si sono occupati della questione concordano nel rilevare la lacuna del GDPR al riguardo ma per motivazioni differenti. M IENCA, G. MALGIERI, *Mental data protection and the GDPR*, cit., ritengono che la lacuna sia dovuta alla mancata inclusione nella previsione normativa dell'art. 9 GDPR come dati personali particolari dei dati relativi a pensieri, emozioni ed altri stati mentali non collegati o non riconducibili alla salute o ad altri ambiti presi in considerazione dalla norma; S. RAINEY, K MCGILLIVRAY, S. AKINTOYE, T. FOTHERGILL, *Is the European Data Protection Regulation Sufficient to Deal with Emerging Data Concerns Relating to Neurotechnology?* in *Journal of Law and the Biosciences*, 2020, 1-19 partono, invece, dalla considerazione che i dati particolari di cui all'art. 9 GDPR sono tali in considerazione delle finalità del trattamento; pertanto, ritengono che se lo scopo del trattamento dei dati mentali inizialmente dichiarato non è legato alla salute, o ad altre finalità contemplate dalla norma, gli stessi non possono essere considerati dati sensibili.

9.4. Una possibile disciplina delle neurotecnologie: i *neurorights*

Le questioni etiche e giuridiche connesse al tema delle neurotecnologie appaiono notevolmente complicate dalla mancanza di un quadro normativo di riferimento, ovvero di una disciplina specifica in relazione alla tutela dei diritti fondamentali dei soggetti che si rapportano a *devices* neurotecnologici. Limitarsi ad una interpretazione delle norme già esistenti non garantisce la tutela effettiva di diritti e valori fondamentali come la *privacy*, l'autonomia e l'integrità psicofisica.

Ciò ha indotto una parte della più attenta dottrina ad elaborare una proposta per l'introduzione di un nuovo complesso di diritti fondamentali c.d. "*neurorights*".

Si tratta di un mutato approccio al tema delle neurotecnologie che tiene conto della necessità di tutelare la mente da accessi illeciti e non autorizzati ai relativi dati attraverso i seguenti nuovi diritti[51]: *privacy* mentale, integrità mentale, libertà cognitiva e continuità psicologica.

Per *privacy mentale* deve intendersi il diritto fondamentale alla tutela della *privacy* con specifico riferimento al dominio della mente e, dunque, degli stati mentali, che in precedenza si è visto non essere necessariamente collegati al dato neurale inteso come informazione sullo stato di salute di una persona. Vi è, pertanto, una distinzione al riguardo che riflette sul piano della disciplina la distinzione in merito alla natura giuridica dei dati relativi alla mente. Ciò in quanto dalla *privacy* mentale deve distinguersi la *neuroprivacy*, intesa come tutela della *privacy* del dato neurale in sé e per sé considerato, anche se da questo non si ricavino inferenze sugli stati mentali dell'individuo.

L'*integrità mentale*[52] è intesa come diritto a non subire manipolazioni della propria attività celebrale attraverso il "*brain hackin*", ovvero la manomissione intenzionale del dispositivo che consente di arrecare un grave pregiudizio per l'utente.

La *libertà cognitiva* si articola in una libertà positiva e in una negativa: la prima implica la possibilità per ciascuno di fare scelte prive di condizionamenti esterni rispetto alla propria attività cognitiva; la

---

[51] M. IENCA, R. ADORNO, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life science Society & Policy*, 2017, 1-27.

[52] Sul punto anche T. DOUGLAS, L. FORSBERG, *Tree Rationales for a Legal Rights to Mental Integrity*, in *Palgrave Studies in Law, Neuroscience, and Human Behavior*, 2021, 179-201; A. LAVAZZA, *Freedom of thought and Mental Integrity: the moral requirements for any neural prosthesis*, in *Frontiers in Neuroscience*, 2018, 1-10.

seconda consente di liberarsi in qualsiasi momento dai condizionamenti esterni non autorizzati della propria attività celebrale.

Infine, la continuità psicologica consente di preservare la propria identità personale da alterazioni esterne non autorizzate.

La teorizzazione dei "neurodiritti" è stata da più parti ripresa ed ampliata nell'ottica di evidenziare la necessità di una disciplina unitaria in tema di neurotecnologie.

Più in particolare, è stata posta l'attenzione sull'opportunità non solo di introdurre nuovi diritti fondamentali in relazione al dominio della mente[53] – solo in parte coincidenti con quelli innanzi analizzati[54] – ma che gli stessi siano inseriti nei trattati internazionali e, più in particolare, nella Dichiarazione Universale dei Diritti Umani.

Di neurodiritti si è occupato anche il Comitato sulle neurotecnologie dell'OCSE che, oltre a porre ancora una volta l'attenzione sulla *privacy* mentale e sulla libertà cognitiva, ha adottato il primo documento che fissa uno *standard* internazionale sull'innovazione responsabile nelle neurotecnologie, applicabile in ogni fase del processo di innovazione - ricerca, trasferimento tecnologico, investimento,

---

[53] R. JUSTE, J. GENSER, S. HERRMANN, *It's Time for Neuro-Rights. New Human Rights for the Age of Neurotechnology*, in *Horizons*, 2021, 154-164; R. YUSTE, S. GOERING, BI. G., CARMENA, J. M., CARTER, et al., *Four ethical priorities for neurotechnologies and AI*, in *Nature* 2017, 159–163; S. GOERING, R. YUSTE, *On the Necessity of Ethical Guidelines for Novel Neurotechnologies*, in *Cell 167*, 2016, 882-885. In prospettiva critica sui neurodiritti D. BORBÓN, L. BORBÓN, *A critical perspective on neurorights: comments regarding ethics and law*, in *Frontiers in Human Neuroscience*, 2021, 1-4.

[54] *The Right to Personal Identity*: Boundaries must be developed to prohibit technology from disrupting the sense of self. When Neurotechnology connects individuals with digital networks, it could blur the line between a person's consciousness and external technological inputs. *The Right to Free-Will*: Individuals should have ultimate control over their own decision making, without unknown manipulation from external neurotechnologies. *The Right to Mental Privacy*: Any data obtained from measuring neural activity ("NeuroData") should be kept private. Moreover, the sale, commercial transfer, and use of neural data should be strictly regulated. *The Right to Equal Access to Mental Augmentation*: There should be established guidelines at both international and national levels regulating the development and applications of mental-enhancement neuro- technologies. These guidelines should be based on the principle of justice and guarantee equality of access to all citizens. *The Right to Protection from Algorithmic Bias*: Countermeasures to combat bias should be the norm for machine learning. Algorithm design should include input from user groups to foundationally address bias. https://neurorightsfoundation.org/

commercializzazione, regolamentazione - al fine di anticipare le sfide etiche, giuridiche e sociali sollevate dalle nuove neurotecnologie legate alla salute, massimizzando i benefici e minimizzando i rischi, promuovendo un'innovazione che sia al tempo stesso inclusiva e non che generi situazioni pregiudizievoli[55].

Il Comitato Internazionale di Bioetica dell'Unesco ha di recente adottato una *Raccomandazione sull'etica dell'intelligenza artificiale*[56] in cui viene precisato che gli Stati membri debbono garantire che ogni sistema di IA, ivi inclusi le neurotecnologie e le interfacce di BCI, rispetti i diritti umani e le libertà fondamentali, preservando la dignità ed autonomia delle persone vulnerabili o in situazioni di vulnerabilità. Dunque, la considerazione iniziale relativa alla *vulnerabilità relazionale* determinata dalle neurotecnologie sembra trovare un valido riferimento anche nella Raccomandazione Unesco sull'Intelligenza Artificiale.

Non solo dichiarazioni di principio ma anche un preciso intervento normativo al riguardo da parte del Cile, ad oggi l'unico Paese al mondo che, con la "Ley 21.383_*Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías*", oltre ad aver dato una precisa definizione di *dato neurale*[57] e di *neurotecnologie*[58], ha approvato una regolamentazione delle stesse al fine di proteggere i diritti all'identità personale, al libero arbitrio, alla *privacy* mentale, all'accesso equo alle tecnologie che aumentano le capacità umane e il diritto alla protezione contro pregiudizi e discriminazioni.

---

[55] *OECD Recommendation on Responsible Innovation in Neurotechnologies*, adottata in data 11 novembre 2019 e disponibile qui https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm.

[56] Adottata il 24 novembre 2021 dalla Conferenza Generale dell'UNESCO, quale primo strumento normativo che fissa i principi etici dell'IA nel rispetto dei diritti umani e delle libertà fondamentali *Recommendation on the ethics of artificial intelligence***.** *Art.* 126. "*Member States should ensure that human-robot interactions comply with the same values and principles that apply to any other AI systems, including human rights and fundamental freedoms, the promotion of diversity, and the protection of vulnerable people or people in vulnerable situations. Ethical questions related to AI-powered systems for neurotechnologies and brain-computer interfaces should be considered in order to preserve human dignity and autonomy.*", disponibile qui https://unesdoc.unesco.org/ark:/48223/pf0000381137

[57] Dato neuronal "*la información obtenida de la actividad de las neuronas que contiene una representación de la actividad cerebra*l".

[58] Neurotecnologías al "*conjunto de dispositivos o instrumentos que permiten una conexión con el Sistema Nervioso Central para la lectura, registro o modificación de la actividad cerebral y de la información proveniente de ella*".

Il presupposto di tale iniziativa legislativa è rappresentato da un nuovo e diverso concetto di *privacy* che si concentra sui dati neurali e sulle informazioni riguardanti gli stati mentali che da questi possono essere generati, con l'obiettivo di considerare i dati neurali alla stregua di un tessuto organico, che in quanto tale non può essere oggetto di atti di disposizione a titolo oneroso.

Sul territorio europeo, invece, con particolare riferimento alla Spagna, sebbene non sia stato ancora adottato un vero e proprio corpo normativo per la disciplina delle neurotecnologie, nella *Carta Derecho Digital*[59] si è fatto esplicito riferimento all'adozione di una legge per la regolamentazione delle neurotecnologie al fine di tutelare l'autonomia e l'integrità psicofisica dei soggetti, per garantire un utilizzo corretto dei dati che queste sono in grado di registrare. Si è, inoltre, richiamata l'attenzione sulla necessità che la regolamentazione riguardi anche le neurotecnologie impiegate al di fuori del contesto clinico.

Infine, di notevole rilevanza appare la recentissima posizione assunta sul punto dal Parlamento Europeo che ha espressamente invitato la Commissione Europea ad intervenire con l'obiettivo di proteggere il cervello dai rischi connessi alle neurotecnologie come da ultime potenziate dall'intelligenza artificiale, prospettando la possibilità che tali diritti siano inseriti nella Dichiarazione Universale dei Diritti Umani[60]. Più in particolare, si tratta di un *report* sull'intelligenza artificiale in cui si menzionano espressamente i seguenti *neurorights*: *rights to identity, free will, mental privacy, equal access to brain augmentation advances and protection from algorithmic bias*. Con tale documento il legislatore europeo pone l'attenzione sulle esigenze di tutela connesse al dominio della mente, raccogliendo le istanze innanzi prospettate che mettono ben in evidenza come una mera interpretazione in via analogica delle norme già esistenti non è da sola in grado di risolvere adeguatamente le questioni eticamente e giuridicamente rilevanti poste dalle neurotecnologie.

---

[59] Adottata nel mese di luglio 2021 e disponibile qui https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/Carta_Derechos_Digitales_RedEs_140721.pdf

[60] *Report on artificiale intelligence in a digital age* del Parlamento Europeo pubblicato in data 5 aprile 2022, disponibile qui https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_EN.html.

9.5. Neurodiritto e neurodiritti: quale disciplina fornirebbe adeguata tutela a tutti gli interessi coinvolti?

L'intervento del legislatore cileno non può che essere valutato positivamente alla luce di una evidente esigenza che si pone rispetto alla tutela dei soggetti che si relazionano con dispositivi neurotecnologici.

Ciò in considerazione dei possibili pregiudizi connessi alla mancanza di un pieno controllo della propria sfera emotiva e cognitiva quale riflesso pratico di un sempre più incisivo potenziamento delle neurotecnologie grazie all'intelligenza artificiale che, se da un lato, rendono tali dispostivi maggiormente efficienti sul piano della funzionalità, dall'altro, tendono ad automatizzare vari processi rispetto ai quali il singolo potrebbe non essere in grado di sottrarsi.

Deve, pertanto, essere posta la giusta attenzione sui profili di rischio delle neurotecnologie che, sebbene consentano di conseguire risultati ottimali in ambito clinico, sollevano diverse questioni sulle quali occorre prestare attenzione.

In questa prospettiva, il piano della regolamentazione legislativa e, dunque, l'introduzione di norme cogenti, appare certamente il primo ad essere deputato alla definizione di limiti e condizioni per un impiego corretto e consapevole delle neurotecnologie, che non arrechi alcun pregiudizio ai soggetti interessati.

Un intervento normativo che, tuttavia, necessita di uniformità per evitare la proliferazione di diverse legislazioni a carattere nazionale che disciplinino in maniera differente la medesima fattispecie, a tutto discapito del principio di uguaglianza e di non discriminazione.

Al riguardo, sembra possibile rilevare come il legislatore europeo ben potrebbe intervenire in tale ambito, anche integrando proposte già presentate. Non pare si possa valutare positivamente, infatti, la mancata inclusione nell'attuale testo della Proposta di Regolamento Europeo sull'armonizzazione dell'intelligenza artificiale di un chiaro riferimento alle neurotecnologie; sebbene all'articolo 1 relativo all'oggetto della Proposta vi è un riferimento a "*sistemi di riconoscimento delle emozioni*", nel successivo articolo 3, numero 34 si precisa che si tratta di "*sistema di AI finalizzati all'identificazione e alla deduzione di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici*", senza alcun riferimento esplicito alle neurotecnologie. Tale Proposta appare sicuramente un primo passo verso il riconoscimento e la regolamentazione di sistemi di intelligenza artificiale che sono in grado di accedere a dati

mentali; tuttavia, la prospettiva del legislatore europeo sembra ancora molto ristretta, riferendosi unicamente ai sistemi di rilevamento attraverso i dati biometrici, senza alcuna considerazione dell'ampio e complesso quadro di funzionalità che è tipico delle neurotecnologie e non di qualsiasi altro sistema di intelligenza artificiale.

Dunque, una Proposta che nella sua formulazione attuale porterebbe all'adozione di un Regolamento in materia di intelligenza artificiale parziale e lacunoso, lasciando ancora una volta all'interprete il compito di definire l'esatto ambito applicativo di disposizioni che non disciplinano espressamente le fattispecie concrete che necessitano di adeguata tutela.

A ciò si aggiunga che il piano della regolamentazione normativa non sarebbe in grado di contemperare tutti gli interessi coinvolti. Sarebbe auspicabile, pertanto, che accanto alla *binding regulation*, ovvero ad un corpo di norme cogenti, siano introdotti anche adeguati strumenti di *soft law*, come codici etici e codici di condotta che orientino le scelte di coloro che sono deputati alla progettazione e all'impiego delle neurotecnologie.

In altre parole, stabilire delle regole di comportamento per le varie categorie di professionisti interessati – produttori, aziende ma anche personale medico – unitamente ad un adeguato quadro normativo in materia, potrebbe meglio garantire la tutela dei diritti fondamentali dei soggetti che si rapportano alle neurotecnologie.

Infine, con specifico riferimento alla fase prodromica della ricerca e della progettazione, sarebbe opportuno elaborare degli standard condivisi (anche in relazione ai test di valutazione dei dispositivi) ed in generale delle *best practices* per creare uniformità e per integrare ricerca e progettazione. Dunque, delle precise indicazioni per indirizzare il lavoro di ricercatori, progettisti, aziende tecnologiche e altri *steackholders* coinvolti, al fine di indurre una evoluzione tecnologica *human centred*, ovvero che riesca a bilanciare adeguatamente le logiche di mercato con le esigenze di tutela eticamente e giuridicamente rilevanti, ponendo al centro la persona e la sua sfera di interessi.

Più in particolare, parrebbe opportuno l'inserimento di una figura professionale di area giuridica all'interno delle aziende tecnologiche per finalità di ricerca scientifica, ovvero che si occupi non soltanto di contrattualistica (predisposizione di clausole d'uso dei prodotti e definizione del regime di responsabilità derivante dall'impiego dei medesimi) ma anche di analisi comportamentale,

focalizzandosi sull'osservazione dell'interazione tra *devices* ed utilizzatori finali, per prospettare i potenziali danni prodotti dalle tecnologie, prima dell'immissione sul mercato, di modo da regolarne le condizioni, le responsabilità e le tutele.

Favorire in tal modo la cooperazione con professionalità operanti in vari ambiti ponendo l'attenzione sulle implicazioni etiche e alle esigenze di veri e propri "*Spazi Etici*"[61] di giudizio e di tutela in cui operare attraverso le neurotecnologie.

9.6. Conclusioni

L'analisi dei rischi determinati dalle neurotecnologie nell'ottica di evitare condizioni di *vulnerabilità relazionale* non deve condurre a minimizzare l'impatto positivo che queste sono in grado di avere, specie per le persone con grave disabilità, per le quali possono potenzialmente porsi come ausilio per ridurre le distanze sociali e garantire adeguati livelli di libertà ed autonomia.

Dall'altro lato, bisogna prestare attenzione che proprio la solidarietà e l'inclusione, quali valori fondamentali di rango normativo, non diventino lo strumento per favorire la produzione di tecnologie che, grazie all'intelligenza artificiale, siano utilizzate per predeterminare le scelte degli individui.

Ciò diventa tanto più rilevante se si considera che tali tecnologie stanno pervadendo sempre di più il mercato dei prodotti di consumo, rispetto ai quali non si pone soltanto una questione attinente alla tutela della libertà del singolo ma anche di accesso indiscriminato ai dati relativi alle sue funzioni cognitive.

In altre parole, ben consci del valore economico – anche solo indiretto e potenziale – dei dati personali, ciò che si deve con forza evitare è la creazione di logiche di *business* connesse alla sfera più intima e riservata degli individui, attraverso un impiego distorto di dispositivi progettati per uso medico e testati su persone con gravi patologie.

Pertanto, se da un lato occorre rafforzare la ricerca clinica con dispositivi neurotecnologici per la diagnosi e il trattamento di gravi malattie neurodegenerative, migliorando così la qualità della vita delle

[61] Sulla definizione di spazio etico L. BATTAGLIA, L. GATT, A. MORRESI, P. GRIMALDI, *Spazi Etici per i* minori, in *Familia,* 2021, 933-944.

persone coinvolte, dall'altro lato occorre anche massimizzare l'affidabilità del sistema di IA come i dispositivi di BCI, rendendoli sicuri e ed evitando i rischi associati all'analisi dei dati neurali e mentali a fini inferenziali e predittivi.

L'obiettivo di porre le persone al centro della trasformazione digitale sembra essere non solo un auspicio ma anche una necessità che ha trovato un suo chiaro riconoscimento nella "*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*"[62] in cui non solo sono riaffermati i principi di solidarietà e inclusione ma è posta, altresì, l'attenzione sulla libertà di scelta quale valore fondamentale da porre alla base di ogni forma di interazione delle persone con algoritmi e sistemi di intelligenza artificiale.

[62] https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles

10. I sistemi di raccomandazione nelle interazioni tra professionisti e consumatori: il punto di vista del diritto dei consumi (e non solo)

Roberta Montinaro (Università di Napoli L'Orientale)

10.1. I *recommender systems*: definizione ed impiego nel commercio online

I *recommender* (o *recommendation*) *systems*[1] (d'ora in poi "*RS*") sono algoritmi che orientano la scelta di contenuti informativi disponibili online, sulla base della previsione di interessi e preferenze degli utenti della Rete[2], compiuta impiegando una mole notevole di dati[3].

Quanto al modo in cui sono concepiti, secondo le prassi più diffuse, i *RS* sono di due specie, *collaborative filtering-based* ("*CFB*") o *content-based* ("*CB*")[4]. I primi consigliano contenuti sulla base di certe

[1] J. Stray, *Beyond Engagement: Aligning Algorithmic Recommendations with Prosocial Goals*, in https://partnershiponai.org/beyond-engagement-aligning-algorithmic-recommendations-with-prosocial-goals/

[2] Si utilizza qui il termine utente della Rete in senso lato, per indicare l'utente finale/destinatario della raccomandazione algoritmica, salvo poi, nel corso dell'analisi, ove pertinente, aggiungere connotazioni soggettive desumibili dalle diverse discipline di volta in volta richiamate (consumatore, soggetto interessato, destinatario del servizio di intermediazione online, etc.).

[3] I RS impiegano tre diversi ordini di dati, dati relativi: *i)* alle caratteristiche di ciascun utente, *user's data* (genere, età, formazione, etc.); *ii)* al comportamento online di questi o di terzi, *usage data* (tempo speso online, precedenti acquisti, salvataggio di una pagina *web*, *ranking* assegnato ad un oggetto, etc.); e *iii)* allo *usage environment* (il tipo di *software* e *hardware* dell'utente, il luogo in cui si trova, etc.). Tali dati sono ottenuti anche grazie al monitoraggio (o, se si preferisce, alla "sorveglianza"[3]) dei comportamenti degli utenti. Cfr., in merito, S. Zuboff (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books.

[4] Cfr. M. Ferrari Dacrema, P. Cremonesi, D. Jannach, *Methodological Issues in Recommender Systems Research* (Extended Abstract), *Proceedings of the Twenty-Ninth*

caratteristiche inferite, che valgono a collocare l'utente all'interno di un gruppo. Questo tipo di *RS*, che presuppone un'attività di *profilazione*[5], non si limita ad usare i dati del singolo, ma impiega anche dati di terzi. Viceversa, i *RS* di tipo *CB* selezionano il contenuto in considerazione di determinati attributi dello stesso[6].

I sistemi di raccomandazione servono a dare vita a pratiche di *personalizzazione*, vale a dire, a forme di analisi predittiva, che usano insiemi di dati per "adattare" contenuti informativi, comunicazioni commerciali, prodotti, etc., alle caratteristiche di ciascun utente[7].

Oltre che dall'algoritmo, un RS è costituito da altri elementi, tra i quali, ai fini dell'analisi giuridica, occorre menzionare l'interfaccia online (c.d. *user interface*) la quale consente l'interazione del sistema con il suo utente. Il modo in cui quest'ultima viene concepita costituisce un fattore che può essere determinante nella scelta dei contenuti consigliati (cfr. *ultra*)[8].

International Joint Conference on Artificial Intelligence (IJCAI-20) Sister Conferences Best Papers Track, disponibile in https://www.ijcai.org/proceedings/2020/0650.pdf. "Collaborative-filtering recommender systems operate by suggesting items to a user based on the interests and behaviors of other users who are identified as having similar preferences or tastes".

[5] M Hildebrandt, Defining Profiling: A New Type of Knowledge?, in M. Hildebrandt, S. Gutwirth (eds), *Profiling the European Citizen* (Springer 2008), p. 34, che offre la seguente definizione di profilazione: 'the process of 'discovering' correlations between data in databases that can be used to identify and represent a human or nonhuman subject (individual or group) and/or the application of profiles (sets of correlated data) to individuate and represent a subject or to identify a subject as a member of a group or category'. Si veda inoltre, la definizione di cui all'art. 4 (4) GDPR e l'interpretazione fornitane dall'*Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev01, 2017), p. 6.

[6] Nella realtà, le due tipologie innanzi descritte non sono quasi mai nettamente distinguibili. I sistemi di raccomandazione più avanzati appartengono al tipo *CFB* e di solito adottano metodologie di *machine learning*.

[7] M. Eltzrow, A. Kobsa, *Impacts of user privacy preferences on personalized systems. A Comparative Study*, in M.Teltzrow, A. Kobsa, *Designing Personalized User Experiences in eCommerce*, Dordrecht, Kluwer Academic Publisher, 2004, p.1.
la quale definisce la personalizzazione as "predictive analysis of consumer data used to adapt targeted media, advertising and merchandising to consumer needs"; personalization can be viewed as a cycle of recurring processes consisting of 'data collection', 'profiling' and 'matching': from collected data, user profiles can be created that are the basis for adapting user interfaces to individuals or groups of individuals".

[8] R. Di Resta, *Up Next: A Better Recommendation System*, in *WIRED*, 11 aprile 2018.

I *RS* presentano indubbia utilità, giacché, grazie ad essi, diviene più agevole orientarsi in un contesto, quale quello online, connotato da sovrabbondanza di informazioni (c. d. *information overloading*)[9]. La 'ottimizzazione' nella fruizione di queste ultime costituisce, infatti, la loro funzione più evidente[10]. Tuttavia, la considerevole importanza in termini economici, che tale tecnologia riveste[11], dipende, a ben vedere, dal fatto che le imprese la impiegano sia al fine di promuovere beni o servizi attraverso forme di pubblicità comportamentale mirata, sia per far sì che gli utenti restino "attivi" online il più a lungo possibile[12]. In tale seconda funzione essi costituiscono un portato della c.d. *economia dell'attenzione* [13] : quest'ultima rappresenta, nella moderna società dell'informazione, la risorsa più rilevante e, al tempo stesso, scarsa, che va dunque catturata dalle imprese ricorrendo ai più svariati stratagemmi[14]; il grado di 'coivolgimento' (dal temine inglese '*engagement*')

[9] Cfr., circa il rapporto tra sovrabbondanza di informazioni, sistemi automatici di filtraggio dei contenuti disponibili online ed autonomia dell'utente, C. Reed, E. Kennedy, S. Silva, *Responsibility, Autonomy and Accountability: Legal Liability for Machine Learning* (October 17, 2016), *Queen Mary School of Law Legal Studies Research Paper No. 243/2016*, disponibile in SSRN: https://ssrn.com/abstract=2853462, p. 19. Si vedano, inoltre, N. Helberger, K. Karppinen, L. D'Acunto, *Exposure diversity as a design principle for recommender systems*, in *Information, Communication & Society*, (2018) 21:2, p. 191-207, p. 192.

[10] N. Helberger, *Merely facilitating or actively stimulating diverse media choices? Public service media at the crossroad*, in *International Journal of Communication* (2015) 9, pp. 1324–1340.

[11] Sono specialmente vantaggiosi per le imprese, come ci indicano alcuni studi. Cfr. J. Hassler, *The power of personalized product recommendations*, Carrollton: Intelliverse, 2018, in http://www.intelliverse.com/blog/the-power-of- personalized-product-recommendations/; D. Jannach, M. Jugovac, *Measuring the business value of recommender systems*, in *ACM Transactions on Management Information Systems*, 10(4), 2019.

[12] J. Cobbe, J. Singh, *Regulating Recommending: Motivations, Considerations, and Principles*, in *European Journal of Law and Technology*, (2019) 10(3), disponibile in SSRN: https://ssrn.com/abstract=3371830 or http://dx.doi.org/10.2139/ssrn.3371830, p. 8: "Recommender systems play two fundamental roles in surveillance capitalism. The first of these is in delivering behaviourally-targeted advertising and other paid-for content to bring direct revenue from advertisers and others. The second is personalisation to drive engagement, thus indirectly contributing to the maintenance of direct revenue streams".

[13] R. Tushnet, *Attention Must Be Paid: Commercial Speech, User-Generated Ads, and the Challenge of Regulation*, in *Georgetown Public Law and Legal Theory Research Paper* No. 10-59, 2010, p. 721 ss., disponibile in http://scholarship.law.georgetown.edu/facpub/436/ . Cfr., altresì, T. Wu, *Blind Spot: The Attention Economy and the Law*, in *Antitrust Law Journal*, 82/2019, pp. 771 ss., disponibile in https://scholarship.law.columbia.edu/faculty_scholarship/2029.

[14] N. Seaver, *Captivating Algorithms: Recommender Systems as Traps*, in (2019) 24 Journal of Material Culture 421, la quale descrive la parabola dei sistemi di raccomandazione,

costituisce fonte di ingenti profitti, per via dei dati che possono ricavarsene e grazie alle ricordate forme di pubblicità mirata[15].

Il presente saggio intende analizzare le pratiche di raccomandazione diffuse nel contesto del commercio elettronico, realizzate da una varietà di operatori economici (siti di e-commerce e mercati online, ma anche da motori di ricerca, siti di *social networking*, etc.).

L'uso di RS è alla base del fenomeno del trattamento differenziato dei consumatori, il quale, per alcuni profili, costituisce oggetto di specifiche disposizioni presenti nella direttiva UE 2161/2019 del Parlamento europeo e del Consiglio[16] (d'ora in poi, "direttiva omnibus"), come si noterà nella parte I di questa analisi.

I *RS* servono, come detto, ad 'adattare' contenuti informativi, comunicazioni commerciali, offerte contrattuali, alle caratteristiche di ciascun consumatore, ma, in linea di principio, non ne escludono la libertà di scelta, che essi si limitano a *guidare*, offrendo una gamma di opzioni. La letteratura giuridica ha, tuttavia, messo in luce alcune possibili conseguenze negative, collegate al loro impiego[17], tra cui: *i)* il rischio di trattamenti discriminatori nella selezione dei contenuti e/o dei

inizialmente preoccupati esclusivamente dell'accuratezza del consiglio fornito, ma poi, in una fase successiva, concepiti per "catturare" l'attenzione del destinatario. Secondo questa prospettiva, si tratta di una moderna trappola, paragonabile alle rudimentali tecnologie impiegate per catturare animali: ciò in quanto la bontà di questi sofisticati sistemi è valutata esclusivamente alla luce della loro capacità "to capture user attention, or 'engagement' (cfr. p. 9)"). Cfr, anche S. Gurses, J.V.J. van Hoboken (2017, May 2), *Privacy after the Agile Turn*, disponibile in https://doi.org/10.31235/osf.io/9gy73 e C.N. Griffin, *Systemically Important Platforms* (March 19, 2021), in Cornell Law Review (2021 Forthcoming), in SSRN: https://ssrn.com/abstract=3807723

[15] Tanto è vero che questa seconda forma di impiego di RS costituisce il fulcro del modello di *business* prescelto da alcune grandi imprese dell'economia digitale. Cfr., in merito, P. Barwise, L. Watkins, *The evolution of digital dominance: how and why we got to GAFA*, in *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, a cura di M. Moore, D. Tambini, Oxford University Press. (2018), disponibile in http://lbsresearch.london.edu/914/.

[16] Direttiva 2019/2161/UE del Parlamento europeo e del Consiglio del 27 novembre 2019.

[17] S. Milano, M. Taddeo, L. Floridi, *Recommender systems and their ethical challenges*, in *AI&Society* (2020) 35:957-967): "Recommender systems can encroach on individual users' autonomy, by providing recommendations that nudge users in a particular direction, by attempting to "addict" them to some types of contents, or by limiting the range of options to which they are exposed.

relativi destinatari[18]; *ii)* la limitazione delle opportunità di ricevere comunicazioni commerciali e/o offerte contrattuali alternative e, dunque, la compressione dell'ambito delle opzioni cui i consumatori sono esposti; *iii)* la menomazione dell'autonomia di tali ultimi soggetti, allorché il sistema sia congegnato in modo tale da indirizzarli verso certi contenuti, attraverso forme di vera e propria manipolazione digitale (in quest'ultima eventualità, anziché guidare, essi distorcono la volontà del consumatore e, per tale loro capacità, vengono denominati da una certa letteratura "*hyper-nudges*"[19]; cfr. *ultra*); *iv)* infine, catturare l'attenzione degli utenti per indurli a restare attivi online.

Quelli appena descritti non sono però corollari ineluttabili dell'impiego di questa tecnologia, quanto piuttosto rischi che il diritto è chiamato a governare[20], nei modi (e con i limiti) che si osserveranno nella parte II del presente scritto.

La originaria versione della Proposta di Regolamento del Parlamento europeo e del Consiglio relativa al Mercato Unico per i Servizi Digitali (il c.d. Digital Services Act, d'ora in poi " Proposta *DSA*")[21] già contemplava i *RS*, all'articolo 2 (lett. *o*), in cui si definiva un *RS* come

---

[18] E. Bozdag (2013) Bias in algorithmic filtering and personalization. Ethics and Information Technology, 15(3), 209–227.

[19] M. Lanzing, "Strongly Recommended". Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies, in Philos. Technol. (2019) 32:549–568 https://doi.org/10.1007/s13347-018-0316-4.

[20] Questa stessa tecnologia, secondo alcuni studiosi, potrebbe persino contribuire ad ovviare alle conseguenze negative della sovrabbondanza di informazioni fruibili online, se concepita e realizzata in linea con il principio di c.d. "*diversity by design*", in modo tale, cioè, da garantire la diversità dei contenuti cui gli utenti sono esposti. Cfr. N. Helberger, K. Karppinen, L. D'Acunto, *Exposure diversity as a design principle for recommender systems*, in *Information, Communication & Society*, (2018) 21(2), pp. 191–207.

[21] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15.12.2020 COM(2020) 825 final - 2020/0361 (COD). Cfr. G. Alpa, *La legge sui servizi digitali e la legge sui mercati digitali*, in *Contratto e impr*., 2022, p. 1 ss. Secondo le informazioni reperibili sul sito istituzionale del Parlamento Europeo (https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act; ultimo accesso 15 luglio 2022), "Il Parlamento e il Consiglio hanno raggiunto un accordo politico provvisorio sulla DSA nell'aprile 2022. L'accordo provvisorio è soggetto all'approvazione del Consiglio e del Parlamento europeo. La Commissione per il mercato interno e la protezione dei consumatori (IMCO) del Parlamento ha approvato l'accordo provvisorio (36 voti a favore, 5 contrari e un'astensione) il 16 giugno 2022 e il Parlamento riunito in seduta plenaria dovrebbe approvare il testo definitivo durante la sessione di luglio 2022 (traduzione nostra)". Nel saggio si citerà la versione frutto di tale accordo provvisorio, salva diversa indicazione nel testo o in nota.

quel "sistema interamente o parzialmente automatizzato che una piattaforma online utilizza per suggerire ai destinatari del servizio informazioni specifiche tramite la propria interfaccia online, anche in base ad una ricerca avviata dal destinatario o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate".

Definizione criticata, in quanto incapace di descrivere pienamente le funzioni dei *RS*: tali sistemi non si limitano a raccomandare contenuti, ma più esattamente 'curano' gli stessi e, dunque, sono in grado di *determinare* il modo in cui gli utenti interagiscono con le informazioni nell'ambiente online[22]. Ragion per cui, l'intermediario online che impieghi *RS* su contenuti resi disponibili da terzi si reputa in grado di stabilire, attraverso un processo decisionale automatizzato e sulla base di criteri predeterminati, quali informazioni promuovere e quali, invece, posporre[23].

Le modifiche alla Proposta DSA approvate dal Parlamento europeo a gennaio 2022[24] hanno poi integrato la suddetta definizione, precisando che si tratta (cfr. art. 2, lett. o) di "un sistema interamente o parzialmente automatizzato che una piattaforma online utilizza per suggerire, *mettere in ordine di priorità o selezionare* per i destinatari del

[22] Cfr. *European Data Protection Supervisor* (d'ora in poi "*EDPS*"), *Opinion 1/2021 (*10 febbraio 2021) *on the Proposal for a Digital Services Act*. La medesima Autorità chiarisce, poi, che tale attività è spesso svolta sulla base di trattamenti automatizzati, che possono includere forme di profilazione degli utenti (cfr. art…), con tutti i conseguenti rischi segnalati dalla stessa *EDPS*, "Opinion 3/2018 *EDPS Opinion on online manipulation and personal data*", 19 March 2018, p. 9, https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf).

[23] Il suo intervento non è dunque di natura meramente tecnica e passiva, con la conseguenza che un simile intermediario non può giovarsi della immunità di cui alla disciplina sulla responsabilità degli *Internet service provider*, contenuta nella direttiva sul commercio elettronico. Cfr., in tal senso, Jennifer Cobbe and Jatinder Singh (2019) 'Regulating Recommending: Motivations, Considerations, and Principles', European Journal of Law and Technology, 10 (3), p. 5. Tuttavia, nel Considerando n. 22 Proposta DSA, si legge "*il fatto che un fornitore indicizzi automaticamente i contenuti caricati sul suo servizio, che disponga di una funzione di ricerca o che raccomandi contenuti sulla base dei profili o delle preferenze dei destinatari del servizio non è un motivo sufficiente per ritenere che tale fornitore abbia una conoscenza "specifica" delle attività illegali svolte su tale piattaforma o dei contenuti illegali in essa memorizzati. "*

[24] Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)).

servizio informazioni specifiche tramite la propria interfaccia online…"[25].

La difficoltà di individuazione delle funzioni della tecnologia di cui si tratta tradisce la complessità delle relative implicazioni, da esaminare giovandosi di una pluralità di prospettive, desumibili da apparati normativi di varia ispirazione: tra essi, oltre a disposizioni appartenenti al diritto dei consumatori, rientra anche la disciplina in materia di protezione dei dati personali. Particolare rilievo riveste, poi, la già ricordata Proposta *DSA*, riguardante i c.d. servizi di intermediazione online offerti da una pluralità di operatori economici. Le disposizioni relative ai RS concernono i fornitori di piattaforme digitali, in generale, e di piattaforme e di motori di ricerca[26], di grandi dimensioni, in particolare, nelle rispettive interazioni con i destinatari del servizio, i quali possono coincidere o meno con i consumatori[27] (anche se la veste di consumatore per il destinatario del servizio è sottintesa nella *ratio* di molte previsioni). Nella prospettiva del DSA, i RS costituiscono oggetto di un servizio accessorio a quello di intermediazione online (cfr. *ultra*).

---

[25] Definizione perspicua, poiché mette in luce tre funzioni, di raccomandazione in senso stretto, di classificazione e di selezione di contenuti disponibili online. Successivamente, per effetto dell'accordo provvisorio tra Parlamento e consiglio dell'aprile 2022, la definizione è stata modificata nei termini che seguono: "'per "sistema di raccomandazione" si intende un sistema completamente o parzialmente automatizzato utilizzato da una piattaforma online per suggerire o dare priorità nella sua interfaccia online a informazioni specifiche per i destinatari del servizio, anche come risultato di una ricerca avviata dal destinatario del servizio o determinando in altro modo l'ordine relativo o la prominenza delle informazioni visualizzate". Si mette pur sempre in luce, dunque, la funzione di curare i contenuti, propria di tali sistemi.

[26] Cfr. Art. 2, ha, DSA: "'un servizio digitale che consente agli utenti di inserire query per effettuare ricerche, in linea di principio, su tutti i siti web o su tutti i siti web in una determinata lingua, sulla base di un'interrogazione su qualsiasi argomento sotto forma di parola chiave, richiesta vocale, frase o altro input, e restituisce risultati in qualsiasi formato in cui sia possibile trovare informazioni relative al contenuto richiesto".

[27] Secondo l'art. 2 DSA, si intende per ""destinatario del servizio": qualsiasi persona fisica o giuridica che utilizza il servizio intermediario in questione *per cercare informazioni o per renderle accessibili*"; mentre è consumatore "qualsiasi persona fisica che agisce per fini che non rientrano nella sua attività commerciale, imprenditoriale, *artigianale* o professionale". Molte delle disposizioni che recano riferimento alla prima figura, e che attengono al tema di cui al presente contributo, sono in realtà concepite avendo riguardo agli interessi del consumatore.

10.2. Le specifiche disposizioni del diritto dei consumi applicabili a RS impiegati nelle interazioni online tra professionisti e consumatori. Il *ranking* personalizzato ed il *search advertising*

I *RS* usati nell'e-commerce sono alla base del fenomeno del *trattamento differenziato* dei consumatori, che si riscontra talvolta nel contesto online, nel quale le imprese sono oramai in grado, su larga scala, di interagire con ciascun consumatore, indirizzandogli informazioni di natura commerciale e/o offerte contrattuali "personalizzate", diverse cioè (anche sul piano economico; cfr. ultra) da quelle rivolte ad altri consumatori. La standardizzazione delle interazioni tra professionisti e consumatori, propria della produzione di massa, ha mutato pelle per effetto dell'evoluzione tecnologica, fino ad includere le pratiche di personalizzazione[28].

Una prima manifestazione di questo fenomeno è costituita dal c.d. *ranking personalizzato* o *differenziato*, che si ha quando vengono impiegati *RS* al fine di adattare i risultati della ricerca online, a misura di ciascun utente. La personalizzazione del *ranking* è compiuta dall'algoritmo di raccomandazione sulla scorta di una pluralità di criteri, ivi incluso l'interesse economico dell'impresa che li utilizza o di terze parti.

E' ben noto che il posizionamento prominente di un'offerta commerciale all'interno dei risultati di ricerca online è in grado di influenzare le scelte dei consumatori. A tale proposito, la Commissione UE ha chiarito che questi ultimi, a meno che non siano informati diversamente, maturano un affidamento circa il fatto che i risultati della ricerca sono inclusi e classificati solo sulla base della pertinenza con la parola chiave di ricerca prescelta, e non in virtù di altri criteri[29]. Omettere una simile informazione costituisce pratica commerciale sleale ai

[28] Cfr., in per un'analisi in merito, O. Lynskey, H.W. Micklitz, P. Rott, *Personalised Pricing and Personalised Commercial Practices* , Micklitz, Helberger et al. (2021) *EU Consumer Protection 2.0: Structural asymmetries in consumer markets*, disponibile in https://www.beuc.eu/publications/beucx-2021-018_eu_consumer_protection.0_0.pdf, p. 94, p. 102.

[29] European Commission's *Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices* (SWD(2016)163), p. 133, d'ora in poi, "Linee guida della Commissione UE del 2016".

sensi della direttiva 2005/29/CE del Parlamento e del Consiglio, dell'11 maggio 2005, idonea a distorcere il comportamento economico dei consumatori (come affermato dall'autorità francese della concorrenza in un provvedimento riguardante la personalizzazione del *ranking* praticata dal motore di ricerca *Google*[30]).

Un espresso requisito di trasparenza è stato introdotto dalla direttiva omnibus: i professionisti sono tenuti ad informare circa i parametri principali che determinano la classificazione dei risultati della ricerca online (c.d. *search transparency*), nonché circa l'importanza relativa tra i vari parametri, in modo chiaro e comprensibile (un "riferimento nei termini o condizioni standard" non appare sufficiente, secondo il Considerando 19); in difetto di che, può aversi una pratica commerciale ingannevole[31]. Tale disposizione non si applica ai motori di ricerca, per i quali vale, tuttavia, il principio ricavato dalla Commissione e testé rammentato (i consumatori debbono essere informati circa il fatto che i criteri impiegati per elaborare la classificazione dei risultati della ricerca *online* non sono naturali, non sono cioè basati sul solo criterio della loro rilevanza rispetto alla ricerca condotta dal consumatore).

Essendovi un conflitto tra esigenza di trasparenza sul funzionamento delle classifiche online e protezione dei segreti commerciali, la direttiva omnibus chiarisce che la descrizione dei parametri non richiede la divulgazione di informazioni dettagliate sull'algoritmo, bastando a tal fine una dichiarazione generica (cfr. *ultra*). Inoltre, la portata di un simile obbligo di trasparenza è non poco ridimensiona dal fatto che, al fine del suo adempimento, è sufficiente una descrizione

---

[30] Autorité de la concurrence, *Decision 19-MC-01 of 3 January 2019 regarding a request for interim measures from Amadeus*, available at http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=697&id_article=3343&la.

[31] All'art. 7 dir. 2005/29/CE è inserito un nuovo par. 4 bis: " Nel caso in cui sia fornita ai consumatori la possibilità di cercare prodotti offerti da professionisti diversi o da consumatori sulla base di una ricerca sotto forma di parola chiave, frase o altri dati, indipendentemente dal luogo in cui le operazioni siano poi effettivamente concluse, sono considerate rilevanti le informazioni generali, rese disponibili in un'apposita sezione dell'interfaccia online che sia direttamente e facilmente accessibile dalla pagina in cui sono presentati i risultati della ricerca, in merito ai parametri principali che determinano la classificazione dei prodotti presentati al consumatore come risultato della sua ricerca e all'importanza relativa di tali parametri rispetto ad altri parametri. Il presente paragrafo non si applica ai fornitori di motori di ricerca online definiti ai sensi dell'articolo 2, punto 6, del regolamento (UE) 2019/1150 del Parlamento europeo e del Consiglio.".

standardizzata dei principali parametri di classificazione, che non deve quindi essere fornita individualmente ed *ex post* per ogni ricerca effettuata[32]. Ciò solleva la questione se tale previsione possa avere un effetto pratico significativo nel ristabilire la capacità di scelta del consumatore (cfr. *ultra*).

Il c.d. *search advertising* si ha, invece, quando l'algoritmo di raccomandazione è guidato espressamente dall'intento di favorire una data impresa, collocandola nella classificazione in posizione preminente rispetto ad altra/altre. E' ciò che avviene allorché il ranking sia determinato dal pagamento di imprese terze, per influenzare la classificazione dei risultati[33].

In merito, un espresso dovere di informazione è stato introdotto dalla richiamata direttiva con un nuovo art. 11 bis, aggiunto alla dir. 2005/29/CE, per il quale rientra tra le pratiche commerciali vietate "Fornire risultati di ricerca in risposta a una ricerca online del consumatore senza che sia chiaramente indicato ogni eventuale annuncio pubblicitario a pagamento o pagamento specifico per ottenere una classificazione migliore dei prodotti all'interno di tali risultati"[34].

Non è espressamente contemplato il caso in cui, a condizionare il *ranking*, vi sia un interesse economico della stessa piattaforma (c.d. *self-preferencing*), come avviene allorché il provider di un mercato online non sia un imparziale intermediario nella fornitura di beni e servizi dei propri clienti-professionisti, ma abbia interesse a promuovere beni o servizi, che esso stesso (o una società figlia o con cui ha cointeressenze) fornisce. Una simile ipotesi, tuttavia, appare anch'essa agevolmente riconducibile alla regola, appena ricordata, espressa dalla Commissione europea, per la quale è vietato fare leva sull'aspettativa dei consumatori circa il carattere naturale dei criteri di classificazione dei risultati

[32] Cfr. dir. 2019/2161, Considerando n. 23), secondo cui i professionisti "dovrebbero fornire una descrizione generale dei principali parametri di classificazione che determini i principali parametri predefiniti da essi utilizzati e l'importanza relativa di tali parametri rispetto ad altri parametri, ma tale descrizione non deve necessariamente essere fornita individualmente per ogni ricerca effettuata".

[33] Cfr. Autorità garante concorrenza e mercato, casi Expedia e Booking.com, Comunicato stampa del 18 dicembre 2020: https://ec.europa.eu/commission/presscorner/detail/it/ip_20_2444 .

[34] Si tratta a ben vedere di una specificazione della regola generale, applicabile anche alle piattaforme di comparazione dei prezzi di bene e servizi, per la quale ogni comunicazione commerciale deve essere chiaramente identificabile come tale da parte dei destinatari della stessa. Cfr. Linee guida della Commissione Ue del 2016.

di una ricerca online, allorché questi ultimi siano influenzati da altri fattori, di cui i consumatori sono ignari.

La determinazione del *ranking* ed i relativi parametri adottati rilevano anche ad altri effetti, che qui si possono solo menzionare: i) costituisce oggetto di un dovere di trasparenza nei rapporti contrattuali tra il gestore di un online *marketplace* ed il suo utente-imprenditore, alla luce dell'art. 5 Reg. (EU) 1150/2019; ii) può venire in rilievo sotto forma di condotta anticoncorrenziale (come testimoniato dal caso *Google LLC e Alphabet Inc. v. Commissione Europea*)[35].

10.3. Il prezzo personalizzato

Le imprese attive nel contesto digitale sfruttano la tecnologia in parola anche per indirizzare ai consumatori offerte commerciali differenziate sul piano economico, recanti cioè un prezzo differenziato ("*price differentiation*")[36]. Ciò può avvenire alla luce di una serie di parametri, tra cui la inferita propensione di ciascun consumatore a pagare un certo prezzo, nel qual caso si discute di "personalizzazione del

[35] Tribunale UE novembre 2021 (Case T-612/17) nella causa *Google LLC e Alphabet Inc. v. Commissione Europea* for annulment of Commission Decision C(2017) 4444 final of 27 June 2017 relating to proceedings under Article 102 TFEU and Article 54 of the EEA Agreement (Case AT.39740 – Google Search (Shopping)), consultabile in https://curia.europa.eu/juris/document/document.jsf?text=&docid=249001&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2371119. Si vedano le prime note di commento di V. Falce, *La Corte di Giustizia anticipa le misure del Digital Market Act*, in *Il Sole24Ore, Norme e tributi*, 4 gennaio 2022. Cfr., in dottrina, per il rapporto tra RS e disciplina della concorrenza, J. Cobbe, J. Singh, *Regulating Recommending: Motivations, Considerations, and Principles* (April 15, 2019), in *European Journal of Law and Technology*, 10(3), disponibile in SSRN: https://ssrn.com/abstract=3371830 or http://dx.doi.org/10.2139/ssrn.3371830, p. 25.

[36] Si veda *OECD, Personalised Pricing in the Digital Era.* Background Note by the Secretariat, 28 November 2018, available at https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf. See *Consumer market study on online market segmentation through personalised pricing/offers in the European Union* conducted for DG Just by Ipsos, London Economics and Deloitte, June 2018, available at https://ec.europa.eu/info/publications/consumer-market-study-online-market-segmentation-through- personalised-pricing-offers-european-union_en. With regard to differentiated practices occurring in platforms to businesses relations, see the Reports of the *Observatory for the Online Platform Economy* [C(2018), 2393 final], available https://ec.europa.eu/digital-single-market/en/news/commission-expert-group-publishes-progress-reports-online platform- economy.

prezzo"[37]. La differenziazione del prezzo non costituisce di per sé pratica vietata alla luce del diritto dei consumatori[38], giacché tale può dirsi soltanto quando associata ad altre condotte, tra cui omettere di informare i consumatori circa il ricorso a tecniche di personalizzazione[39]. Ed infatti, in ossequio ad un principio di trasparenza nelle interazioni tra professionisti e consumatori, i primi sono tenuti a fornire una simile informazione[40], come ora espressamente statuito dalla direttiva omnibus, per la quale occorre avvertire i consumatori "….che il prezzo è stato personalizzato sulla base di un processo decisionale automatizzato " (cfr. art. 6 *e bis* direttiva 2011/83/UE)[41]. L'avvertenza circa la personalizzazione del prezzo, richiesta dalla ricordata norma in tema di protezione dei consumatori, costituisce informazione rilevante, in difetto della quale può aversi una pratica commerciale ingannevole.

---

[37] Si vedano anche O. Lynskey, H.W. Micklitz, P. Rott, *Personalised Pricing and Personalised Commercial Practices*, in Micklitz, Helberger et al., *EU Consumer Protection 2.0: Structural asymmetries in consumer markets*, 2021, in https://www.beuc.eu/publications/beucx-2021-018_eu_consumer_protection.0_0.pdf, p. 94.

[38] Cfr. European Commission, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, SWD(2016) 163 final, p. 134. A questo proposito, la cosiddetta direttiva sui servizi (direttiva 2006/123/CE del Parlamento europeo e del Consiglio, del 12 dicembre 2006, relativa ai servizi nel mercato interno) prevede un divieto generale di discriminazione dei prezzi solo quando è basata sulla nazionalità e sul luogo di residenza del consumatore.

[39] Si veda *OECD, Personalised Pricing in the Digital Era*, cit., p. 37: ".. stating that a personalized price is the "best price" when other consumers are offered better prices, making an invitation to buy a product at a specified price and then adjust the personalised price upwards as the consumer goes through the buying process, omitting the fact that the price or discount offered is personalized; etc.".

[40] Si veda F. ZUIDERVEEN BORGESIUS, *Online price discrimination and data protection law*, in Amsterdam Law School Research Paper No. 2015-32,1–21, <ssrn.com/abstract=2652665>; EC (2018), *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*, European Commission, https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_fin al_0.pdf.

[41] Cfr. considerando n. 45: "I professionisti possono personalizzare il prezzo delle loro offerte per determinati consumatori o specifiche categorie di consumatori sulla base di processi decisionali automatizzati e di profilazione del comportamento dei consumatori che permettono ai professionisti di valutare il potere d'acquisto dei singoli consumatori. I consumatori dovrebbero pertanto essere chiaramente informati quando il prezzo che è loro offerto è personalizzato sulla base della decisione automatizzata, in modo da poter tenere conto dei potenziali rischi insiti nel loro processo decisionale di acquisto. Pertanto, è opportuno inserire nella direttiva 2011/83/UE una disposizione relativa all'obbligo di informare il consumatore quando il prezzo offertogli è personalizzato sulla base di un processo decisionale automatizzato. ..".

Il quadro delle tutele da accordarsi ai destinatari di tecniche di personalizzazione del prezzo ai sensi del diritto dei consumi prevede anche, secondo l'opinione di alcuni studiosi[42], la nullità ai sensi delle disposizioni in tema di clausole vessatorie nei contratti con i consumatori, per cui il sindacato in ordine alla natura vessatoria di una clausola si estende alle clausole relative al corrispettivo, allorché esse manchino di intelligibilità; il quale requisito, include l'onere per i professionisti di rendere i consumatori consapevoli delle conseguenze economiche del contratto[43]. Sarebbe contraria a tale precetto allora la personalizzazione del prezzo che lasciasse i consumatori all'oscuro sulla base fattuale e sul metodo di calcolo impiegato da algoritmi.

La direttiva omnibus rimanda poi alla regolamentazione in tema di trattamento automatizzato di cui al *General Data Protection Regulation* del Parlamento europeo e del Consiglio (d'ora in poi "GDPR")[44] e, implicitamente, all'intero complesso normativo ivi recato [45]. Dimostrando, quindi, che il carattere sleale della pratica non viene escluso dalla (e che i doveri del professionista non si esauriscono nella) mera osservanza del ricordato obbligo di trasparenza, potendo sussistere, nonostante l'assolvimento di tale obbligo, in una serie di casi[46].

---

[42] F. Zuiderveen Borgesius, *Online price discrimination and data protection law*, in *Amsterdam Law School Research Paper* No. 2015-32,1–21, <ssrn.com/ abstract=2652665>; EC (2018), *Consumer market study on online market segmentation through personalised pricing/offers in the European Union*, European Commission, https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/ai d_and_development_by_topic/documents/synthesis_report_online_personalisation_study_fin al_0.pdf.

[43] Caso C-186/16, *Andriciuc e altri*, ECLI:EU:C:2017:703, paragrafi 44 e 45.

[44] Regolamento (EU) 2016/679 del Parlamento europeo e del Counsiglio del 27 aprile 2016 [2016], OJ L 119/1. Cfr. il considerando 45 della direttiva omnibus, secondo cui "...Questo obbligo di informazione non pregiudica le disposizioni del regolamento (UE) 2016/679, che stabilisce, tra l'altro, il diritto delle persone fisiche di non essere assoggettate a processi decisionali automatizzati relativi alle persone fisiche, inclusa la profilazione".

[45] E, dunque, fa dipendere la tutela dell'autodeterminazione dei consumatori dal rispetto delle disposizioni ivi presenti, per le quali debbono ricorre alcune condizioni di liceità del trattamento (un valido consenso da parte del consumatore/soggetto interessato, un'adeguata informazione, un lecito utilizzo dei dati personali da parte del professionista che ricorre a tale pratica, etc.), nonché debbono essere previste alcune salvaguardie per tale soggetto.

[46] Quali, ad esempio, la raccolta di dati per personalizzare i prezzi senza il consenso dei consumatori, l'utilizzo di dati per personalizzare i prezzi, quando tali dati sono stati richiesti per altri motivi dichiarati, l'uso della conoscenza di una specifica condizione

10.4. L'impiego di RS nelle comunicazioni commerciali. I rischi di discriminazione e compromissione dell'autodeterminazione dei consumatori

La regolamentazione sin qui considerata tipizza talune condotte implicanti uso di RS, prescrivendo requisiti di trasparenza ispirati a specifiche finalità[47], la cui inosservanza rileva alla luce della disciplina in tema di pratiche commerciali ingannevoli. I RS sono, però, utilizzati nell'ambito di una vasta gamma di interazioni con i consumatori, le quali comportano rischi che non possono essere fronteggiati attraverso la mera previsione di requisiti di trasparenza (cfr. *ultra*).

10.4.1. Vecchie e nuove forme di discriminazione di singoli o di gruppi di consumatori

Innanzitutto, l'uso di RS nelle comunicazioni commerciali può dare luogo a forme di discriminazione di individui o gruppi[48]. Ciò avviene

di vulnerabilità ottenuta attraverso l'osservazione in tempo reale di un singolo consumatore, etc.

[47] Le regole di trasparenza sul ranking mirano ad impedire ai professionisti di trarre profitto dall'affidamento dei consumatori circa la neutralità delle decisioni assunte dalle tecnologie impiegate dalla prima categoria di soggetti (nella specie, circa il fatto che il ranking sia basato su parametri oggettivi, etc.). Rispetto poi all'applicazione di un prezzo personalizzato, la *ratio* della imposta trasparenza consiste nel dare ai consumatori la possibilità di scegliere un diverso professionista (possibilità che, però, diviene concreta solamente ove vi siano nel medesimo mercato operatori concorrenti, che si astengano dall'applicare tale pratica).

[48] Gli algoritmi di raccomandazione non sono neutrali. Cfr. sul punto E. Bozdag (2013) *Bias in algorithmic filtering and personalisation*, in *Ethics in Information Technology*, 15, pp.209-227. Available at https://link.springer.com/article/10.1007/s10676-013-9321-6, nonché David Gareth, *The Social Power of Algorithms*, in Information, Communication and Society, 2017, pp. 1-13, disponibile in https://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1216147. Secondo l'A., "Algorithms are inevitably modelled on visions of the social world, and with outcomes in mind, outcomes influenced by commercial or other interests and agendas". Indeed, at a high level any algorithm can be understood to consist of a sequence of steps intended to produce a desired outcome. Algorithmic systems generally and recommender systems specifically are therefore inherently normative in nature. They are also contextual and contingent in nature, in that they are always embedded within and a product of the wider socio-technical context of their development and deployment; not just the goals of the organisation in question, but also the assumptions, priorities, and practices adopted by engineers, designers, managers, and users. As a

allorché il sistema di raccomandazione scelga i destinatari di messaggi pubblicitari, nonché di offerte contrattuali, alla luce di caratteristiche, le quali, a seconda dei casi, possono consistere in caratteristiche 'protette', cioè tradizionalmente contemplate dalla disciplina sul divieto di discriminazione (come razza, età, sesso, religione, etc.), o 'atipiche' (quali capacità reddituale, stato di famiglia, residenza in aree economicamente svantaggiate, etc.).

Con il fine di prevenire discriminazioni del primo tipo, il GDPR preclude l'impiego, nell'ambito di trattamenti interamente automatizzati, delle categorie particolari di dati, di cui all'art. 9 dello stesso[49]. Simili limitazioni, però, rivestono scarsa utilità, sol che si pensi alla facilità di desumere caratteristiche protette da dati non appartenenti alle suddette categorie[50]. Tanto è vero che il DSA proibisce le pratiche di pubblicità mirata che impieghino non solo dati particolari, ma anche informazioni inferite da dati non 'sensibili' (cfr. art. 24 par. 1 *ter*).

Le comunicazioni rivolte al pubblico possono dare vita a forme di discriminazione diretta, contrarie al divieto di discriminazioni stabilito dal diritto europeo (come stabilito dalla Corte di giustizia nel caso *Feryn* in relazione alla Direttiva 2000/43/CE[51]). La possibilità di ravvisare una pratica sleale in una condotta non conforme a tale divieto implica, però, che vi sia, in primo luogo, contrarietà alla diligenza professionale e, poi, che la condotta sia idonea a distorcere il comportamento economico del consumatore.

La prima costituisce una clausola generale riassuntiva dei doveri di cura e attenzione incombenti sul professionista, desumibili da una

consequence of their normative, contextual, and contingent nature, their use can never be neutral.

[49] Si veda in merito, l'interpretazione fornita da *Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, cit., per cui anche le inferenze vanno ricondotte alle categorie particolari di dati di cui all'art. 9 GDPR.

[50] J. A. Kroll , J. Huey , S. Barocas, E. W. Felten , J. R. Reidenberg , D. G. Robinson, H. Yu, *Accountable Algorithms*, 165 U. Pa. L. Rev. 633 (2017). Available at: https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3, p. removing protected attributes from the input data fails to provide adequate protection.174 : discrimination law has known for decades about the problem of proxy encodings of protected attributes and their use for making inferences about protected status that may lead to adverse, discriminatory effects.

[51] Corte di Giustizia, sentenza 10 luglio 2008, *Centrum voor gelijkheid van kansen en voor racismebestrijding v Firma Feryn NV* (Case C-54/07).

serie di elementi[52], ivi inclusi i «valori normativi che si applicano nell'ambito specifico dell'attività commerciale»[53]. Tra questi ultimi possono ricondursi i divieti di discriminazione desumibili dal diritto europeo e, in particolare, dalla direttiva 2004/113/CE, del13 dicembre 2004 che attua il principio della parità di trattamento tra uomini e donne per quanto riguarda l'accesso a beni e servizi e la loro fornitura[54].

Ai dubbi in merito alla attinenza di simili regolamentazioni all'ambito del diritto dei consumi, si può replicare osservando che l'economia digitale ci ha reso avvezzi alla diffusione di modelli economici, i quali, per via delle condotte e tecnologie implicate, creano od amplificano dei rischi anche rispetto a situazioni soggettive non comprese tradizionalmente nel perimetro di tale diritto (cfr. *ultra*). Ad esempio, in caso di lesione del diritto alla protezione dei dati personali nel contesto delle interazioni tra professionisti e consumatori, non si esita a fare ricorso alla disciplina in tema di pratiche commerciali sleali[55]. Una recente sentenza della Corte di giustizia dell'UE[56] ha definitivamente consacrato la c.d. *dottrina delle protezioni multilivello*, già sposata dalle corti ed autorità di vigilanza nazionali[57].

Va, poi, rammentato che la Proposta DSA contempla un art. 30 lett. d), relativo al *marketing* personalizzato, secondo cui, per le piattaforme online di grandi dimensioni, è doveroso rendere noto al destinatario del servizio digitale se il messaggio pubblicitario sia concepito per essere indirizzato specificamente ad uno o più gruppi di destinatari e, in caso affermativo, comunicare i principali parametri utilizzati a tale

---

[52] Tra cui, la natura della pratica, il settore e tipo di prodotto o servizio, nonché il consumatore medio destinatario della pratica (S. Orlando, *The Use of Unfair Contractual Terms as an Unfair Commercial Practice, in European Review of Contral Law*, 1/2011, p. 26 ss., p. 38).

[53] Cfr. Orientamenti sull'interpretazione e sull'applicazione della direttiva 2005/29/CE ((2021/C 526/01), d'ora in poi Linee guida Commissione UE - 2021.

[54] Per una dettagliata analisi si rinvia a O. Lynskey, H.W. Micklitz, P. Rott, *Personalised Pricing and Personalised Commercial Practices*, cit., p. 95 ss.

[55] La quale è inequivocabilmente preoccupa di tutelare gli interessi economici dei consumatori. Cfr. l'art. 1 Direttiva 2005/29/CE: "*La presente direttiva intende contribuire al corretto funzionamento del mercato interno e al conseguimento di un livello elevato di tutela dei consumatori mediante l'armonizzazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di pratiche commerciali sleali lesive degli interessi economici dei consumatori*".

[56] Corte di giustizia Ue, 28 aprile 2022, Associazione federale delle organizzazioni e associazioni di consumatori, Germania vs Meta Platform Ireland, Caso C-319/20.

[57] Cons. Stato, sentenza n. 02631/2021 (AGCM/Facebook).

scopo, compresi eventuali parametri usati "per escludere uno o più particolari gruppi". Si tratta di una disposizione che appare preoccupata delle ricadute di certe pratiche di *advertising* (incluse quelle che comportano l'impiego di RS) sugli interessi dei consumatori, nel cui novero viene inserito anche l'interesse alla non-discriminazione (cfr. *ultra*).

Affinché possa venire in rilievo una pratica commerciale scorretta, occorre, inoltre, dimostrare l'incidenza distorsiva della stessa su una decisione di natura economica; elemento che, nel caso di condotte discriminatorie, dovrebbe ravvisarsi nella circostanza che la pratica si sia tradotta nella privazione in radice della possibilità di adottare scelte di tale natura riguardo a certi beni o servizi (cfr. in merito, *ultra*).

Non va, tuttavia, dimenticato che, nei trattamenti automatizzati (quali quelli su cui i RS si basano), forme di discriminazione si verificano, per lo più, in modo non intenzionale, per effetto di *distorsioni* dipendenti dalla qualità dei dati utilizzati o emergenti nella fase di *training* degli algoritmi di raccomandazione [58], allorché proprio i comportamenti osservati durante l'addestramento degli algoritmi siano viziati da pregiudizi ed attitudini discriminatorie[59]. Per una serie di ragioni, si tratta di un aspetto sul quale è assai arduo esercitare un

[58] Si veda in merito E. Pellecchia, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leggi civ. comm.*, 2018, pp. 1210 ss., nonché P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law*, in *Common Market Law Review*, 2018, p. 1143 ss., disponibile in https://www.academia.edu/36494567/Teaching_Fairness_to_Artificial_Intelligence_Existing_and_Novel_Strategies_against_Algorithmic_Discrimination_under_EU_Law_Common_Market_Law_Review_2018_1143_1185_.

[59] J. A. Kroll , J. Huey , S. Barocas, E. W. Felten , J. R. Reidenberg , D. G. Robinson, H. Yu, *Accountable Algorithms*, 165 U. PA. L. REV. 633 (2017). Available at: https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3, p. 680: "algorithms that include some type of machine learning can lead to discriminatory results if the algorithms are trained on historical examples that reflect past prejudice or implicit bias, or on data that offer a statistically distorted picture of groups comprising the overall population. Tainted training data would be a problem, for example, if a program to select among job applicants is trained on the previous hiring decisions made by humans, and those previous decisions were themselves biased". Cfr., altresì, Zuiderveen Borgesius, F. (2018). *Discrimination, artificial intelligence, and algorithmic decision-making*. Council of Europe, Directorate General of Democracy. https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

controllo[60]. A questo fine, la proposta di regolamento presentata dalla Commissione Europea, nota come *Artificial Intelligence Act*, del 21 aprile 2021[61] (d'ora in poi "Proposta AIA") prevede requisiti relativi alla qualità dei dati, personali e non, impiegati dai fornitori di sistemi di Intelligenza Artificiale ad alto rischio, nonché impone l'adozione di adeguate pratiche di *governance* e di gestione dei dati, anche al fine di prevenire forme di discriminazione (cfr. artt. 10 e 17 AIA). Le suddette disposizioni, tuttavia, si applicheranno solamente ad una gamma ristretta di sistemi di IA, nel cui novero non rientrano i RS (come buona parte dei sistemi suscettibili di causare pregiudizi agli interessi dei consumatori[62]).

Il GDPR non dedica al problema specifica attenzione, pur menzionando l'eventualità che la profilazione possa produrre esiti

[60] Study *Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice* (PE 662.913, June 2021), in http://www.europarl.europa.eu/supporting-analyses, ove si propone, quale misura di prevenzione di tale rischio, l'accesso ai dati: "an access obligation that refers to not only the working algorithm but also grants access to data which was used to build and test the algorithm (so called "training data") is crucial for evaluating the compliance of these systems. Without the associated training data, it is difficult to backward-engineer the construction of the algorithm and assess its potential for, e.g., biases in content moderation or potential for data-based discrimination within recommender systems.

[61] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts {SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}.

[62] E' questo il punto di vista espresso nello studio della European Consumer Organization - Beuc, *Regulating AI to protect the consumer. Position paper on the AI Act* (BEUC-X-2021-088 - 07/10/2021), p. 17.

discriminatori[63]. E, tuttavia, sia nel regolare i trattamenti automatizzati[64], sia, più in generale, sancendo i due principi della *data protection by design* e *by default*, esso richiede al titolare del trattamento (che di regola non coincide con il fornitore del sistema di IA) l'adozione di adeguate misure tecniche ed organizzative di prevenzione, da integrare nella stessa elaborazione dell'attività di trattamento[65]. Nel caso di impiego di sistemi di IA, un simile requisito comporta la predisposizione, da parte del titolare del trattamento, di misure idonee a prevenire rischi di discriminazione e di scarsa accuratezza dei dati impiegati, almeno secondo l'interpretazione offerta dall' *Article 29 Data Protection Working Party* [66].

---

[63] Nel Considerando n. 71, il GDPR osserva che "è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti". Secondo alcuni commentatori, così statuendo, il GDPR presta attenzione all'accuratezza dei dati piuttosto che al loro impiego a fini discriminatori (G. Noto La Diega, *Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, 9 (2018) JIPITEC 3 para 1, p. 9: "it would seem that the GDPR's focus is misplaced. The point with discrimination is not only that the data are inaccurate or that they are not secure").

[64] Cfr. art. 22 GDPR (per il quale "*quando il trattamento interamente automatizzato è consentito sulla base del contratto o del consenso dell'interessato, il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato*…").

[65] Per un'analisi dei dati, distinta per tipi di piattaforme e rischi, cfr. L. Chen, R. Ma, A. Hannák, C. Wilson, *Investigating the Impact of Gender on Rank in Resume Search Engines*, in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (p. 651). *ACM*, 2018, disponibile in http://personalization.ccs.neu.edu/static/pdf/chen-chi18.pdf; nonché T. Zarsky, *Understanding Discrimination in the Scored Society*, in *Washington Law Review*, 89, 2014, pp. 1375 ss.

[66] G. Sartor, F. La Gioia, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, European Parliamentary Research Service, PE 641.530 – June 2020, p. 75:" With regard to AI, these measures should include controls over the representativeness of training sets, over the reasonableness of the inferences (including the logical and statistical methods adopted) and over the absence of unfairness and discrimination". Per una disamina delle misure adeguate, da adottare ai sensi dell'art. 22 GDPR, si vedano le raccomandazioni formulate in *Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of*

Un elemento di debolezza del GDPR, tuttavia, si rinviene rispetto ai casi in cui vengano in rilievo interessi di gruppi, anziché di specifici individui. Così accade, ad esempio, allorché la profilazione prenda di mira certe categorie, o viceversa, le escluda alla luce di date caratteristiche[67]: è arduo, in simili ipotesi, individuare una situazione giuridica individuale violata, come pure isolare un singolo soggetto interessato che sia stato leso dalla pratica. La disciplina in tema di decisione automatizzata di cui al GDPR appare, invero, preoccupata delle conseguenze significative della decisione automatizzata sull'interessato, senza contemplare i rischi collettivi derivanti dal modo in cui il sistema intelligente è usato, sebbene questi ultimi rappresentino la specie di rischi più frequentemente associata a tali sistemi[68]. Un'inversione di rotta potrebbe aversi per effetto di una recente decisione della Corte di giustizia UE, che, nel giudicare coerente con l'impianto e gli obiettivi del GDPR una normativa nazionale con cui si riconosca, ad associazioni a tutela dei diritti dei consumatori, la legittimazione a far valere qualsivoglia violazione delle disposizioni in tema di protezione dei dati personali[69] (sul presupposto che una tale violazione sia altresì in

Regulation 2016/679, cit., p. 31: "Il titolare del trattamento dovrebbe effettuare valutazioni frequenti degli insiemi di dati che tratta, in maniera da rilevare eventuali distorsioni, e sviluppare metodi per affrontare eventuali elementi pregiudizievoli, compreso un eccessivo affidamento sulle correlazioni. I sistemi che verificano gli algoritmi e i riesami periodici dell'esattezza e della pertinenza del processo decisionale automatizzato, compresa la profilazione, sono ulteriori misure utili. Il titolare del trattamento dovrebbe introdurre procedure e misure adeguate per prevenire errori, inesattezze o discriminazioni sulla base di categorie particolari di dati. Queste misure dovrebbero essere attuate ciclicamente; non soltanto in fase di progettazione, ma anche in continuativamente, durante l'applicazione della profilazione alle persone fisiche. L'esito di tali verifiche dovrebbe andare ad alimentare nuovamente la progettazione del sistema".

[67] N. Cherciu, *Non-personal data processing – why should we take it personally*?, in *European Journal of Privacy Law and Technologies*, 2020/2, p. 183 ss., p. 190.

[68] G.Comandé, G. Shneider, *Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of 'Health Data*, in European Journal of Health Law, 25 (2018) 284-307, p. 305: "the risks related to the processing of a certain dataset are not any more related to the single data subject but rather to the category in which the single data subject has been systematized"; Cfr. L. Kammourieh, *Group Privacy in the Age of Big Data*, in L. Taylor, L. Floridi and B. Van der Sloot (eds.), *Group Privacy-New Challenges of Data Technologies* (Springer: Basel, 2016), p. 37-66.

[69] Corte di giustizia Ue, 28 aprile 2022, Associazione federale delle organizzazioni e associazioni di consumatori, Germania vs Meta Platform Ireland, Caso C-319/20. Il quesito posto alla Corte era del seguente tenore: "..se l'articolo 80, paragrafo 2, dell'RGPD debba essere interpretato nel senso che esso osta ad una normativa nazionale che

contrasto con il divieto di ricorrere a pratiche commerciali scorrette e/o a clausole contrattuali vessatorie[70]), ha sostenuto l'ammissibilità di un'azione collettiva in caso di non conformità al GDPR, anche indipendentemente dalla lesione di una situazione giuridica di uno specifico soggetto interessato[71] (e dal conferimento di un mandato da parte di questi all'associazione). Ci si trova, dunque, al cospetto di una interpretazione volta ad estendere i confini del sistema della protezione dei dati personali, nella misura massima possibile[72], nonché ad un esempio di osmosi tra tale sistema ed il diritto dei consumi. Quest'ultimo, infatti, è per costituzione orientato a considerare anche interessi di natura collettiva: le disposizioni in tema di clausole vessatorie e quelle concernenti le pratiche commerciali scorrette possono entrare in gioco

consente ad un'associazione di tutela degli interessi dei consumatori di agire in giudizio, in assenza di un mandato che le sia stato conferito a tale scopo e indipendentemente dalla violazione di specifici diritti di un interessato, contro il presunto autore di un atto pregiudizievole per la protezione dei dati personali, facendo valere la violazione del divieto di pratiche commerciali sleali, la violazione di una legge in materia di tutela dei consumatori o la violazione del divieto di utilizzazione di condizioni generali di contratto nulle.".

[70] Cfr. Corte di giustizia Ue, 28 aprile 2022, Associazione federale delle organizzazioni e associazioni di consumatori, Germania vs Meta Platform Ireland, cit., par. 66.

[71] Cfr. Corte di giustizia Ue, 28 aprile 2022, Associazione federale delle organizzazioni e associazioni di consumatori, Germania vs Meta Platform Ireland, cit.: "Infatti, è sufficiente rilevare che la nozione di «interessato», ai sensi dell'articolo 4, punto 1, di tale regolamento, ricomprende non soltanto una «persona fisica identificata», ma anche una «persona fisica identificabile», ossia una persona fisica «che può essere identificata», direttamente o indirettamente, tramite un riferimento ad un identificativo... Date tali circostanze, anche la designazione di una categoria o di un gruppo di persone pregiudicate da tale trattamento può essere sufficiente ai fini della proposizione di detta azione rappresentativa". Inoltre, sempre secondo la Corte di giustizia, "in virtù dell'articolo 80, paragrafo 2, dell'RGPD, l'esercizio di un'azione rappresentativa non è neppure subordinato all'esistenza di una violazione concreta dei diritti di cui una persona beneficia sulla base delle norme in materia di protezione dei dati."; essendo sufficiente che l'ente legittimato ai sensi della normativa nazionale "«ritenga» che i diritti di un interessato previsti dal regolamento in parola siano stati violati in seguito al trattamento dei suoi dati personali..". In sintesi, a giudizio della Corte, "è sufficiente far valere che il trattamento di dati controverso è idoneo a pregiudicare i diritti che persone fisiche identificate o identificabili si vedono riconosciuti dal suddetto regolamento, senza che sia necessario provare un danno reale subito dall'interessato, in una situazione determinata, a causa della lesione dei suoi diritti. (cfr. paragrafi 70, 71 e 72)".

[72] J. Ausloos and R. Mahieu, *Harnessing the collective potential of GDPR access rights: towards an ecology of transparency*, in *Internet Policy Review.* 2020, available at https://policyreview.info/articles/news/harnessing-collective-potential-gdpr- access-rights-towards-ecology-transparency/1487.

a prescindere dalla lesione di una specifica situazione giuridica soggettiva ed anche nel caso di sola probabilità di lesione di simili interessi (cfr. *ultra*).

Ciò che, invece, occorre chiarire è se, per il caso di discriminazione non intenzionale prodotta da un trattamento automatizzato (dipendente, cioè, dal modo in cui un sistema di IA è concepito ed addestrato da colui che lo fornisce), la disciplina in tema di pratiche commerciali sleali possa fornire al professionista (che usa il sistema di IA) adeguati incentivi affinché quest'ultimo si adoperi per prevenire un simile rischio. Rilevante, per offrire risposta a tale interrogativo, appare ancora una volta il canone della diligenza professionale. Per aversi contrasto con tale parametro, non è necessaria l'intenzionalità dell'azione od omissione in cui la pratica consiste, bastando ravvisare l'esistenza dei doveri di attenzione e cura[73] in capo ai professionisti, desumibili alla luce della natura della pratica, del settore e tipo di prodotto o servizio, nonché del consumatore medio destinatario della pratica.

Pertanto, rispetto alle pratiche implicanti uso di RS, sono pertinenti, sia i doveri di protezione inerenti al rapporto contrattuale, che si instaura (anche in via tacita[74]) tra il fornitore del servizio digitale ed il suo destinatario, sia il grado di cura e attenzione desumibile dalla «legislazione settoriale applicabile alle piattaforme online» (cfr. Linee guida 2021).

Invero, si può notare che l'uso di RS rileva sotto forma di servizio accessorio (servizio di raccomandazione algoritmica, nelle diverse declinazioni, di pubblicità mirata, di classificazione delle informazioni, etc.) rispetto a quello principale, di intermediazione online, oggetto del contratto. Con la conseguenza che il professionista che lo eroga deve predisporre misure per sondare l'esistenza di rischi conoscibili e prevenirli (è cioè titolare di doveri di salvaguardia). Doveri di tal fatta invero sussistono in via generale allorché la natura o l'oggetto del

[73] Secondo l'art. 2, lett. *h)* direttiva 2005/29/CE, occorre avere riguardo al «normale grado della specifica competenza ed attenzione che ragionevolmente i consumatori attendono da un professionista nei loro confronti rispetto ai principi generali di correttezza e di buona fede nel settore di attività del professionista .

[74] Si vedano, in merito, le considerazioni di T. Rodríguez de las Heras Ballell, *The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU*, in *Italian Law Journal*, (2020) Vol. 03 – No. 01, pp. 149-176, p. 166; C. Camardi, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, in *Juscivile*, 2021/4, p. 870 ss., cfr. p. 912; S. Thobani, *L'esclusione da Facebbok tra lesione della libertà di espressione e diniego di accesso al mercato*, in *Persona e mercato* 2021/2, p. 427 ss.

contratto implichino una relazione tra le parti tale da giustificare esigenze di protezione della loro sfera patrimoniale e/o personale, tanto più quando si tratti di contratti che espongono una parte a rischi specifici connessi all'attività dell'altra[75].

Quanto sopra trova conferma nelle previsioni del DSA, per le quali le informazioni su criteri e finalità del servizio di raccomandazione fanno parte delle condizioni praticate dalle piattaforme online[76]. Sempre il DSA, inoltre, riconosce, rispetto alle pratiche che utilizzano tali sistemi, l'esistenza di rischi per le situazioni soggettive del destinatario del servizio/consumatore e, per talune specie di essi, espressamente pone dei doveri di protezione in capo alle piattaforme online di grandi dimensioni (cfr. ultra). Così, ad esempio, rispetto alle comunicazioni commerciali od offerte contrattuali personalizzate, il professionista deve predisporre misure per sondare e prevenire rischi di discriminazione legati al malfunzionamento del sistema di raccomandazioni impiegato (ricorrendo a forme di auditing degli algoritmi[77], etc.).

Simili considerazioni valgono anche per i motori di ricerca, con i quali l'utente conclude un contratto[78], da cui derivano doveri di protezione; ed ai quali – se si tratta di motori di ricerca di grandi dimensioni – si applica buona parte dell'impianto normativo del DSA[79].

---

[75] R. Scognamiglio, voce *Responsabilità contrattuale ed extracontrattuale*, in *Noviss. dig. it.*, XV, 1968 e in *Responsabilità civile e danno*, Torino, 2010.

[76] Perspicua appare la versione inglese dell'art. 24a DSA*:* «Online platforms shall set out in their terms and conditions…the main parameters used in their recommender systems…». Nel DSA il lemma condizione («terms and conditions») attiene all'assetto dei rapporti tra le parti (cfr. art. 2, lett. q DSA).

[77] Come desumibili dal principio di *accountability* di cui al GDPR, oramai estesi oltre l'ambito del trattamento dei dati personali. Cfr. M. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, in 92 *Southern California Law Review* (2019), p. 1529.

[78] Un contratto avente ad oggetto la prestazione di un servizio remunerato indirettamente attraverso la raccolta dei dati personali del destinatario e l'offerta di pubblicità. Cfr., in merito, N. Helberger, B.F. Zuiderveen, A. Reyna, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, in *Common Market Law Review*, 54, 2017, p. 1427 ss., p. 1444-1445. Milita a favore della natura contrattuale del rapporto tra servizio offerto dal provider del motore di ricerca ed il suo destinatario l'art. 12 Proposta DSA, secondo cui vanno chiaramente predisposte e comunicate a quest'ultimo le condizioni e termini del servizio stesso.

[79] Si applica, tra l'altro, ai motori di ricerca la sezione 4, del Capitolo III, DSA.

10.4.2. Segue. Il consumatore "schiavo dell'algoritmo" e vittima della "tirannide della maggioranza"

Inoltre, poiché i *RS* presuppongono un'attività di profilazione e quest'ultima, come ricordato, può basarsi, non solo sui dati personali dell'interessato, ma anche su quelli di intere popolazioni o categorie (con le quali il singolo condividerebbe alcune caratteristiche), il sistema potrebbe compiere inferenze non corrette, in quanto non corrispondenti a caratteristiche, comportamenti e bisogni del singolo consumatore [80]. Tale ultimo soggetto è di regola ignaro delle scelte alternative che gli vengono sottratte e non conosce il profilo[81] cui è stato assegnato e sulla cui base viene stabilita la gamma di opzioni resegli disponibili: egli sottostà alla "tirannide della maggioranza" (ogni qualvolta la raccomandazione sia il frutto di una previsione basata sull'osservazione di comportamenti predominanti di terzi nonché di una valutazione probabilistica che pone in relazione il soggetto considerato con il gruppo in cui è collocato[82]) e, in più, è "schiavo dell'algoritmo" (anziché autore di scelte compiute in autonomia)[83], giacché il professionista crea un "alter ego" digitale del consumatore ed utilizza le conoscenze che possiede su gusti e attitudini di costui, per condizionarne l'autonomia.

La più accorta letteratura si interroga in ordine alle opportune tutele e, innanzitutto, cerca una soglia di rilevanza giuridica oltre la quale sia possibile invocare i rimedi predisposti dal diritto.

Alcuni indici, in merito, possono trarsi dalla disciplina presente nel GDPR. Questo, invero, non vieta la profilazione che non si avvalga di dati personali non appartenenti a particolari categorie, ma si limita ad individuarne il fondamento giuridico nel consenso dell'interessato

---

[80] G. Comandè, *Regulating Algorithms' Regulation? First Ethico-Legal Principles, Problems and Opportunities of Algorithms*, in T. Cerquitelli, D. Quercia, F. Pasquale (eds.), *Transparent Data Mining for Small and Big Data* (Basel: Springer, 2017) 169, 174-176.

[81] Il punto 1, lett. *d)* dell'Allegato alla Raccomandazione CM/Rec (2010)13 del Consiglio d'Europa definisce "profilo": l'«insieme di dati caratterizzanti una categoria di persone fisiche che si intende applicare ad una persona fisica determinata».

[82] S. Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioural Advertising*, in *Berkeley Technology Law Journal*, Vol. 35, No. 2, 2020, in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639.

[83] L. Edwards, M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, (2017)16, disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855##]

(salve deroghe) ed a stabilire che a costui debbano essere fornite informazioni, affinché possa esprimere un valido consenso[84].

Sempre il GDPR detta una disciplina concernente le decisioni esclusivamente automatizzate in grado di incidere in modo significativo sull'interessato, ivi incluse quelle basate sulla profilazione (art. 22); la quale disciplina abbraccia anche i casi in cui una simile decisione si traduca in un condizionamento del comportamento economico e delle scelte di tale soggetto nel contesto di un rapporto di consumo. Alla luce della interpretazione che si suole fornire di tale regolamentazione, nella specifica ipotesi della pubblicità personalizzata che usa RS, il requisito del carattere significativo degli effetti della decisione sugli interessi economici dell'interessato-consumatore risulta soddisfatto soltanto in presenza di certe condizioni, che si tende ad individuare nel tipo di dati e tecniche impiegate, nelle aspettative dei consumatori (*ad es.*, nel fatto di essere ignari di interagire con un sistema intelligente), nella situazione del singolo o del gruppo di consumatori presi di mira, etc. Così, a titolo di esempio, la pratica del prezzo differenziato potrebbe essere sussunta nella previsione in parola, se il prezzo più gravoso venisse applicato ad una categoria svantaggiata sotto il profilo reddituale (in presenza quindi di conseguenze economiche pregiudizievoli) ovvero sfruttando la conoscenza da parte del professionista delle debolezze cognitive del singolo consumatore (conoscenza conseguita "spiandone" i comportamenti o applicando tecnologie di tipo predittivo).

In sintesi, la semplice menomazione della libertà di scelta di beni e servizi non viene considerata sufficiente ad attivare le tutele ivi considerate, occorrendo una significativa incidenza su interessi attinenti alla condizione del consumatore nella sfera digitale, tra i quali rientrano i già menzionati rischi di menomazione

[84] Il perno della tutela è dunque costituito dalla trasparenza del trattamento, tanto è vero che le linee guida del *Gruppo di lavoro Art. 29 per la protezione dei dati personali* interpretano le relative norme, in modo tale da ricavarne il dovere del titolare del trattamento di informare l'interessato, oltre del fatto di fare luogo a profilazione, anche circa i dati utilizzati e le relative finalità, con il fine di esercitare un controllo sulle possibili conseguenze svantaggiose del trattamento. L'eccessivo peso conferito dal GDPR al consenso informato dell'interessato viene tuttavia considerato un fattore di debolezza della soluzione di *policy* in questione, non soltanto perché è notoria la tendenza dei consumatori profilati a non prestare attenzione alcuna alle informazioni ricevute, ma anche per via dell'elevato grado di complessità che processi automatizzati, quali quello in questione, di regola, presentano (cfr. *ultra*).

dell'autodeterminazione, di lesione degli interessi economici di categorie già svantaggiate, di preclusione all'accesso a beni e servizi essenziali, etc.

Diverso appare, come si vedrà, il punto di vista del diritto dei consumi, per cui rileva la distorsione del comportamento economico del consumatore medio, in contrasto con la diligenza professionale (cfr. *ultra*).

10.4.3. La manipolazione dei consumatori attuata abusando delle modalità di interazione nel contesto online

L'impiego di RS può sfociare in vere e proprie forme di manipolazione, allorché siano ad essi associate pratiche ascrivibili al fenomeno dei c.d. *dark patterns*: si intende con tale espressione il ricorso a elementi di architettura delle interfacce online[85] o, più in generale, a strategie, atte a 'indurre' i consumatori ad assumere determinate decisioni di natura economica[86]. Nel contesto online, invero, i professionisti prestabiliscono le modalità tecniche delle interazioni con i consumatori e sono in grado di predeterminarne le risposte: il modo in cui le opzioni vengono presentate ai consumatori accresce le probabilità che date scelte siano assunte, ed altre vengano scartate. In tal caso, il professionista non si limita a selezionare le opzioni presentate al consumatore, ma 'dirige' quest'ultimo nelle proprie decisioni[87]. I c.d. *dark patterns* rappresentano una forma di abuso dell'asimmetria nei rapporti tra professionisti e consumatori, come riconosciuto dallo stesso Parlamento europeo[88], per il quale "*Le piattaforme online di dimensioni molto grandi*

[85] Secondo l'art. 2 lett. k, Proposta DSA, si intende per ""interfaccia online": qualsiasi software, compresi i siti web o parti di essi e le applicazioni, incluse le applicazioni mobili, *che consente ai destinatari del servizio di accedere al servizio intermediario in questione e di interagire con lo stesso*".

[86] Cfr. Linee guida Commissione UE – 2021, par. 4.2.7.

[87] E. Mik, *The erosion of autonomy in online consumer transactions*, (2016) 8(1), *Law, Innovation and Technology*, 1-38.

[88] Si veda il un nuovo Considerando n. 39a della Proposta DSA, versione approvata dal Parlamento europeo, secondo cui: "*I destinatari di un servizio dovrebbero essere in grado di adottare una decisione o una scelta libera, autonoma e informata quando si avvalgono di un servizio e i prestatori di servizi intermediari non dovrebbero utilizzare alcun mezzo, nemmeno attraverso la propria interfaccia, per fuorviare o compromettere tale decisione. In particolare, i*

dovrebbero attuare misure tecniche e organizzative appropriate per assicurare che i sistemi di raccomandazione siano progettati in modo orientato al consumatore e non influenzino il comportamento degli utenti finali attraverso dark pattern"[89].

La protezione da forme di indebito condizionamento del consumatore medio, implicanti (o idonee a determinare) una significativa distorsione del suo processo decisionale, è rimessa, nel diritto dei consumatori, al generale divieto di ricorso a pratiche commerciali sleali e, nel diritto generale dei contratti (allorché venga in rilievo la decisione relativa alla conclusione di un contratto), alle disposizioni in tema di vizi del consenso e/o di responsabilità precontrattuale. Senza soffermarsi sul secondo aspetto[90], basti rammentare, quanto al primo, il ruolo destinato ad essere assunto dalla clausola generale della diligenza professionale (anche in considerazione della difficoltà di sussumere simili pratiche nell'alveo di specifiche tipologie di pratiche sleali, come le pratiche aggressive[91]). Il concetto di diligenza professionale comprende principi quali quelli di 'pratica di mercato onesta', 'buona fede' e 'buona prassi di mercato'. Di conseguenza, le imprese, nel progettare l'interfaccia attraverso la quale interagiranno con i

destinatari del servizio dovrebbero poter prendere una siffatta decisione, tra l'altro, per quanto riguarda l'accettazione e le modifiche delle condizioni generali, delle pratiche pubblicitarie, delle impostazioni di riservatezza e di altro tipo e dei sistemi di raccomandazione quando interagiscono con i servizi intermediari. Tuttavia, talune pratiche di solito sfruttano le distorsioni cognitive e inducono i destinatari del servizio ad acquistare beni e servizi che non desiderano o a divulgare informazioni personali che essi preferirebbero non divulgare. Pertanto, ai prestatori di servizi intermediari dovrebbe essere vietato ingannare o esortare i destinatari del servizio e distorcere o limitare l'autonomia, il processo decisionale o la scelta dei destinatari del servizio attraverso la struttura, la progettazione o le funzionalità di un'interfaccia online o di una parte della stessa ("dark pattern").

[89] Cfr. Considerando n. 62, Proposta DSA, nella versione approvata dal Parlamento europeo il 20 gennaio 2022.

[90] Cfr. A. Gentili, *Pratiche sleali e tutele legali: dal modello economico alla disciplina giuridica*, in *Riv. dir. privato*, 2010, p. 60 ss.

[91] Ai sensi della disciplina in tema di pratiche commerciali aggressive, si ha indebito condizionamento in caso di "sfruttamento di una posizione di potere rispetto al consumatore per esercitare una pressione, anche senza il ricorso alla forza fisica o la minaccia di tale ricorso, in modo da limitare notevolmente la capacità del consumatore di prendere una decisione consapevole". Nel caso dei c.d. dark patterns, una posizione di potere del professionista è costituita dal fatto che questi, avendo disegnato la struttura dell'ambiente digitale, è in grado di condizionare l'interazione con il consumatore; ben più arduo appare, invece, ravvisare l'elemento della "pressione" da parte del professionista.

consumatori, devono attenersi a tali principi, facendo in modo che i consumatori non siano fuorviati nelle loro decisioni[92].

10.5. L'uso di RS per 'catturare' l'attenzione dei consumatori

Infine, i RS sono utilizzati per far sì che gli utenti restino 'attivi' online il più a lungo possibile, indirizzando loro contenuti informativi (spesso gratuiti), coerenti con il profilo dell'utente, in maniera tale da catturarne l'attenzione e ricavare introiti, grazie alla raccolta di dati e/o in virtù della pubblicità comportamentale (cfr. retro). Il DSA stabilisce in merito un requisito di trasparenza, laddove impone alle piattaforme online di grandi dimensioni di indicare per quali obiettivi il sistema in questione è stato 'ottimizzato', ivi incluso l'obiettivo di potenziare la risposta dell'utente alla pubblicità mirata (secondo la lettera dell'art. 24a DSA); la medesima proposta, poi, sottopone tali tecnologie e le relative pratiche ad un complesso di regole improntato alla individuazione e gestione dei relativi rischi (cfr. *ultra*).

Indipendentemente da tale specifica disciplina, anche la direttiva 2005/29/CE può venire in rilievo ogni qualvolta un simile modello economico si traduca in pratiche sleali, perché distorsive del comportamento economico dei consumatori.

Tale nozione invero viene interpretata estensivamente (nel senso di comprendere ogni decisione direttamente collegata con la decisione se acquistare o meno un prodotto, come, ad es., entrare in un negozio o visitare un sito Internet), sino ad includere comportamenti dei consumatori congruenti con il modello economico prescelto dal professionista. Così, se il professionista ottiene guadagni dalla circostanza che l'attenzione del consumatore venga catturata (si tratta della c.d. 'monetizzazione' dell'attenzione), il comportamento economico non può

[92] Beuc – Bureau européen des unions de consommateurs, *"Dark patterns" and the EU Consumer Law Acquis*, BEUC-X-2022-013 - 07/02/2022, p. 6. ACM (2021), "Protection of the online consumer. Boundaries of online persuasion", guidelines https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-onlineconsumer.pdf. Cfr., altresì, Linee guida Commissione UE – 2021, par. 4.2.7.: "Come principio generale, in base agli obblighi di diligenza professionale di cui all'articolo 5 della direttiva, i professionisti devono adottare misure appropriate per garantire che la progettazione della loro interfaccia non falsi le decisioni di natura commerciale dei consumatori".

non abbracciare l'atto di apporre un «*like*» o di «scorrere un *feed*», etc.; e qualsiasi pratica idonea a distorcere la decisione del consumatore a tale riguardo deve ritenersi sleale alla stregua di tale direttiva (ad es. fornire contenuti fuorvianti che si presentino come notizie)[93].

10.6. La tutela dell'autonomia dei consumatori alla mercé dei RS. La necessità di un cambio di paradigma: centralità da riconoscere alla c.d. privacy decisionale

Alla luce di quanto sopra, appare chiara la necessità di attuare un vero e proprio cambio di paradigma: si tratta invero di prestare protezione ai consumatori sia dinanzi a forme di 'sorveglianza' [94], attuate dalle imprese dell'economia digitale (la dimensione denominata *informational privacy*), sia, e soprattutto, da pratiche di condizionamento della loro autonomia (la c.d. *decisional privacy*)[95].

Così, i rischi del primo tipo possono essere fronteggiati incentivando modalità di raccolta e conservazione dei dati personali, che siano conformi alla disciplina concernente tracciamento ed *e-privacy*[96] e, soprattutto, ai principi in materia di protezione dei dati[97].

---

[93] Linee guida Commissione UE 2021: «..la direttiva riguarderebbe anche pratiche commerciali come quella di catturare l'attenzione del consumatore, che sfocia nell'adozione di decisioni di natura commerciale quali continuare a utilizzare il servizio (per es. scorrendo un feed), visualizzare un contenuto pubblicitario o cliccare su un link»

[94] Così M. Lanzing, *Strongly Recommended". Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies*, in *Philos. Technol*. (2019) 32, pp. 549–568 https://doi.org/10.1007/s13347-018-0316-4.

[95] Si vedano già su questi temi N. Irti, *Letture bettiane sul negozio giuridico*, Milano, 1991; nonché S. Rodotà, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, 26th International Conference on Privacy and Personal Data Protection, Poland, Wroclaw, 14-16 Settembre 2004, in *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1049293*.

[96] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[97] Ad esempio, uso di architetture *privacy-enhancing* per conservare i dati in separati e decentralizzati *database*; ricorso all'anonimizzazione, uso dell'*encryption*, etc. Cfr. Cong Wang, Yifeng Zheng, Jinghua Jiang, Kui Ren, *Toward Privacy-Preserving Personalized Recommendation Services*, in *Engineering* 4 (2018), pp. 21–28.

Invece, il ricorso alla sole regolamentazioni appena ricordate rischia di rivelarsi inadeguato a difendere il singolo da menomazioni della libertà di autodeterminarsi[98].

Si consideri, infatti, che la profilazione di un utente online, su cui i RS di basano, può avere luogo utilizzando dati anche di natura non personale, quali dati anonimizzati e dati di terzi. Inoltre, le inferenze ottenute grazie all'attività di profilazione, e tra queste, lo stesso profilo assegnato all'utente, costituiscono nuova conoscenza; è dubbio quindi che esse possano ricevere - o, quanto meno, che possano ricevere sempre e comunque – la qualifica di dati personali[99] (a meno che non si adotti una nozione lata di "soggetto interessato", intendendo per tale l'individuo cui i dati inferiti vengono "applicati"[100]).

La soluzione che ravvisa, in tali casi, dei dati personali (ed applica il GDPR) va incontro ad incertezze interpretative di non poco conto: ad esempio, se possa essere garantito all'interessato l'esercizio dei diritti riconosciutigli dal GDPR, tra cui quello di accesso e cancellazione del profilo. Evidenti le conseguenze pratiche della soluzione negativa: l'interessato, non potendo accedere all'algoritmo né ai dati personali di terzi, non ha modo di verificare l'accuratezza del profilo, né di sindacare la bontà dell'inferenza[101]. Un simile diritto, poi, andrebbe

---

[98] S. Myers West, *Data Capitalism: Redefining the Logics of Surveillance and Privacy*, in *Business & Society*, (2017), disponibile in https://journals.sagepub.com/doi/full/10.1177/0007650317718185.

[99] M. Hildebrandt, *Profiling: From data to knowledge*', in *Datenschutz und Datensicherheit – DuD*, 2006, 30, pp. 548-550: "If inferred data is ascribed to groups or categories, it may not be personal data. However, in micro- targeting inferred data will often be ascribed to an identified or identifiable natural person, yielding personal data. If inferred data is personal data, there may still be practical issues with data subject rights.".

[100] G.Comandé, G. Shneider, *Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of 'Health Data*, in *European Journal of Health Law*, 25 (2018), pp. 284-307, p. 305: "it must be observed how the collective profiling activities carried out over probabilistically-inferred data seem to impair the same notion of data subject, traditionally intended as the physical individual to which a certain piece or set of data is to be referred to. In consequence of the growing classification patterns through which an individual with certain features is likely to bear the same decision-making outcomes of subjects with same or similar profiles, the latitude of the same notion of data subject should equally be reconsidered. Data subjects are not only- or not any more- the generator of specific data from which new data can be derived, but also the subjects to whom secondary data generated by other similar subjects are applied for the purposes of decision-making".

[101] *B. Custers, Profiling as inferred data. Amplifier effects and positive feedback loops*, in E. Bayamlıoğlu, I. Baraluic, L. Janssens, M. Hildebrandt (eds), *Being Profiled. 10 Years of Profiling the European Citizen*, Amsterdam University Press., 2018, pp. 112-115,

bilanciato con diritti di esclusiva e segreti industriali degli operatori economici che detengono i profili (si consideri il timore che, via *reverse engineering*, l'accesso al profilo consenta di risalire ad elementi protetti, quali il *software*[102].

Tutto quando sopra rilevato offre testimonianza dei limiti insiti nella distinzione tra dati personali e dati non personali[103], quando applicata a tali tecnologie[104]. Ed invita piuttosto a percorrere strade alternative, spostando l'attenzione sulla categoria dei c.d. *consumer behavioral data*[105]. Con tale espressione si intendono le informazioni su tratti della personalità, gusti, bisogni, etc., di cui le imprese si servono, per condizionare il comportamento economico dei consumatori[106]. I

https://ssrn.com/abstract=3466857. Cfr. J. Poort, F. J. Zuiderveen Borgesius, *Does Everyone Have a Price? Understanding People's Attitude towards Online and Offline Price Discrimination*, in *Internet Policy Review* (2019) 8 (1), in https://doi.org/10.14763/2019.1.1383.

[102] Cfr. *Linee guida Article 29 Working party in materia di profilazione*, cit., p. 19, il quale rammenta come ai sensi del Considerando n. 63 GDPR, il diritto di accesso "non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software". Al tempo stesso, secondo le medesime linee guida, "il titolare del trattamento non può fare affidamento sulla protezione dei segreti aziendali come scusa per negare l'accesso o rifiutarsi di fornire informazioni all'interessato".

[103] Critiche alla distinzione dei dati in categorie sono formulate da Autorità per le Garanzie nelle Comunicazioni, *Big Data. Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, p. 14: l'utilizzo di algoritmi applicati ai Big Data consente di estrarre o anche di prevedere informazioni personali, partendo da dataset di informazioni non personali, correlati con altri dataset di differente origine e contenuto. Cfr., in merito, I. Graef, R. Gellert, M. Husovec, *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation* (TILEC Discussion Paper No 2018-029, 2018) p. 8, nonché *European Commission, Communication from the Commission. A European strategy for data* (COM(2020) 66 final), p. 6.

[104] La memorizzazione delle informazioni e l'accesso alle informazioni già memorizzate nell'apparecchiatura terminale di un abbonato/utente (ad esempio, un telefono, un computer, un veicolo connesso o un altoparlante intelligente) richiede il consenso informato preventivo degli abbonati, a prescindere da qualsiasi qualificazione dei dati personali di tali informazioni (cfr. Corte di giustizia UE, sentenza *Planet49 GmbH*, 1° ottobre 2019, C-673/17, EU:C:2019:801, 70 e 71).

[105] M. Hildebrandt, *Profiling: From data to knowledge*', in *Datenschutz und Datensicherheit – DuD*, 2006, 30, pp. 548-550: 'as a consequence of the focus on data instead of knowledge, the debate seems to be directed to anonymisation, or the use of pseudonyms, in order to protect personal data".

[106] G. Sartor, F. La Gioia, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, European Parliamentary Research Service, PE 641.530 – June 2020, p. 74: "Special considerations apply to the inference of personal data. A possible

consumatori, in questa diversa prospettiva, vanno tutelati contro un simile uso di tali informazioni (ad esempio, dall'impiego del profilo in cui sono collocati per interferire con le proprie decisioni), indipendentemente dalla loro natura.

Le autorità di vigilanza dei mercati tendono a ricavare dalle norme in tema di pratiche commerciali ingannevoli un dovere del professionista di fornire tutte quelle informazioni che, se omesse, possono falsare il comportamento economico del consumatore medio e, dunque, anche di informare se fa luogo ad attività quali il tracciamento online, la profilazione e le connesse pratiche di *personalizzazione*[107], per finalità commerciali. La disciplina sulle pratiche ingannevoli è impiegata con il dichiarato fine di ampliare l'arsenale delle tutele invocabili dal soggetto interessato, includendovi quelle proprie del diritto dei consumi; essa, tuttavia, non pare idonea a farsi carico di due ordini di problemi: il grado di consapevolezza conseguibile grazie alle informazioni trasmesse[108]; il tipo di asimmetria dei rapporti tra professionisti e consumatori nel contesto online, la quale non assume carattere esclusivamente informativo[109].

---

approach could consist in distinguishing the cases in which an inference of personal data is accomplished without engaging in consequential activities, i.e., the inferred personal data are merely the output of a computation which does not trigger consequential actions, and the cases in which the inferred data are also used as input for making assessment and decisions. In the latter case, the data should definitely count as newly collected personal data".

[107] Si veda *European Commission, Staff Working Document on Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices*, SWD(2016)163 final, p. 24, sulla profilazione e personalizzazione, e p. 37.

[108] Altra e diversa questione è, invece, dedurre dal divieto di omettere informazioni rilevanti, di cui alla disciplina in parola, un dovere di informazione esteso a far conseguire consapevolezza circa il grado di personalizzazione, il tipo di informazioni impiegate, etc. Cfr. M. Ebers, *Liability For Artificial Intelligence And EU Consumer Law*, in *Journal of Intellectual Property, Information technology and E-commerce Law*,12/2021, pp.204 ss., p. 209.

[109] Nei mercati digitali, l'asimmetria tra professionisti e consumatori non è meramente informativa, bensì di triplice natura: 1) strutturale, legata al fatto che il professionista usa dati, anche personali (ed è in grado di conoscere e prevedere comportamenti, bisogni, interessi, etc., dei consumatori) e stabilisce con le interfacce online le modalità delle interazioni con i consumatori; ii) relazionale, giacché il potere negoziale del consumatore è modesto, disponendo egli dispone di poche o di nessuna alternativa (il prodotto o servizio può non essere essenziale, ma è difficilmente sostituibile con prodotti e servizi di analoga natura e qualità); ii) basata su un deficit di consapevolezza da parte del consumatore in ordine ai rischi inerenti alle tecnologie usate, le quali sono connotate da opacità (tecnica e legale), tale da rendere difficile persino la supervisione delle autorità di vigilanza. Cfr., in merito, Beuc, Bureau Européen des Unions de

10.6.1. La "fallacia della trasparenza". La comprensibilità della logica dei RS

La pertinente letteratura registra la prassi delle piattaforme digitali di divulgare informazioni tecniche circa i più noti RS (ad es., quelli utilizzati da Google, Twitter o da YouTube); gli esperti di *computer science*, tuttavia, ci rendono avvertiti del fatto che, se pure fossero resi conoscibili i codici di cui gli algoritmi sono composti, questi ultimi nulla "significherebbero" (persino per gli stessi esperti e, dunque, tanto meno) per il destinatario della raccomandazione[110].

Si mostra allora in tutta la sua evidenza la c.d. fallacia della trasparenza[111], che si ha quando la trasmissione di informazioni non sortisce il risultato di conferire al destinatario della stessa maggior consapevolezza, né quindi miglior tutela (specialmente allorché il consumatore non abbia valide alternative, in termini di fungibilità dei prodotti o servizi, o perché certe pratiche sono comuni a tutti i concorrenti in un determinato mercato). In un simile vizio incorrono le discipline già ricordate (quali quella presente nella direttiva di modernizzazione), che si limitano ad informare in modo standardizzato il consumatore del fatto che alla interazione con il professionista sovraintende un algoritmo (nella specie un RS), descrivendone genericamente caratteristiche tecniche e/o criteri[112].

Ancor più criticabile appare poi la Proposta AIA, laddove obbliga i fornitori di sistemi di IA destinati ad interagire con le persone fisiche - indipendentemente dall'impiego di dati personali e dal grado di

---

Consommateurs, *EU consumer protection 2.0. Protecting fairness and consumer choice in a digital economy*, BEUC-X-2022-015 – 10/02/2022, p. 5.

[110] J. Stray, *Show me the algorithm: transparency in recommendation systems*, in https://srinstitute.utoronto.ca/news/recommendation-systems-transparency; M.Z. van Drunen, N. Helberger, M. Bastian, *Know your algorithm: what media organizations need to explain to their users about news personalization*, in *International Data Privacy Law*, 2019, Vol. 9, No. 4 , p. 220-235.

[111] L. Edwards, M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, (2017)16, disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855##].

[112] A. Weller, *Challenges for transparency*, *Paper presented at the 2017 ICML Workshop on Human Interpretability in Machine Learning (WHI 2017), Sydney*, disponibile in https://arxiv.org/abs/1708.01870; M. Ananny, K. Crawford, *Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability*, in *New Media & Society*, 20/2016, p. 973.

rischio in essi insito - a progettare e sviluppare gli stessi in modo tale che queste siano informate del fatto di stare interagendo con tali sistemi (cfr. art. 52, par.1). I primi commentatori della proposta ne ricavano un obbligo di trasparenza talmente debole da consistere in una mera avvertenza[113].

Si tratta, dunque, di declinare la trasparenza in altro modo: quale elemento inserito in un disegno normativo più ampio, che prenda in considerazione non soltanto i consumatori/destinatari di un servizio digitale, ma anche le autorità di supervisione, i regolatori, gli enti della società civile, etc., e valga così ad agevolare la supervisione e l'*enforcement*, pubblico e privato (cfr. *ultra*), individuale e collettivo, di pratiche implicanti uso di tecnologie quali quella in parola. In quest'ottica vanno interpretati, di conseguenza, contenuti e modalità degli stessi requisiti di trasparenza.

Così, una prima opzione di *policy*, caldeggiata da più parti, suggerisce di indurre i professionisti che usano *RS* a fornire informazioni, il cui oggetto sia "ritagliato su misura" del destinatario: informazioni personalizzate, dunque, proprio come il consiglio che questi riceve dall'algoritmo, e consistenti in spiegazioni circa il modo in cui vengono generate le raccomandazioni, vale a dire, intorno alle ragioni per cui il sistema ritiene che alcune opzioni siano rilevanti per il destinatario e, quindi, circa il profilo in cui egli è collocato. In sintesi, la tutela giuridica ottimale risiede, in quest'ottica, nel fornire una giustificazione della raccomandazione algoritmica, che sia specifica e comprensibile per il singolo destinatario. Ciò, tuttavia, comporta che siano impiegate delle tecnologie le cui logiche siano spiegabili[114] o, quanto meno, il cui risultato (l'output, secondo la terminologia corrente) sia interpretabile[115]. Il perno della questione consiste dunque nella capacità degli istituti giuridici esistenti di offrire adeguati incentivi affinché

[113] Cfr. European Consumer Organization - Beuc, *Regulating AI to protect the consumer. Position paper on the AI Act* (BEUC-X-2021-088 - 07/10/2021), p. 20.

[114] Il che può non accadere allorché siano impiegate metodologie di *machine learning*, che apprendono da diverse fonti e sono capaci di adattamento, in una parola, che sono opache, per ragioni tecniche (o perché protette da diritti di esclusiva e segreti commerciali). A.D. Selbst, J. Powles, *Meaningful information and the right to explanation*, in *International Data Privacy Law,* 39/2017, p. 233.

[115] P. Hacker, R. Krestel, S. Grundmann, F. Naumann, *Explainable AI under contract and tort law: legal incentives and technical challenges*, in *Artificial Intelligence and Law*, 28/2020, pp. 415 ss., p. 431.

tali tecnologie vengano, a monte, concepite e sviluppate in maniera tale da essere intellegibili [116].

Nell'ambito del GDPR, alla ridotta capacità di controllo dell'individuo sui trattamenti automatizzati che lo riguardano dovrebbe ovviarsi grazie all'art. 22, disposizione che però presta il fianco a numerose critiche. E' ivi previsto, invero, un divieto di fare luogo a decisioni solamente automatizzate, dalle maglie eccessivamente larghe, giacché tollera troppe deroghe (il consenso dell'interessato è sufficiente a rimuovere il divieto[117]). Inoltre, il dettato normativo prevede che siano fornite *ex ante* "informazioni significative" sulla logica utilizzata e sulle conseguenze previste del trattamento per l'interessato[118]; senza, tuttavia, chiarire cosa debba intendersi per informazioni significative[119]. Un analogo diritto è riconosciuto all'interessato anche *ex post*, la cui natura, tuttavia, è a dir poco dibattuta, incerto essendo se egli possa pretendere, anziché una mera informazione[120], una vera e propria spiegazione[121]. Cosicché la protezione di cui egli astrattamente gode dipende, in ultima istanza, sia dalla acquisita consapevolezza circa l'esistenza

---

[116] C. Reed, E. Kennedy, S. Silva, *Responsibility, Autonomy and Accountability: Legal Liability for Machine Learning*, cit., p. 26. In questa logica sembra muoversi l'art. 13 Proposta AIA, per il quale il fornitore di un sistema di IA ad alto rischio deve garantire che il funzionamento dello stesso sia sufficientemente trasparente, nonché deve consentire agli utenti (da intendere nell'accezione ivi accolta) di interpretare l'*output* del sistema anche al fine di essere in grado di adempiere agli obblighi imposti dalla legge, ivi inclusi gli obblighi di informazione nei confronti dei destinatari delle decisioni algoritmiche. Tale previsione, tuttavia, non si applica ai RS.

[117] C. Kuner, *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, in *International Data Privacy Law* 2017, vol. 7, n.1, p. 1 ss.: "[m]achine learning is data driven, typically involving both existing data sets and live data streams in complex training and deployment workflow [therefore it] may be difficult to reconcile such dynamic processes with purposes that are specified narrowly in advance".

[118] Cfr. articoli 13(2)(f) e14(2)(g) GDPR.

[119] M.Z. van Drunen, N. Helberger, M. Bastian, *Know your algorithm: what media organizations need to explain to their users about news personalization*, cit., p. 222.

[120] Così, S. Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, cit., nonché L. Edwards, M. Veale, *Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*, in *Duke Law & Technology Review*, 2017, 16(1) 18.

[121] G. Malgieri, G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, (2017) 7(4), p. 243. Cfr. M.Brkan, *AI-Supported Decision-Making under the General Data Protection Regulation*, Proceedings of the 16th international conference on Artificial intelligence and law (2017) 5 <https://doi. org/10.1145/3086512.3086513>

del trattamento e le relative implicazioni[122]; sia dalla di lui volontà di esercitare tale diritto. E' realistico stimare che entrambi tali fattori difficilmente si riscontrino nel contesto delle interazioni online, non fosse altro che per la rapidità e scarsa razionalità che le contraddistinguono. Modesta incidenza in termini di effettività della tutela presentano, dunque, soluzioni – quale quella innanzi ricordata in tema di prezzo personalizzato (cfr. *retro*) - che rimettano al solo GDPR la tutela degli interessi dei consumatori.

10.6.2. Dalla comprensibilità dei RS alla promozione dell'autodeterminazione del destinatario della raccomandazione. L''illusione del controllo'

Un presidio alternativo, propugnato dagli esperti di *data science* e successivamente fatto proprio da una parte della letteratura giuridica, consiste nell'indurre a predisporre strumenti per promuovere (la c.d. *agency*, vale a dire) la capacità del singolo di autodeterminarsi nelle interazioni con un sistema intelligente, permettendogli di esercitare un certo grado di controllo sullo stesso o su alcune sue funzionalità, in modo che egli non resti assoggettato a decisioni che non possa influenzare. Si tratta, in quest'ottica, di indurre le imprese ad utilizzare *RS* che siano *by design* modificabili ed adattabili dal destinatario[123], che abilitino, cioè, quest'ultimo a controllare quali dati vengono utilizzati ed in qual modo (ad esempio, escludendo *in toto* l'impiego di dati personali o soltanto di certe categorie di essi) e/o a 'regolare' il livello di personalizzazione dei RS. Verrebbe, in tal modo, creato un alter-ego digitale, alternativo rispetto a quello costruito unilateralmente dal professionista.

---

[122] I. Mendoza, L. A. Bygrave, *The Right Not to Be Subject to Automated Decisions Based on Profiling* in TE. Synodinou, P. Jougleux, C. Markou, T. Prastitou (eds) EU Internet Law. Springer, Cham, in EU Internet Law (Springer International Publishing, 2017/ 85, pp. 77 ss., <http://link.springer.com/10.1007/978-3-319-64955-9_4> .

[123] Sugli impieghi dei RS nel commercio elettronico, cfr. Paraschakis (2016, 2017, 2018): per il quale i rischi ad essi collegati trovano soluzione adottando un *user-centred design approach.*

Diverse critiche possono essere mosse anche a quest'ordine di pensiero: innanzitutto, esso presuppone che sia garantita una sorta di accesso al profilo applicato al consumatore, il quale, però, anch'esso, proprio come il codice dell'algoritmo, scarso significato avrebbe per il destinatario della raccomandazione[124]; inoltre, fare affidamento su una simile soluzioni equivarrebbe ad offrire livelli di protezione di intensità diversa, a seconda del grado di consapevolezza e abilità tecnica di ciascun consumatore. Si avrebbe allora un *empowerment* soltanto nominale dei consumatori, su cui verrebbe a ricadere interamente la responsabilità della tutela dei propri interessi[125]. Soprattutto, non si raggiungerebbe l'obiettivo di garantire il diritto ad interagire online nella veste di "consumatore qualunque", che non sia cioè bersaglio di consigli, comunicazioni commerciali ed offerte contrattuali, di natura personalizzata.

10.6.3. L'opzione di policy che fa leva sulla supervisione pubblica degli standard imposti ai professionisti che impiegano RS nelle loro interazioni con i consumatori

In sintesi, la predisposizione di strumenti di tale natura non può essere vista come una panacea, ma soltanto come una scelta di *policy* complementare rispetto ad altre, maggiormente adeguate al dominio dei rischi insiti in tali tecnologie.

Appare decisivo, piuttosto, promuovere *l'accountability* dei professionisti che usano RS, attraverso adeguata supervisione ed *enforcement*

---

[124] S. Milano, M. Taddeo, L. Floridi, *Recommender systems and their ethical challenges*, cit., p. 962: "the category 'dog owner' may be recognisable as significant to a user, while 'bought a novelty sweater' would be less socially significant; yet the RS may still regard it as statistically significant when making inferences about the preferences of the user".

[125] Non vanno invero dimenticati né i rischi insiti nell'eccesso di opzioni (si pensi al c.d. "control paradox"), né le insidie proprie del ricorso a strumenti che spesso servono soltanto a creare l'illusione di una possibilità di controllo da parte dell'individuo. Cfr. A. Acquisti, L. Brandimarte, G. Loewenstein, *Privacy and Human Behavior in the Age of Information*, in *Science* 347 2015(6221), pp. 509–514, in https://doi.org/10.1126/science.aaa1465, nonché K. Vaccaro et al., *The Illusion of Control: Placebo Effects of Control Settings*, in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Aprile 2018, Paper No.: 16, pp. 1–13, in https://doi.org/10.1145/3173574.3173590

da parte delle autorità pubbliche[126]. A tal fine, tuttavia, è necessario superare l'ostacolo rappresentato dall'elevato grado di sofisticatezza e opacità raggiunto da tali tecnologie, attraverso regole di trasparenza, che abbiano come destinatari principalmente tali autorità (anziché solamente gli utenti finali). A queste ultime, innanzitutto, è opportuno che sia diretto il flusso informativo, il cui oggetto e le cui forme vanno dunque adeguati al tipo di destinatari ed alle relative finalità. Nell'ambito di simili strumenti, la letteratura sui RS menziona il ricorso a forme di *auditing* da parte di esperti indipendenti, l'introduzione di doveri di documentazione dei dati, di *logging* per registrare il funzionamento e l'uso dei sistemi intelligenti, etc.[127]; in sintesi, si tratta di soluzioni di politica legislativa volte ad arginare la schiavitù dell'individuo dinanzi all'algoritmo, restituendogli il potere decisionale perduto. In tale direzione si muove, come si dirà, la Proposta DSA (cfr. *ultra*).

10.7. I RS nella Proposta DSA. Trasparenza e controllo dei RS da parte del destinatario dei servizi erogati da piattaforme online. Il diritto ad essere "consumatori qualunque"

La Proposta DSA, nella versione originaria, si limitava ad introdurre un requisito di trasparenza relativo all'impiego di RS da parte di piattaforme di grandi dimensioni, da adempiere però fornendo un'informazione standardizzata, indicando cioè, all'interno di termini e condizioni contrattuali, i principali parametri impiegati dal sistema; si statuiva poi che l'informazione dovesse riguardare anche eventuali funzionalità presenti nel sistema, aventi il fine di consentire al

[126] Ed infatti, stabilire obblighi di diligenza non appare bastevole, in caso insufficiente oversight and enforcement delle violazioni della pertinente disciplina by public bodies. M. Perel, M., N. Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, in *Florida Law Review*, 2017/69, p. 181, nonché P.T. Kim, *Auditing Algorithms for Discrimination*, in *University of Pennsylvania Law Review Online*, 2017 166(1), 189.

[127] Cfr. S. Singh, *Why Am I Seeing This? How Video and E-Commerce Platforms Use Recommendation Systems to Shape User Experiences*, 25 marzo 2020, p. 44, in https://d1y8sb8igg2f8e.cloudfront.net/documents/Why_Am_I_Seeing_This_2020-03-25.pdf. Cfr., altresì, Id., *Charting a Path Forward. Promoting Fairness, Accountability, and Transparency in Algorithmic Content Shaping*, in https://www.newamerica.org/oti/reports/charting-path-forward/.

destinatario del servizio di modificare ed influenzare i suddetti parametri, inclusa l'opzione di non basare la raccomandazione sull'attività di profilazione, intesa nell'accezione di cui al GDPR[128]. Ancora una volta, il legislatore dava mostra di riporre eccessiva fiducia nella introduzione di un requisito di trasparenza, ricalcando, per giunta, la tanto contestata previsione di cui all'art. 22 GDPR in materia di trattamenti automatizzati[129]. Il dettato normativo, inoltre, non obbligava tali specie di piattaforme a mettere a disposizione del destinatario del servizio una simile opzione, né offriva incentivi di sorta per far sì che le prime facessero a meno della profilazione[130].

Successivamente, il Parlamento europeo, tra gli emendamenti alla Proposta originaria di DSA del gennaio 2022[131], ha inserito una disposizione *ad hoc*, l'art. 24a (cfr. considerando 52c), indirizzata ad ogni piattaforma online (intesa nell'accezione ivi chiarita[132]). Secondo tale disposizione, oltre ad una chiara comunicazione standardizzata nell'ambito delle condizioni d'uso: *i)* occorre che l'utente sia avvisato di essere destinatario di una raccomandazione algoritmica già nel contesto dell'interfaccia tra sistema e utente stesso[133]; *ii)* debbono, poi,

---

[128] Invero, secondo l'art. 29 del DSA, versione del dicembre 2020, "Very large online platforms that use recommender systems shall set out in their terms and conditions, in a clear, accessible and easily comprehensible manner, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters that they may have made available, including at least one option which is not based on profiling, within the meaning of Article 4 (4) of Regulation (EU) 2016/679".

[129] Hacker, cit., p. 28, con l'unica differenza che l'informazione da fornire secondo l'art. 29 DSA concerne i principali parametri usati dal sistema.

[130] N. Helberger, M. van Drunen, S. Vrijenhoek, J.Möller, *Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath*, in https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large.

[131] Critiche relative al tenore dell'Articolo 29 (1) della Proposta DSA sono state manifestate dall'EDPS, nella Opinion 1/2021 in merito alla Proposta DSA (Opinion 1/2021 (10 febbraio 2021) on the Proposal for a Digital Services Act). Secondo l'Autorità, tale diposizione non appare adeguata a perseguire le declamate finalità della regolazione: l'Autorità raccomandava di imporre dei requisiti di *legal design* al fine di rendere l'informazione più efficace, e, prima ancora, di chiarire cosa debba intendersi per "principali parametri" sulla cui base la raccomandazione algoritmica viene elaborata, da esporre al destinatario della raccomandazione.

[132] Cfr. Art. 2, let. h, DSA: "'online platform' means a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service".

[133] Giacché, come alcune ricerche mostrano, i consumatori hanno scarsa consapevolezza che le comunicazioni loro indirizzate sono, ad un tempo, basate su informazioni

essere comunicati i parametri individualmente e collettivamente più rilevanti impiegati dal sistema (unitamente alla importanza relativa degli stessi); *iii)* vanno, infine, spiegati sia le finalità del sistema, sia, se pertinente, il ruolo assunto, nella elaborazione della raccomandazione, dal comportamento dei destinatari del servizio[134]. Le informazioni prescritte in tale versione sono dunque molto dettagliate, tanto è vero che alcune di esse sono state rimosse nella versione della proposta dell'aprile 2022[135].

Nei casi di ricorso a RS per fini di pubblicità personalizzata, vengono in rilievo altresì i requisiti di trasparenza aggiuntivi previsti dalla Proposta DSA[136], di cui sono destinatarie le piattaforme online di grandi dimensioni.

---

ricavate dal loro comportamento, osservato per mezzo di sistemi di tracciamento, ma anche condizionate da previsioni circa il loro comportamento futuro. Cfr. T. Dehling, Y. Zhang, A. Sunyaev, *Consumer Perceptions of Online Behavioral Advertising*, in *Proceedings of the 21st IEEE Conference on Business Informatics*, 2019.

134 Cfr. articolo 24°, gennaio 2022: "1. Le piattaforme online indicano nelle loro condizioni generali e tramite una risorsa online designata, direttamente raggiungibile e facilmente reperibile mediante l'interfaccia online della piattaforma online, quando un contenuto viene raccomandato, in modo chiaro, accessibile e facilmente comprensibile, i principali parametri utilizzati nei loro sistemi di raccomandazione, nonché le eventuali opzioni messe a disposizione del destinatario del servizio per consentirgli di modificare o influenzare tali parametri principali. 2. I principali parametri di cui al paragrafo 1 includono quanto meno le informazioni seguenti: a) i principali criteri utilizzati dal sistema in questione che, singolarmente o collettivamente, sono più significativi per determinare le raccomandazioni; b) l'importanza relativa di tali parametri; c) per quali obiettivi il sistema in questione è stato ottimizzato; nonché d)se applicabile, una spiegazione del ruolo che svolge il comportamento dei destinatari del servizio rispetto a come il sistema in questione produce i suoi risultati. I requisiti di cui al paragrafo 2 non pregiudicano le norme in materia di protezione dei segreti commerciali e dei diritti di proprietà intellettuale...

135 Cfr. articolo 24°, aprile 2022 - Trasparenza dei sistemi di raccomandazione :1 I fornitori di piattaforme online che utilizzano sistemi di raccomandazione devono indicare nei loro termini e condizioni, in un linguaggio semplice e comprensibile, i parametri principali utilizzati nei loro sistemi di raccomandazione, nonché tutte le opzioni che consentono ai destinatari del servizio di modificare o influenzare tali parametri principali. 2. I parametri principali di cui al paragrafo 1 spiegano perché determinate informazioni vengono suggerite al destinatario del servizio. Essi comprendono almeno: (a) i criteri più significativi per determinare le informazioni proposte al destinatario del servizio; (b) le ragioni dell'importanza relativa di tali parametri.

136 Cfr. S. Tommasi, *Verso il Digital Services Act: la Proposta di Regolamento sul "mercato unico dei servizi digitali" del 15.12.2020*, in Persona e mercato, 1/2021, p. 215. "L'*online advertising transparency* è affidata, in prima battuta, ad alcuni obblighi che riguardano tutte le piattaforme e che sono delineati dall'art. 24. Ogni singolo destinatario del messaggio pubblicitario, infatti, deve essere in grado di identificare, in modo chiaro e non

L'informazione sui principali parametri testé ricordati, dovrebbe, nel disegno del legislatore, rendere comprensibile all'utente la logica applicata dal *RS*. Non si tratta, però, a ben vedere, di una spiegazione resa su base individuale, ma di un'informazione standardizzata da rendere *ex ante*, il cui contenuto e le cui modalità vengono precisate dalla previsione legislativa, sempre fatti salvi eventuali diritti di proprietà intellettuale e segreti industriali della piattaforma o di terzi. Valgono dunque anche rispetto alle modifiche apportate dal Parlamento europeo le medesime critiche formulate nei riguardi dell'originaria proposta legislativa: un'informazione circa i principali parametri non è in grado di accrescere il controllo dei consumatori sulla "logica" del sistema, tanto più alla luce della complessità di sistemi di intelligenza artificiale che impiegano una pluralità di criteri (collettivi e individuali, seguendo le distinzione della citata norma, cioè relativi ad un singolo o ad una categoria cui il singolo è ascritto).

Il medesimo art. 24a precisa che le suddette informazioni rientrano tre le "condizioni" praticate dalle piattaforme nei confronti dei destinatari dei propri servizi. Poiché la proposta DSA chiarisce che il lemma condizione attiene all'assetto dei rapporti tra le parti (cfr. art. 2, lett. q), deve ritenersi che un inadempimento di tale dovere rilevi anche su un simile piano (ad esempio, a titolo di responsabilità precontrattuale), con tutti i corollari in punto di *private enforcement* (espressamente contemplato dalla stessa Proposta di DSA; cfr. *ultra*).

Si prevede, inoltre, per il solo caso in cui la piattaforma online metta a disposizione una pluralità di tipi di *RS*, basati su diverse opzioni, che l'informazione debba riguardare anche le funzionalità che consentono al destinatario del servizio di determinare e modificare in ogni momento l'opzione preferita[137]. In sintesi, si impone, non già di offrire agli

ambiguo, e in tempo reale, la natura pubblicitaria delle informazioni visualizzate, la persona fisica o giuridica per conto della quale viene visualizzata la pubblicità, nonché le informazioni rilevanti sui principali parametri utilizzati per determinare il destinatario al quale viene mostrata la pubblicità". In merito occorre sottolineare che, ai fini della disciplina di cui si tratta, 'advertisement' means information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes, and displayed by an online platform on its online interface against remuneration specifically for promoting that information (cfr. Art. 2, lett. n; considerando n. 52).

[137] Cfr. articolo 24a , 3 par.: "Quando sono disponibili diverse opzioni ai sensi del paragrafo 1 per i sistemi di raccomandazione che determinano l'ordine relativo delle informazioni presentate ai destinatari del servizio, i fornitori di piattaforme online devono anche rendere direttamente e facilmente accessibile dalla sezione specifica

utenti diverse opzioni, ma soltanto di dare informazioni circa tali opzioni, ove presenti (proprio come previsto nella originaria versione dell'art. 29 Proposta DSA).

Invece, un nuovo art. 29, applicabile esclusivamente alle piattaforme online di grandi dimensioni che utilizzano sistemi di raccomandazione, richiede che venga messo a disposizione del destinatario almeno un RS non basato sulla profilazione, nonché, nell'interfaccia online del sistema, che vengano rese disponibili funzionalità per selezionare e modificare in ogni momento le opzioni preferite per ciascun RS[138].

Mentre appare giustificato mostrare un certo scetticismo circa il conferimento ai consumatori di tale ultima facoltà (per via della notevole complessità del sistema, dovuta alla molteplicità di parametri impiegati), non può che plaudirsi, invece, alla introduzione dell'obbligo di mettere a disposizione un RS che non sia basato sulla profilazione[139], giacché con esso si esprime la regola per cui si deve poter interagire nel contesto online come "consumatori qualunque" (cfr. *retro*). Lodevole appare, in particolare, la scelta, assunta dal legislatore comunitario, di prescindere dalla revoca del consenso da parte del consumatore alla profilazione (presupposto, invece, dai c.d. meccanismi di *opting-out*) e di far propria la scelta di prescrivere *by default* che il singolo non sia assoggettato a pratiche di personalizzazione.

---

dell'interfaccia online della piattaforma online in cui le informazioni vengono classificate in ordine di priorità una funzionalità che consenta al destinatario del servizio di selezionare e modificare in qualsiasi momento l'opzione preferita".

[138] Cfr. Articolo 29: "Oltre ai requisiti di cui all'articolo 24 bis, le piattaforme online di grandi dimensioni che utilizzano sistemi di raccomandazione forniscono almeno un sistema di raccomandazione non basato sulla profilazione, ai sensi dell'articolo 4, paragrafo 4, del regolamento (UE) 2016/679".

[139] Si mira a tutelare l'autodeterminazione del singolo, dando sempre la possibilità di usufruire di un RS che non sia basato sulla profilazione. Cfr. Considerando n. 62, versione DSA del gennaio 2022, secondo cui "le piattaforme online di grandi dimensioni dovrebbero lasciare che siano i destinatari a decidere se vogliono essere soggetti a sistemi di raccomandazione basati sulla profilazione e garantire che ci sia un'opzione che non si basa sulla profilazione. Inoltre, le piattaforme online dovrebbero garantire che i destinatari siano adeguatamente informati sull'uso dei sistemi di raccomandazione e che possano influenzare le informazioni presentate loro attraverso scelte attive". Nella versione approvata a giugno 2022, al tema è dedicato un considerando 52c, il quale, viceversa, enfatizza il ruolo della informazione sui principali parametri usati dai RS.

10.7.1. Segue. La prevenzione nel DSA dei rischi connessi all'impiego di RS e la introduzione di misure di trasparenza volte a favorire la supervisione da parte delle autorità di vigilanza

Alla luce degli artt. 27, par. 2°[140], e 26, par. 1, lett. b), Proposta DSA (secondo le modifiche approvate dal Parlamento europeo), le piattaforme online di grandi dimensioni che usano RS debbono compiere una valutazione dei rischi sistemici[141] che, tra l'altro, tenga conto delle conseguenze pregiudizievoli sugli interessi dei consumatori. Tuttavia, nell'ambito dei rischi di tale natura, le piattaforme sono tenute a considerare non *sic et simpliciter* qualsivoglia interesse di tali soggetti, ma soltanto quelli che abbiano attinenza con i diritti fondamentali (alla luce dell'art. 38 Carta di Nizza), come la dignità dell'individuo, il diritto alla protezione dei dati personali e alla non-discriminazione, etc.[142]. Si allude dunque al processo di 'costituzionalizzazione' di taluni

---

[140] "2. Nello svolgimento delle valutazioni dei rischi, le piattaforme online di dimensioni molto grandi *esaminano*, in particolare, *se e come* i loro sistemi di moderazione dei contenuti, *le condizioni generali, le norme della comunità, i sistemi algoritmici, i sistemi* di raccomandazione e *i sistemi* di selezione e visualizzazione della pubblicità, *nonché la raccolta, il trattamento e la profilazione dei dati di base* influenzano i rischi sistemici di cui al paragrafo 1, compresa la diffusione potenzialmente rapida e ampia di contenuti illegali e di informazioni incompatibili con le loro condizioni generali.".

Cfr., inoltre, il Considerando n. 62, si ribadisce quanto sopra: "Gli obblighi di valutazione e mitigazione dei rischi dovrebbero far scattare, caso per caso, la necessità per i fornitori di piattaforme online molto grandi e di motori di ricerca molto grandi di valutare e, se necessario, adattare la progettazione dei loro sistemi di raccomandazione, adottando misure per prevenire o ridurre al minimo i pregiudizi che portano alla discriminazione di persone in situazioni vulnerabili…. ".

[141] C. N. Griffin, *Systemically Important Platforms*, in 107 Cornell Law Review (forthcoming 2021), disponibile in https://ssrn.com/abstract=3807723; S. J. Lindsay, T. R. Samples, *On the Systemic Importance of Digital Platforms*, in *University of Pennsylvania Journal of Business Law*, vol. 25 (forthcoming 2022), p. 5 e 6 sul concetto di rischio sistemico, disponibile in https://ssrn.com/abstract=4040269. In ordine al DSA, cfr. Z. Efroni, *The Digital Services Act: risk-bases regulation of online platforms*, in *Internet Policy Review*, 16 novembre 2021, in https://policyreview.info/articles/news/digital-services-act-risk-based-regulation-online-platforms/1606.

[142] Ai sensi di tale disposizione, occorre valutare "(b)eventuali effetti negativi *concreti e prevedibili* per l'esercizio dei diritti fondamentali, *anche in materia di protezione dei consumatori, relativi* al rispetto *della dignità umana e* della vita privata e familiare, *alla protezione dei dati di carattere personale* e alla libertà di espressione e di informazione, *nonché alla libertà e al pluralismo dei media*, *al* diritto alla non discriminazione e *ai* diritti del minore, sanciti rispettivamente dagli articoli *1*, 7, *8*, 11, 21, *23*, 24 *e 38* della Carta"

interessi dei consumatori, quelli la cui lesione travalica l'ambito tradizionale del diritto dei consumi, per toccare situazioni soggettive di rango superiore, quali quelle testé ricordate. A ben vedere, è quel che si verifica in molte delle pratiche in cui vengono impiegati sistemi di raccomandazione (cfr. *retro*). Ne discende per l'interprete il delicato compito di individuare il confine superato il quale, alle discipline squisitamente consumeristiche, si sommano le tutele che si vanno illustrando (chiarendone la reciproca interazione; cfr. *ultra*).

La citata Proposta DSA fa altresì obbligo alle piattaforme di grandi dimensioni di adottare idonee misure di mitigazione di tali rischi (di cui occorre stilare un elenco, da sottoporre alle autorità di vigilanza), ivi inclusi il monitoraggio e l'adeguamento dei sistemi di raccomandazione (art. 27, par. 1, lett. ca); nonché di sottoporsi annualmente ad *auditing* indipendente (art. 28) con il fine di valutare, attraverso l'eccesso a tutti i dati necessari, l'adempimento dei suddetti obblighi.

Valutazione del rischio, misure di mitigazione ed *auditing* indipendente consistono in salvaguardie aventi il pregio di prescindere dall'iniziativa di singoli consumatori. Soprattutto, implicano per i professionisti dei doveri di protezione dai suddetti rischi, dando concretizzazione, anche in un'ottica *by design*[143], a quel principio di effettiva protezione degli interessi dei consumatori[144], che, altrimenti, nel contesto digitale resterebbe lettera morta. In quest'ottica, le misure di mitigazione testé ricordate debbono essere volte, ad esempio, a prevenire involontarie discriminazioni dovute a indesiderati sviluppi dei sistemi autonomi di apprendimento, quali i RS, nonché nel rendere comprensibili logiche ed implicazioni legate all'uso di questo ultimi, affinché siano preservate le condizioni per un'autonoma capacità decisionale dei consumatori (cfr. *retro*).

A ciò vanno aggiunte le disposizioni volte a rendere possibile l'esercizio di poteri di sorveglianza da parte di autorità pubbliche e di

[143] In merito, a poco rileva la circostanza che i professionisti che usano sistemi quali quelli in parola nell'ambito di pratiche commerciali non ne siano anche gli sviluppatori ed i fabbricanti e che, dunque, non possano incidere sulla concezione e sviluppo del sistema, in maniera tale che esso sia esente dal creare dati rischi; in ogni caso, porre doveri di individuazione dei rischi e di protezione a carico delle piattaforme di grandi dimensioni si traduce indirettamente in un incentivo nella medesima direzione anche rispetto a sviluppatori e fabbricanti dei sistemi, quando meno sulla scorta dei rapporti interni di questi ultimi con le piattaforme ste

[144] G. Vettori, *Il diritto ad un rimedio effettivo nel diritto privato europeo*, in *Juscivile*, 2017, 2, p. 133 s., p. 139.

esponenti della stessa società civile e, dunque, di penetrare quella sorta di "scatola nera", costituita dai sistemi di IA, di cui qui si tratta.

Infatti, con l'obiettivo di promuovere l'*accountability* delle piattaforme digitali di grandi dimensioni che veicolano comunicazioni commerciali[145], viene loro imposto l'obbligo di creare e mantenere repositori accessibili al pubblico attraverso le proprie interfacce online, contenenti talune informazioni minime atte a promuoverne la trasparenza (art. 30 Proposta DSA; cfr. *retro*).

Inoltre, sempre in vista del suddetto fine, le medesime piattaforme sono tenute a concedere l'accesso, da parte delle autorità di vigilanza e di ricercatori autorizzati, ai dati necessari per accertare l'osservanza delle prescrizioni imposte dallo stesso DSA, relative all'individuazione e mitigazione dei rischi rilevanti ai sensi di tale disciplina (art. 31 Proposta DSA), ivi incluse le disposizioni concernenti i sistemi di raccomandazione[146]. Proprio in relazione a questi ultimi, il DSA, nella versione dell'aprile 2022, include una specifica previsione per la quale "Ai fini del paragrafo 1, i fornitori di piattaforme online di grandi dimensioni, su richiesta del Coordinatore dei servizi digitali o della Commissione, spiegano la progettazione, il funzionamento logico e la sperimentazione dei loro sistemi algoritmici, compresi i sistemi di raccomandazione (art. 31, par. 1b)".

Quest'ultima previsione riveste notevole importanza, sol che si consideri che, senza accesso ai dati, la ricerca e la supervisione delle pubbliche istituzioni non appaiono fattibili, innanzitutto, per via del difetto di conoscenza dei fenomeni da governare e della loro reale entità[147].

Al rafforzamento della supervisione ad opera di autorità pubbliche mirano anche alcune modifiche alla Proposta DSA, introdotte dal Parlamento europeo, consistenti nella espressa previsione del ricorso a rimedi di stampo privatistico e, in particolare, al risarcimento del danno

---

[145] C. Camardi, *Contratti digitali e mercati delle piattaforme. Un promemoria per il civilista*, in *Juscivile*, 2021/4, p. 870 ss., cfr. p. 912.

[146] In merito, il Considerando n. 64 precisa che" il Coordinatore dei Servizi Digitali di stabilimento o la Commissione possono richiedere l'accesso o la segnalazione di dati e algoritmi specifici. Tale requisito può comprendere, ad esempio, i dati necessari per valutare i rischi ed i possibili danni causati dai sistemi della piattaforma, i dati sull'accuratezza, il funzionamento e il test dei sistemi algoritmici di moderazione dei contenuti, dei sistemi di raccomandazione o dei sistemi pubblicitari".

[147] Cfr. M. Perel, N. Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 Fla. L. Rev. 181 (2017)

ai sensi delle normative europee e nazionali, in caso di pregiudizi causati dalla violazione degli obblighi imposti dal regolamento ai prestatori di servizi di intermediazione (art. 43 a)[148]. Sgomberando il campo da qualsivoglia dubbio in merito[149], viene dunque chiarito che i destinatari dei suddetti servizi, oltre ad essere legittimati a proporre reclami all'autorità di vigilanza, possono invocare i rimedi di *private enforcement* previsti dalle pertinenti normative, ivi inclusi i rimedi attinenti alla disciplina del contratto.

10.8. Conclusioni

Si assiste ad una 'nuova stagione regolatoria', mirante a disciplinare le attività dei molteplici attori dell'economia digitale[150], la complessità del cui operato chiama in causa diverse fonti.

All'interno di tale quadro permane decisivo il ruolo della disciplina sulle pratiche commerciali scorrette[151], di recente oggetto di riforma sotto il profilo delle sanzioni irrogabili (e della relativa efficacia deterrente), nonché dei meccanismi di private *enforcement*[152].

---

[148] Ai sensi di tale articolo, "Fatto salvo l'articolo 5, i destinatari del servizio hanno il diritto di chiedere un risarcimento, conformemente al pertinente diritto unionale e nazionale, ai prestatori di servizi intermediari qualora abbiano subito danni o perdite diretti a seguito di una violazione degli obblighi stabiliti dal presente regolamento da parte dei prestatori di servizi intermediari".

[149] Cfr. N. Helberger, H.W. Micklitz, P. Rott, *Eu Consumer Protection 2.0. The Regulatory Gap: Consumer Protection in the Digital Economy*, studio commissionato da Beuc, The European Consumer Protection, dicembre 2021, p. 16.

[150] G. Alpa, *La legge sui servizi digitali e la legge sui mercati digitali*, cit., p. 1.

[151] Secondo Linee guida Commissione UE 2021, par. 4.2.7., "Le pratiche di personalizzazione basate sui dati nel rapporto tra impresa e consumatore comprendono la personalizza zione della pubblicità, sistemi di raccomandazione, la tariffazione, la classificazione delle offerte nei risultati di ricerca, ecc. Le norme e i divieti di principio contenuti nella direttiva possono essere utilizzati per contrastare le pratiche commerciali sleali delle imprese nei confronti dei consumatori oltre ad altri strumenti del quadro giuridico dell'UE, come la direttiva relativa alla vita privata e alle comunicazioni elettroniche, il GDPR oppure la legislazione settoriale applicabile alle piattaforme online".

[152] Ivi inclusi quelli di natura collettiva di cui alla direttiva 2020/1828/UE del Parlamento e del Consiglio del 25 novembre 2020 relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (L 409/1), la quale si ripropone di governare i due fenomeni della globalizzazione e della

Quest'ultima è innanzitutto strumento per regolare il mercato e proteggere l'autodeterminazione dei consumatori, ed appare dotata di grande duttilità giacché si presta a tutelare situazioni soggettive, tanto individuali che collettive e si applica anche laddove la pratica commerciale sia diretta ad un singolo[153] anziché ad una platea di consumatori[154].

Nella direttiva omnibus troviamo poche condotte tipizzate, consistenti in, o suscettibili di dare vita a pratiche ingannevoli. Esse non esauriscono la gamma dei comportamenti, implicanti utilizzo di RS, qualificabili come sleali (cfr. *retro*).

Ed infatti le pratiche che impiegano RS, come visto, implicano rischi 'nuovi', per i quali la sola informazione non giova, incidenti non solamente su interessi di natura economica, ma su autodeterminazione, autonomia di scelta, accesso a beni e servizi, parità di trattamento e, in ultima istanza, sulla stessa dignità della persona[155].

Gli orientamenti della Commissione UE sull'interpretazione e sull'applicazione della direttiva 2005/29/CE enunciano con nettezza il ruolo che tale ultima direttiva riveste nella regolazione delle suddette pratiche, unitamente ad altri plessi normativi, con essa complementari, quali il GDPR, la regolamentazione sulla tutela della vita privata nelle comunicazioni elettroniche e la «legislazione settoriale applicabile alle

---

digitalizzazione offrendo tutele improntate al principio di effettività e concernenti gli interessi collettivi (cfr. Considerando 1 e 7).

[153] Il singolo consumatore il cui interesse sia leso dalla pratica può invocare una tutela individuale (art. 11° dir. 29/95/CEE, come modificata dalla direttiva di modernizzazione).

[154] N. Helberger, O. Lynskey, H.W. Micklitz, P. Rott, *EU Consumer Protection 2.0. Structural asymmetries in digital consumer markets*, A joint report from research conducted under the EUCP2.0 project, BEUC, The European Consumer Organization, marzo 2021, p. 59: "Commercial practices are by nature a form of standardised marketing strategy. That is why the enforcement of possible infringements is put into the hands of consumer agencies or consumer organisations, or both. The CJEU has held that even commercial practices that target one single consumer come under the scope of application (CJEU C-388/13 UPC Magyarország ECLI:EU:C:2015:225), and the Omnibus Directive has granted consumers the individual right to pursue. This means that the consumer who is targeted individually may enforce their rights individually and is no longer dependent on collective enforcement, whether private or public".

[155] A riprova di ciò, il considerando 52 DSA, versione di gennaio 2022, in merito ai c.d. "nuovi modelli pubblicitari", basati sulla personalizzazione, constata come essi abbiano "…generato profondi cambiamenti nel modo in cui le informazioni sono presentate e hanno creato nuovi modelli di raccolta dei dati personali e modelli aziendali che potrebbero incidere sulla vita privata, sull'autonomia personale, …, nonché agevolare la manipolazione e la discriminazione».

piattaforme online»[156]. Evidente l'allusione alla dottrina della 'protezione multilivello' (o, meglio, all'ordine giuridico integrato dell'economia digitale), oramai data per acquisita nelle decisioni delle corti, nazionali e non, ed estesa alle normative di settore.

Nell'ottica di sfruttare la massima capacità espansiva della disciplina in tema di pratiche commerciali sleali, assume speciale rilievo la clausola generale della diligenza professionale, la quale riassume l'insieme dei doveri di cura e attenzione incombenti sul professionista, desumibili tenendo conto della natura della pratica, del settore e tipo di prodotto o servizio, nonché del consumatore medio destinatario della stessa.

Rispetto alle interazioni con il consumatore nei mercati digitali, simili doveri implicano che il professionista si astenga dal (e si adoperi per non) trarre vantaggio dalla condizione di asimmetria, in cui il consumatore medio versa, la quale non può essere colmata attraverso la sola trasmissione di informazioni.

Per le pratiche che comportano uso di RS, vanno tenuti in conto i «valori normativi che si applicano nell'ambito specifico dell'attività commerciale»[157]. Rilevanza in merito assumono, dunque, innanzitutto, i doveri di protezione inerenti al rapporto contrattuale che si instaura (anche in via implicita) tra il fornitore del servizio e il destinatario. Per i servizi digitali oggetto della Proposta di DSA, inoltre, simili doveri costituiscono il corollario di una disciplina tesa a responsabilizzare il gestore di piattaforme di grandi dimensioni: quest'ultimo, in base ai risultati della valutazione dei rischi sistemici e dell'auditing indipendente cui deve sottoporsi annualmente (cfr. *retro*), individua e adotta adeguate misure di mitigazione di tali rischi, ivi incluse le misure atte a gestire quei rischi involontariamente discendenti da vizi del sistema di RS sviluppato da terzi (di discriminazione, manipolazione etc.).

Anche al requisito costituito dalla idoneità della pratica a distorcere il comportamento economico del consumatore medio occorre dare una estensione suscettibile di comprendere le pratiche di personalizzazione che impiegano RS.

E' noto che tale nozione tende ad essere interpretata estensivamente (ogni decisione direttamente collegata con decisione se acquistare o meno un prodotto, ad es., entrare in un negozio o visitare un sito Internet) e può comprendere comportamenti dei consumatori

[156] Linee guida Commissione UE 2021, loc. ult. cit.
[157] Cfr. Linee guida Commissione UE – 2021, par. 2.7.

congruenti con il modello economico prescelto dal professionista. Allo stesso modo, nel valutare la capacità della condotta del professionista a menomare la libertà decisionale del consumatore medio, occorre tenere conto, tra gli altri elementi, del tipo di destinatario della stessa. Le pratiche di personalizzazione, per definizione, isolano un gruppo o un individuo, sulla base di caratteristiche, vulnerabilità, etc. (in sintesi, alla luce della sua suscettibilità rispetto alla pratica, ben nota al professionista che la mette in atto). E la disciplina in questione si presenta malleabile abbastanza da consentire di avere riguardo proprio all'individuo medio di tale gruppo o addirittura al singolo preso di mira[158]. A tale soggetto vanno parametrate le tutele legali, piuttosto che al modello astratto del consumatore informato e razionale, "arbitro del mercato"[159].

[158] Così Linee guida Commissione UE – 2021, par. 3.7., per le quali anche il parametro del consumatore medio o vulnerabile può essere valutato alla luce del gruppo considerato e, se la pratica è altamente personalizzata, persino formulato dal punto di vista di una singola persona che è stata oggetto di specifica personalizzazione. Cfr. per i riferimenti dottrinali in merito già N. Helberger, B.F. Zuiderveen, A. Reyna, *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, cit., p. 1458.

[159] Cfr. già N. Irti, *Letture bettiane sul negozio giuridico*, Milano, 1991, secondo il quale, nel contesto "spersonalizzante" della produzione di massa, non c'è spazio per l'autonomia negoziale, nell'accezione che ci restituisce il codice civile (art. 1322), e residua soltanto la scelta del singolo, che spetta al diritto proteggere. Seguendo questa linea di pensiero e riportandola al presente, dinanzi a certi fenomeni dell'economia digitale, il diritto deve ergersi a difesa della libertà del singolo, più ancora che preoccuparsi dei di lui interessi economici.

11. Linguaggi di programmazione e responsabilità

Salvatore Orlando (Università di Roma La Sapienza)

1.1. Introduzione

Comincerò citando una frase del filosofo Emil Cioran: "*Non si abita un Paese, si abita una lingua. Una patria è questo, e nient'altro*" ([1]).

Per i motivi che proverò a dire, ritengo che, nei discorsi che ci riguardano, la forza di suggestione di questa frase abbia una capacità di agire in almeno due direzioni.

I discorsi che ci riguardano sono i discorsi sulle norme e sui progetti di norme intesi a costituire la c.d. *governance* delle tecnologie digitali ed in particolare dei sistemi *software* della c.d. intelligenza artificiale. Si tratta non soltanto delle regole di responsabilità ([2]), ma anche di quelle

---

*Questo articolo costituisce la traccia scritta della relazione dallo stesso titolo tenuta dall'A. alla *Summer School* '*La responsabilità civile nell'era digitale*' del Dipartimento di Giurisprudenza dell'Università di Foggia dal 6 al 10 settembre 2021.

[1] E. CIORAN, *Confessioni e anatemi*, trad. it di M. Bortolotto, Adelphi, Milano, 2^ ed. 2007, p. 23.

[2] Per quanto riguarda i progetti e gli studî può qui citarsi la *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL))* (su cui v. S. GARREFFA, *La risoluzione del Parlamento europeo del 20 ottobre 2020 sul regime di responsabilità civile per l'intelligenza artificiale*, nella rubrica '*Diritto e nuove tecnologie*', in *Persona e mercato*, 2020, p. 502 ss.: http://www.personaemercato.it/wp-content/uploads/2020/11/Osservatorio.pdf); nonché lo studio di Andrea Bertolini sullo stesso argomento (https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf), pubblicato dal Parlamento europeo nel luglio dello stesso anno (su cui v. E. W. DI MAURO, *Lo studio del luglio 2020 su "Intelligenza Artificiale e responsabilità civile" commissionato dalla Commissione JURI del Parlamento europeo*, nella rubrica '*Diritto e nuove tecnologie*', in *Persona e mercato*, 2020, p. 324 ss.: http://www.personaemercato.it/wp-content/uploads/2020/09/Osservatorio-14.9.2020.pdf). Cfr. anche, per un'impostazione che può dirsi ormai largamente superata, la precedente *Risoluzione del Parlamento europeo del 16 febbraio* 2017 recante

che hanno una rilevanza indiretta sul tema della responsabilità, come i progetti di discipline che si propongono di governare i requisiti di progettazione nonché i limiti, le modalità e i divieti di commercializzazione e di utilizzo dei sistemi *software* di intelligenza artificiale avuto riguardo alla tutela dei diritti fondamentali e al quadro delle altre discipline generali e di settore dell'UE ([3]).

La prima direzione - forse la più evidente - è quella tracciata dall'ambito di applicazione delle norme di cui si discute: è il tema dello scarto oggettivo (quanto meno nella sua dimensione formale) ravvisabile tra l'*universalità* dei linguaggi *software* - che impartiscono *ordini ai dispositivi tecnologici* - e la *territorialità* delle norme giuridiche - che impartiscono *ordini sui dispositivi tecnologici* ossia che prevedono specifici doveri di comportamento per i costruttori,

raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

[3] Si fa riferimento, naturalmente, in primo luogo, alla proposta di regolamento della Commissione europea del 21 aprile 2021 (COM(2021) 206 *final*) nota come proposta dell'*Artificial Intelligence Act* o AIA dal suo acronimo: *Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione* (su cui v. S. ORLANDO, *Verso l' Artificial Intelligence Act: la Proposta di Regolamento del 21.04.2021 su regole armonizzate in materia di intelligenza artificiale*, nella Rubrica *Diritto e nuove tecnologie*, in *Persona e mercato*, 2021, p. 416 ss: http://www.personaemercato.it/wp-content/uploads/2021/03/Osservatorio-1.pdf). Si fa inoltre riferimento a tutti i precedenti documenti del Parlamento europeo, del Consiglio e della Commissione. In particolare, quanto al Parlamento europeo, oltre alla sopra citata *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)),* possono ricordarsi le due coeve risoluzioni sull'etica e il *copyright* (*European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL)*; e la *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI)*). Per quanto riguarda il Consiglio europeo, si ricorda: lo *European Council meeting (19 October 2017) – Conclusion EUCO 14/17*, 2017, p. 8; l' *Artificial intelligence b) Conclusions on the coordinated plan on artificial intelligence-Adoption 6177/19, 2019*; lo *Special meeting of the European Council (1 and 2 October 2020) – Conclusions, EUCO 13/20, 2020,* p. 6; le *Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*, 11481/20, 2020. Quanto alla Commissione, prima della citata proposta dell'AIA, si ricorda il libro bianco sulla IA del febbraio 2020, ossia lo *European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust,* COM(2020) 65 final, 2020; il *Digital Education Action Plan 2021-2027: Resetting education and training for the digital age, which foresees the development of ethical guidelines in AI and Data usage in education – Commission Communication* COM(2020) 624 final.

sviluppatori, distributori, venditori ed utilizzatori dei sistemi di intelligenza artificiale e dei loro *output*.

Se questo tema – nei suoi elementi problematici - sembra sufficientemente chiaro, ve ne è un altro, meno evidente, ed anzi decisamente in ombra. Ed è di quest'altro tema che proveremmo a parlarvi oggi.

Riteniamo infatti che quella frase di Emil Cioran ("*Non si abita un Paese, si abita una lingua. Una patria è questo, e nient'altro*") abbia una capacità di suggerire linee di riflessione lungo la strada interna di comprensione dell'oggetto stesso delle normative che ci interessano. Come proveremo a dire, proponiamo un approfondimento in *medias res* sulle strutture di creazione e di governo *tecnico* delle tecnologie digitali, ed in particolare una riflessione sul linguaggio informatico. Una riflessione che ci sembra idonea a evidenziare anche una pluralità di elementi rilevanti ai fini della impostazione dei più generali problemi di responsabilità giuridica.

Il punto di partenza della nostra proposta consiste nell'osservazione di quella che ci sembra una vera e propria assenza nel dibattito *giuridico* sui temi legati all'intelligenza artificiale: viene comunemente aggettivata come 'artificiale' l'intelligenza, o anche la nuova realtà creata dalle tecnologie digitali, ma si manca comunemente di orientare la riflessione sull'artificialità dei linguaggi - a partire dai linguaggi di programmazione utilizzati per scrivere quei *software*, ossia i programmi per elaboratori - che creano e governano questi fenomeni. E, conseguentemente, si manca di riflettere sugli specifici problemi che comportano l'adozione e l'uso di questi linguaggi.

11.2. Anatomia ed etimologia

Linguaggio deriva da lingua, e di lingua parlava in quel modo il filosofo, come ricordavamo. Da qui conviene dunque cominciare.

Cominciamo letteralmente con l'osservare che 'lingua' - nel significato rimandato dagli usi che identificano uno specifico codice, es. la lingua italiana, francese etc., deriva dall'organo anatomico della cavità orale avente lo stesso nome.

Tale organo è implicato in un fenomeno - l'atto del parlare – che, a ben vedere, riguarda solo la lingua parlata e non anche la c.d. 'lingua' scritta, tanto meno gli altri linguaggi diversi dal linguaggio verbale, ad es. la 'lingua' dei segni dei non udenti e gli altri linguaggi diversi dal

c.d. linguaggio naturale: il linguaggio informatico, il linguaggio musicale etc.

L'etimologia e l'impiego della parola 'lingua' per tutti questi altri usi estranei all'atto del parlare si spiega naturalmente con l'affermazione originaria e fondativa della comunicazione orale («in principio era il verbo») e dunque con il primato storico dei codici della lingua parlata sui codici degli altri linguaggi.

È un primato che sembra non esistere più.

D'altronde, la stessa parola 'parola' rimanda a quel fenomeno fisico – il parlare – non necessariamente implicato dal suo significato generale per il quale con 'parola' si intende qualsiasi unità isolabile di un discorso, anche scritto, e lo stesso potrebbe dirsi a proposito del sostantivo 'discorso', che viene da 'discorrere' etc.

11.3. I linguaggi di programmazione

Venendo al linguaggio informatico, la sua rilevanza è evidente; ciò in quanto, come si sa, tutte le applicazioni e i sistemi della tecnologia digitale, sui quali ci interroghiamo oggi, sono governati da *software*, da programmi scritti in linguaggio informatico.

Proviamo quindi ad entrare in questo linguaggio artificiale, non come programmatori - si intende - ma con la finalità di ricercare e mettere in luce i punti di rilevanza giuridica del fenomeno. Del quale è sufficiente conoscere alcune nozioni elementari. Sufficiente, ma anche necessario.

Quando si parla di linguaggio informatico, ci si può riferire generalmente ai linguaggi di programmazione utilizzati dai programmatori (esseri umani) per scrivere programmi per elaboratori (*software*), ossia a linguaggi di programmazione di c.d. alto livello, oppure a linguaggi di programmazione c.d. di basso livello, ossia a lingue del linguaggio '*assembly*' o del 'linguaggio macchina'.

Come noto, il linguaggio di programmazione c.d. di alto livello utilizzato dai programmatori è un linguaggio che si esprime attraverso parole, numeri, simboli di puntuazione e altri simboli grafici. Si manifesta in una pluralità (centinaia se non migliaia) di lingue e perfino di "dialetti" variamente diversificati in termini sintattici e semantici ed è preordinato all'elaborazione di istruzioni da tradurre in definitiva nel linguaggio macchina che serve a trasmettere le medesime istruzioni agli elaboratori per la loro esecuzione.

Come detto, si distingue il linguaggio di programmazione c.d. di alto livello (che è normalmente il primo linguaggio di programmazione utilizzato dai programmatori) e linguaggio di programmazione c.d. di basso livello ovvero le lingue del linguaggio *assembly* e del linguaggio macchina.

L'*assembly* è un linguaggio intermedio tra quello di alto livello e il linguaggio macchina. La sintassi e la semantica dell'*assembly* si avvicinano di più al linguaggio macchina e per questo motivo è più difficile da utilizzare e da comprendere anche da parte dei programmatori.

Il linguaggio macchina è composto di bit convenzionalmente rappresentati con i numeri 0 e 1, c.d. alfabeto o codice binario di bit, ovvero anche - per ridurne la lunghezza, in codice esadecimale: numeri da 0 a 9 e lettere da A a F.

Anche il linguaggio macchina si manifesta in una pluralità di 'lingue' o codici o linguaggi, diversificati in funzione delle caratteristiche degli elaboratori (architettura hardware).

11.4. La molteplicità dei software implicati nella scrittura ed esecuzione di un programma software

Il passaggio dal linguaggio di programmazione di c.d alto livello al linguaggio macchina può avvenire in diverso modo, ma sempre avviene attraverso altri *software* che "traducono" un codice in un altro codice oppure – come diremo meglio più avanti - lo "interpretano" ed "eseguono" direttamente: *software* c.d. compilatori (*compilers*), o c.d. assemblatori (*assemblers*: quando il programma in questione è in una lingua del linguaggio *assembly*) che traducono il programma da un linguaggio ad un altro producendo un *file* in linguaggio macchina da eseguire oppure *software* c.d. interpreti (*intepreters*) che traducono e contestualmente eseguono direttamente il programma scritto in linguaggio di c.d. alto livello ("codice sorgente") senza predisporre un *file* in linguaggio macchina ("codice oggetto"); o ancora procedure ibride a metà strada (il linguaggio di programmazione può passare attraverso una fase di c.d. precompilazione in *bytecode*: è il caso, ad es., del linguaggio Python).

Quale che sia la modalità, ai nostri fini è importante osservare che c'è sempre l'intervento di uno o più *software* per assicurare il passaggio - ossia la trasmissione - all'elaboratore delle istruzioni previste dai programmatori in linguaggio di programmazione: sia che si tratti di

"compilazione", sia che si tratti di "interpretazione" o "esecuzione" (come dicono i programmatori) e quindi c'è sempre una traduzione (dal linguaggio di programmazione al linguaggio macchina): quello che può mancare è la creazione di un *file* come prodotto della traduzione.

Naturalmente questi *software* possono non funzionare bene, e in gergo tecnico questi malfunzionamenti si chiamano *bugs* ed esistono *software* che servono a loro volta per scoprire e rimuovere i *bugs*: i *debuggers* (e tali *software*, a loro volta, in quanto tali, possono funzionare più o meno bene).

Ma prima ancora che nella predetta fase di trasmissione del programma già scritto, c'è un ampio impiego di *software* nella stessa fase della scrittura del programma: *software* di editing, *software* c.d. IDE (*Integrated Developement Environment*), più o meno calibrati e specializzati in relazione alla specifica lingua del linguaggio di programmazione prescelta, *software* c.d. di base che servono per la generalità dei programmi etc.

Infine, come noto, esistono i *software* dei sistemi operativi che costituiscono per così dire l'interfaccia tra l'*hardware* e il *software* applicativo. Quindi vedete quanti programmi *software* intervengono *a latere* e strumentalmente alla scrittura e alla esecuzione di un *software* applicativo, ossia del *software* di cui abbiamo esperienza – come *users* - per determinate applicazioni.

Naturalmente anche tutti questi *software* sono stati a loro volta previamente scritti con linguaggi di programmazione.

11.5. "Se → allora"

Come risaputo, le istruzioni impartite ad un elaboratore attraverso un programma per elaboratore sono tutte riducibili allo schema logico se → allora: il programma – seppure scritto attraverso lingue di programmazione che possono utilizzare le più diversificate sintassi e i più diversi stili compositivi suddivisibili in c.d. paradigmi di programmazione (programmi cc.dd. imperativi, funzionali, dichiarativi o logici etc.), che a loro volta conoscono subdistinzioni, prevede sempre in essenza certe condizioni, soddisfatte le quali si chiede all'elaboratore di compiere una o più operazioni.

In questo modo viene creato e affidato agli elaboratori (*hardware*) qualunque istruzione di qualunque programma per elaboratore (*software*) quale che ne sia il contenuto e la funzione.

Nel linguaggio corrente, il programma per elaboratore viene anche chiamato *code*, ossia ('codice'). Il programma scritto in linguaggio di programmazione viene chiamato 'codice sorgente', mentre quello scritto in linguaggio macchina, che viene eseguito dal computer, viene chiamato 'codice macchina' o anche 'codice oggetto'.

11.6. Gli adattamenti e le traduzioni delle istruzioni dal linguaggio naturale al linguaggio macchina

In prima approssimazione, possiamo dire che le istruzioni che vengono impartite all'elaboratore sono il prodotto di una serie di adattamenti e traduzioni che originano dal linguaggio naturale per essere espresse infine in linguaggio macchina.

Ed invero, ogni *software* è tipicamente pensato per soddisfare determinati requisiti, che vengono originariamente (e tipicamente) concepiti ed espressi in linguaggio naturale, e dovranno poi essere trasfusi e in sequenza tradotti in uno o più linguaggi di programmazione, come sopra visto, fino alla traduzione finale in linguaggio macchina.

Mentre la prima traduzione (quella dal linguaggio naturale al linguaggio di programmazione) - che in realtà è definibile più propriamente come un adattamento, per i motivi che proverò a spiegare meglio *infra* - è operata oggi ancora prevalentemente da uomini, i "programmatori" - ma approfondiremo tra breve anche questo tema-, l'ulteriore o le ulteriori traduzioni sono operate dagli elaboratori che lavorano a loro volta eseguendo automaticamente apposite istruzioni contenute in appositi programmi per elaboratore (ossia altri *software*) che servono proprio a questa funzione.

Seppure normalmente i programmatori scrivono il codice sorgente in una lingua di linguaggio di programmazione di alto livello, in rari casi possono farlo – quanto meno limitatamente ad alcune parti del codice - in una lingua del linguaggio *assembly* di basso livello (in passato era questo il linguaggio utilizzato dai programmatori per i primordiali videogiochi).

Ad ogni modo, come detto, anche il linguaggio di programmazione di basso livello *assembly* deve essere tradotto in linguaggio macchina, e questa traduzione avviene attraverso un *software* c.d. *assembler*.

In alcuni casi, infine, come già osservato, si dice che il linguaggio di programmazione viene direttamente eseguito dal computer. In realtà, anche in questi casi vi è pur sempre una traduzione (in linguaggio macchina), solo che la traduzione è contestuale all'esecuzione ed è fatta di volta in volta (ossia allorquando il programma deve essere eseguito), con la vera differenza che in questi casi non viene prodotto un *file* in linguaggio macchina. In gergo informatico si parla in questi casi di "interpretazione" per distinguerla dalla "compilazione", perché quest'ultimo sostantivo esprime proprio il risultato della compilazione consistente nella creazione di un 'oggetto', ossia il *file* in linguaggio macchina che contiene un programma o codice (il 'codice macchina' o 'codice oggetto') che viene eseguito.

Quando vengono utilizzati due livelli di linguaggio di programmazione prima di passare alla traduzione nel linguaggio macchina, le traduzioni sono tre. In particolare, le istruzioni concepite ed espresse nel linguaggio naturale vengono dapprima versate dai programmatori in un primo linguaggio di programmazione c.d. di alto livello (prima "traduzione" o meglio "adattamento": l'adattamento in un linguaggio di programmazione dei requisiti che ci si attende dal *software*, normalmente concepiti ed espressi in linguaggio naturale), successivamente si ha una traduzione del programma per elaboratore espresso in questo linguaggio (codice sorgente) in una seconda lingua di linguaggio di programmazione di c.d. basso livello, l'*assembly* (seconda traduzione), ed infine si ha una traduzione di questo secondo codice espresso in linguaggio *assembly* in linguaggio macchina (terza traduzione).

11.7. Le perdite e le trasformazioni dal linguaggio naturale al linguaggio di programmazione

Come si potrà ora ben intuire, la prima traduzione (dal linguaggio naturale al primo linguaggio di programmazione) è nei fatti il frutto, prima che di una traduzione, di un *adattamento*: i programmatori cercheranno di rendere al meglio in una specifica lingua di un linguaggio di programmazione quanto originariamente concepito ed espresso (nella maggior parte dei casi: da altri, come diremo tra breve) in una specifica lingua del linguaggio c.d. naturale sotto forma di requisiti: *i requisiti che il programma software dovrà contenere*.

I programmatori dovranno dunque innanzitutto comprendere senza riserve (interpretandoli) i requisiti normalmente espressi in una lingua del linguaggio naturale, e, in secondo luogo ridurli ad una serie di istruzioni rispondenti ineluttabilmente alla logica del se → allora; per applicarvi – infine – la sintassi, lo stile e la semantica proprie della specifica lingua di programmazione prescelta (tra le tante esistenti).

Nel far ciò, ci rendiamo allora conto che il programmatore dovrà *scartare* qualsiasi elemento che *secondo il suo giudizio* sia irriducibile alla predetta logica (se → allora). Allo stesso modo, il programmatore dovrà *eliminare e non includere* nel programma per elaboratore qualsiasi elemento che *secondo il suo giudizio* comporti ambiguità circa l'identificazione delle circostanze da soddisfare come condizioni ("se") o delle operazioni richieste al soddisfacimento delle medesime condizioni ("allora") o circa la necessaria consequenzialità tra le une e le altre ("→").

Come anche si potrà facilmente intuire, quest'opera di adattamento è interamente affidata a *interpretazioni e giudizi di vario tipo*, e dunque può ben dar luogo ad *esiti opinabili*, ad *errori* così come, eventualmente (non lo si può escludere *a priori*) a *distorsioni volontarie*: sono evidentemente tutte figure di ipotesi che hanno addentellati ben precisi con le *categorie* e le *teorie* giuridiche della *responsabilità*.

Ciò sta a significare che - consistendo la matrice del fenomeno di adattamento in parola di interpretazioni e giudizi di vario tipo - possono ben verificarsi *ingiustificate* perdite o trasformazioni in questo processo di adattamento.

Precisamente, può verificarsi sia un'*ingiustificata* esclusione dal programma per elaboratore di alcune istruzioni implicitamente o esplicitamente contenute tra i requisiti espressi in linguaggio naturale (in quanto, ad esempio, alcune istruzioni non sono riconosciute come tali dal programmatore o sono da egli ritenute irriducibili alla logica del se → allora, oppure in quanto il programmatore, pur riconoscendo che un pezzo di testo in linguaggio naturale contiene un'istruzione riducibile alla logica del se → allora, ritenga nondimeno che uno o più degli elementi di tale istruzione sia troppo ambiguo e non sia di conseguenza possibile – secondo il suo giudizio – procedere con sufficiente certezza alla sua individuazione) sia, naturalmente, una loro *inesatta* traduzione in linguaggio di programmazione per un *colpevole* fraintendimento o per una *volontaria* deviazione dal significato

testualmente riconoscibile o comunque conosciuto dal programmatore e/o riconoscibile sulla base di elementi extra-testuali.

Qua dobbiamo ora aggiungere che - abbastanza evidentemente – il tasso di difficoltà e di perizia insito in questo lavoro di adattamento – sarà tanto più elevato quanto più il linguaggio utilizzato per definire i requisiti che deve avere il *software* sarà *tecnicamente connotato* in relazione alle funzioni e all'ambiente nel quale il *software* è chiamato a operare - es. linguaggio medico, giuridico ([4]), etc. -, perché, in questo caso, ai programmatori verranno richiesto conoscenze specifiche, ossia di essere essi stessi sufficientemente competenti per comprendere appieno il linguaggio tecnico impiegato nel testo della lingua naturale che essi devono tradurre per comprendere i requisiti che deve avere il *software*, o di avere o fruire dei mezzi di un'organizzazione che abbia sufficienti risorse per assumere, gestire ed assimilare una consulenza che sia a sua volta qualificata in modo sufficiente a colmare pienamente la lacuna di conoscenza del programmatore per i fini dell'interpretazione del testo e della sua traduzione nella lingua di programmazione prescelta.

11.8. Il problema dell'ambiguità del linguaggio naturale e l'ingegnerizzazione dei requisiti del *software* (*Software Requirements Engineering*)

Tutti i temi di cui abbiamo parlato sino ad ora relativamente all'interpretazione dei requisiti che devono avere i programmi *software*, e alle difficoltà che incontrano i programmatori per comprendere appieno tali requisiti espressi in lingue del linguaggio naturale e per trasfonderli nella lingua e nella logica del linguaggio di programmazione, non sono ancora stati indagati dalla scienza giuridica con la necessaria attenzione, benché abbiano un'evidente e plurima rilevanza sul piano delle conseguenze giuridiche, a partire dalle ricadute in materia di responsabilità.

---

[4] A. SLEIMI, N. SANNIER, M. SABETZADEH, L. BRIAND, M. CECI, J. DANN, *An automated framework for the extraction of semantic legalmetadata from legal texts*, in *Empirical Software Engineering*, 2021, (26:43), accessibile su https://doi.org/10.1007/s10664-020-09933-5; E. CICCONI, *Linguaggio giuridico e intelligenza artificiale*, in *Diritto e intelligenza artificiale*, a cura di G. Alpa, Pisa, 2020, p. 59 ss.

Questi temi sono invece tutti conosciuti e affrontati da anni con metodo scientifico dai teorici e dai pratici della *Computer Science*, che gli hanno riconosciuto la dignità di una specifica disciplina con un suo proprio nome: '*Software Requirements Engineering*' che studia proprio le tecniche per rendere efficiente la c.d. elicitazione (*elicitation* in inglese), ossia la ricerca di tutti i requisiti che devono ritenersi necessari e doverosi per il *software*: *anche al di là di quelli richiesti dai committenti*. In questo contesto, una specifica attenzione è dedicata al problema della c.d. *ambiguità del linguaggio naturale*.

Allo stesso modo, e per le stesse finalità, la scienza informatica è avvertita del problema delle specifiche competenze ed esigenze richieste ai fini della programmazione in considerazione delle particolari esigenze dell'ambiente in cui il *software* è chiamato ad operare (*domain* in inglese: per significare un'area di conoscenza o di attività) Es. *software* medicale per un determinato ospedale o per determinata una rete di ospedali; e viene dunque affrontata all'interno di una disciplina di ingegneria della scienza informatica chiamata '*Domain Software Engineering*'.

In questo contesto, da decenni i programmatori studiano tecniche, come dicevo, per ovviare al problema dell'intrinseca ambiguità del linguaggio naturale. È diffuso l'impiego di procedure di raccolta manuale o automatizzata delle informazioni che valgono come espressive dei requisiti del *software* attraverso modelli che fanno impiego del c.d. *linguaggio naturale controllato* o *semplificato*, ossia sistemi di scrittura e comunicazione che hanno una semantica e una sintassi semplificate ed anche una struttura grafica elementare (es. *templates*) al dichiarato fine di ridurre al massimo le possibilità di polisemia, di incertezza e di ambiguità del linguaggio naturale (e si ricorderà che l'eliminazione delle ambiguità – perseguita con l'eliminazione progressiva di parole - era uno dei dichiarati fini del *New Speak* del quale scriveva George Orwell nel suo romanzo '1984').

Esiste addirittura da dieci anni uno *standard* ISO, per questo. Si tratta dello standard ISO 29148, di cui ci sono due edizioni, la prima del 2011 la seconda del 2018: "*Systems and software engineering —Life cycle processes — Requirements engineering*"

L'ISO 29148 così come la letteratura scientifica in materia definisce l'obiettivo del *Software Requirements Engineering* la *comprensione e la definizione delle esigenze di tutti gli stakeholders*; e offre la seguente definizione di *stakeholder*:

"(3.1.28) *individual or organization having a right, share, claim or interest in a system or in its possession of characteristics that meet their needs and expectations. Stakeholders include, but are not limited to:*

end users,
end user organizations,
supporters,
developers,
producers,
trainers,
maintainers,
disposers,
acquirers,
customers,
operators,
supplier organizations,
accreditors and
regulatory bodies".

Ciò sta a significare che, secondo la migliore prassi della scienza informatica, allorquando i programmatori devono scrivere un programma per elaboratore, essi devono tener conto di una *pluralità di requisiti*, e non soltanto, come si potrebbe immaginare, di quelli insiti nelle richieste dei propri committenti. La scienza informatica raccomanda di prendere in considerazione le necessità e anche i veri e propri doveri (vincoli giuridici) come espressi dalla nutrita platea di *stakeholders* sopra ricordata.

Non possiamo qui entrare nel dettaglio delle tecniche delle procedure previste da questo standard ISO se non per sottolineare una volta di più la consapevolezza che tale *standard* esprime su due punti rilevanti anche per il discorso giuridico: da un lato, come dicevamo, l'attenzione verso una costellazione di interessi, da soddisfare attraverso i programmi *software*, dall'altro lato la consapevolezza circa i rischi e le trappole insite nel percorso di adattamento e costruzione del programma *software* a partire dalle trappole linguistiche del linguaggio naturale. A quest'ultimo riguardo, una specifica attenzione è dedicata agli aggettivi, gli avverbi, le frasi declinate in forma negativa etc.: tutti usi linguistici del linguaggio naturale che i programmatori, secondo quello *standard*, devono il più possibile evitare in quanto portatori di ambiguità e non facilmente riducibili alla logica del linguaggio di programmazione.

Assolutamente interessante è ulteriormente ricordare come di recente la scienza informatica si sia rivolta criticamente a quello *standard* ISO, non già per rinnegare le esigenze che esso esprime, bensì per proporre un affinamento e miglioramento delle tecniche idonee a conseguire i risultati a cui quello*standard* mira. Non è qui possibile dilungarci nemmeno su questo tema ([5]) e tuttavia sembra opportuno segnalare come tra i *computer scientists* sia condivisa l'indicazione di automatizzare il più possibile anche le procedure di controllo dei c.d. *RE Artifacts* (*Requirements Engineering Artifacts*) ossia i documenti che riassuntivamente contengono l'elencazione dei requisiti che devono avere i programmi *software*, ivi compreso per servire la finalità di ridurre il tasso di ambiguità del linguaggio naturale.

Siamo cioè di fronte ad un processo di affermazione di procedure automatizzate, tra cui procedure affidate a programmi *software*, per creare altri *software* anche nella fase di controllo e interpretazione dei "requisiti" originariamente concepiti ed espressi in linguaggio naturale.

Estremamente interessante è anche segnalare che la scienza informatica parla senza mezzi termini di difetti di qualità degli *RE Artifacts*:

«*Combining this view with the understanding of Juran, we understand high quality RE artifacts as RE artifacts that are free of RE artifact quality defects, which impair the aforementioned goals*» ([6]); «*A high-quality RE artifact is free of RE artifact quality defects …. RE quality defects are instances of actors of a concrete system, which negatively affect activities to be*

[5] Cfr. per approfondimenti, *ex multis*, H. FEMMER, *Requirements Engineering Artifact Quality: Definition and Control*, Monaco, 2017; H. FEMMER, D. MÉNDEZ FERNÁNDEZ, S. WAGNER, S. EDER, *Rapid quality assurance with Requirements Smells*, in *The Journal of Systems and Software*, 123, 2017, pp. 190–213; C. ARORA, M. SABETZADEH, L. BRIAND, F. ZIMMER, *Automated Checking of Conformance to Requirements Templates Using Natural Language Processing*, in *IEEE Transactions on Software Engineering*, Vol. 41, No. 10, ottobre 2015, pp. 944 - 968; A. VEIZAGA, M. ALFEREZ, D. TORRE, M. SABETZADEH, L. BRIAND, *On systematically building a controlled natural language for functional requirements*, in *Empirical Software Engineering*, 2021, (26:79), accessibile su https://doi.org/10.1007/s10664-021-09956-6; A. SLEIMI, N. SANNIER, M. SABETZADEH, L. BRIAND, M. CECI, J. DANN, *An automated framework for the extraction of semantic legalmetadata from legal texts*, in *Empirical Software Engineering*, 2021, cit.; N. ZENI, E.A. SEID, P. ENGIEL, J. MYLOUPOLOS, *NómosT: Building large models of law with a tool-supported process*, in *Data & Knowledge Engineering*, vol. 117, 2018, pp. 407–418.

[6] H. FEMMER, *Requirements Engineering Artifact Quality: Definition and Control*, op. cit., p. 13; J.M. JURAN e A. BLANTON GODFREY, *Juran's Quality Handbook*, McGraw-Hill, 5 ed., 1998.

conducted with the artifact. Therefore, a high quality RE artifact is efficient and effective to use» ([7]).

In questo contesto, si parla del problema dell'*ambiguità del linguaggio naturale* e si distingue tra *quattro tipi* di ambiguità: *lessicale, sintattica, semantica* e *grammaticale*.

Servendosi degli studi della disciplina informatica e della prassi molto sviluppata nota sotto il nome di NLP (*Natural Language Processing*), si sottolinea come la scienza informatica sia attualmente in grado di individuare e rimediare casi di ambiguità dei primi due tipi (lessicale e sintattica) ma non ancora degli altri due tipi (semantica e grammaticale) per cui si raccomandano controlli e tecniche (volte a far fronte ai difetti di qualità) sia automatizzate che manuali, ivi incluse tecniche che fanno impiego del linguaggio artificiale noto come linguaggio naturale controllato o semplificato.

11.9. *Software* e IA per scrivere *software*: la molteplice e la nuova artificialità

Giunti a questo punto, possiamo provare a riepilogare le nozioni fin sopra riassunte parlando in sintesi di una *molteplice artificialità*, alla quale, come proveremo a dire fra poco, si accoppia anche una *nuova artificialità*.

Con l'espressione 'molteplice artificialità' facciamo riferimento in sintesi ai fenomeni da ultimo descritti, che vedono il concorso di una pluralità di programmi *software* – scritti in linguaggi artificiali – per la scrittura e l'esecuzione di ogni nuovo *software* (scritto a sua volta in linguaggio artificiale).

Con l'espressione 'nuova artificialità' invece intendiamo fare riferimento ad un fenomeno ulteriore, rinvenibile nelle conseguenze applicative di una teoria che parla di '*naturalness*' a proposito dei linguaggi di programmazione. Si tratta di un'apparente contraddizione, che letteralmente può tradursi in italiano come naturalità dei linguaggi di programmazione ([8]). Coloro che hanno propugnato

[7] H. FEMMER, op. ult. cit., p. 15.

[8] M. ALLAMANIS, E.T. BARR, P. DEVANBU, C. SUTTON, *A Survey of Machine Learning for Big Code and Naturalness*, 2018, accessibile su https://arxiv.org/pdf/1709.06182.pdf, p. 3: «*The inspiration for the naturalness hypothesis can be traced back to the "literate programming" concept of D. Knuth, which draws from the insight that programming is a form of human communication: "Let us change our traditional attitude to the construction of programs:*

questa teoria, naturalmente, sono ben consapevoli della natura artificiale dei linguaggi di programmazione *software* e tuttavia, sempre per le finalità divisate dalla disciplina del *Software Requirements Engineering*, hanno proposto di *trattare i codici dei linguaggi di programmazione come testi scritti in lingue del linguaggio naturale*, sottoponendoli ad analisi statistiche secondo le tecniche del NLP (*Natural Language Processing*). Si tratta di tecniche le cui applicazioni sono a tutti note, che comprendono, ad esempio, quelle che suggeriscono come completare una frase su uno smartphone o su un motore di ricerca, e che si avvalgono sempre più di *software* di intelligenza artificiale.

Ebbene, la scienza informatica è arrivata a trattare un'enorme quantità di codici di programmi per elaboratori accessibili in open access, il c.d. Big Code, assoggettando tutti questi codici ad analisi statistiche ed applicazioni di intelligenza artificiale in modo analogo a quello in cui le tecniche di NLP trattano testi scritti in linguaggio naturale, per proporre funzioni come quella di completamento (code completion) ed altre più sofisticate al fine di aiutare i programmatori (esseri umani) a completare o a scrivere i programmi software. Con alcuni risultati positivi, tra cui la riduzione di linee di codice ridondanti, ossia inutilmente lunghe o ripetitive (che rendono difficoltosa la lettura e rallentano l'esecuzione impiegando energia superflua), la riduzione di *bugs* ecc. ([9]).

Siamo cioè sia per il linguaggio naturale che per il linguaggio artificiale di fronte ad *una nuova artificialità che è l'artificialità dei parlanti, più precisamente, degli elaboratori*.

Tradizionalmente, con riferimento alle lingue e ai linguaggi, il carattere dell'artificialità è collegato alla sua creazione: con lingua "artificiale" si intende una lingua originariamente creata e divulgata in un preciso momento nel tempo da una o più persone determinate, riconoscibili come autori di uno specifico e ben definito prodotto intellettuale consistente in un nuovo sistema di comunicazione composto di

---

Instead of imagining that our main task is to instruct a computer what to do, let us concentrate rather on explaining to human beings what we want a computer to do..." » dove il riferimento è a D.E. KNUTH, *Literate programming,* in *Computer Journal*, vol. 27, n. 2, 1984, p. 97 ss.

[9] M. ALLAMANIS, E.T. BARR, P. DEVANBU, C. SUTTON, *A Survey of Machine Learning for Big Code and Naturalness*, 2018, cit., p. 1: «*Unfortunately, developing software is a costly process: software engineers need to tackle the inherent complexity of software while avoiding bugs, and still delivering highly functional software products on time*». Cfr. anche https://www.agendadigitale.eu/cultura-digitale/ai-luci-e-ombre-del-software-che-scrive-software/

specifiche regole semantiche e sintattiche; in contrapposizione dunque all'idea del linguaggio naturale, che identifica invece lingue rilevabili come prodotti storici spontanei di comunità per lo più con origini etniche e territoriali circoscritte, in funzione di comunicazione naturale tra persone di quelle comunità.

Oggi possiamo vedere un *secondo significato di artificialità* del linguaggio (tanto di quello naturale che di quello di programmazione) legato al loro uso da parte di *parlanti artificiali*, gli elaboratori elettronici, che elaborano, processano, trattano testi di linguaggio naturale o di programmazione - *input* - per le più varie finalità, ossia per produrre *output* serventi i più diversi scopi, a seconda delle funzioni delle applicazioni.

Se è vero che all'incessante lavorio dei fruitori-parlanti umani si deve il prodotto del linguaggio nel suo *farsi storico*, ossia nel suo aspetto dinamico, oggi i fruitori sono anche gli elaboratori elettronici, che, con funzioni governate dagli appositi *software* che abbiamo sopra sommariamente ricordato, producono – con la funzione di completamento e altre più sofisticate (*chatbot*, assistente vocale etc. ([10])) – a produrre *output* che privilegiano certi usi linguistici, scartandone altri, sia in lingue di linguaggio naturale che in linguaggi di programmazione.

Si tratta di una dinamicità *sia in costruzione che in distruzione*. Quella in distruzione delle lingue del linguaggio naturale è evidente a tutti. Basti pensare alle funzioni di completamento e agli altri *output* di suggerimenti che incessantemente accompagnano la nostra scrittura sugli *smartphone*, sulle ricerche che compiamo sui motori di ricerca, sui programmi di scrittura etc.: suggerimenti che, selezionando gli usi linguistici più affermati e scartando quelli statisticamente desueti, modificano impercettibilmente, impoverendole, le lingue.

D'altronde la storia ha conosciuto altri fenomeni analoghi legati alle tecnologie ad es. per la lingua italiana con la televisione di Stato. Ci sarebbe da fare in proposito un discorso sulla *spontaneità* e sulla *natura* dell'elaborazione – umana vs artificiale - dei processi di accelerazione dei cambiamenti anche culturali che interessano questi fenomeni, e nuovamente osservare la molteplice e quasi

[10] Cfr. L. VIZZONI, Smart assistant *e dati personali: quali rischi per gli utenti?*, in *Annuario 2021 Osservatorio Giuridico sulla Innovazione Digitale*, a cura di S. Orlando e G. Capaldo, Roma 2021, p. 381 ss.

esclusiva artificialità del processo odierno affidato alle tecniche del NLP. Ma non possiamo soffermarci oltre.

Qui è sufficiente segnalare una nuova artificialità che possiamo chiamare "artificialità di trattamento o elaborazione" da contrapporre all'artificialità tradizionale, che possiamo chiamare "artificialità di creazione", ed osservare che essa ha campo sia per processare testi espressi in lingue del linguaggio naturale che per processare testi espressi in linguaggi artificiali, ed in particolare in linguaggi di programmazione.

Inoltre, come abbiamo visto, e per riassumere:

Nella fase del *software requirements engineering*:

- per scrivere un programma *software* intervengono pratiche (manuali o automatizzate) che si servono del c.d. linguaggio naturale controllato o semplificato dichiaratamente inteso a ridurre il tasso di ambiguità del linguaggio naturale: il c.d. linguaggio naturale controllato o semplificato;

- tra le pratiche automatizzate di *software requirements engineering* si trova proposto l'impiego di programmi *software* attuativi di procedure intese – nuovamente - a correggere le ambiguità dei requisiti di programmazione espressi in linguaggio naturale o in linguaggio naturale controllato.

Nella fase di scrittura dei programmi:

- per scrivere *software*, i programmatori si servono sempre di altri *software* (text editors, IDE etc.) che creano un ambiente per la scrittura;

- ed ancora *software* di IA che suggeriscono come scrivere pezzi di programmi o come completare o correggere pezzi di programma.

Nella fase di trasmissione per l'esecuzione:

- vengono utilizzati *software* che traducono (compilano/assemblano in codice oggetto) e/o interpretano (ovvero direttamente eseguono) i programmi (*assemblers*/*compilers*/*interpreters* e ibridi es. *bytecode*).

Infine, nella fase di ingaggio dei sistemi operativi:

- vengono impiegati gli insiemi dei *software* dei sistemi operativi, il cui "cuore" è denominato *kernel*, che costituiscono l'interfaccia tra il *software* e l'*hardware*.

11.10. Ubiquità del software, immersività, nuova incalcolabilità e pratiche proprietarie

L'ubiquità del *software* nella vita di tutti i giorni è un dato di comune esperienza, e non è necessario aggiungere una sola parola per dimostrarla.

La nuova dimensione sulla quale sembra necessario acquisire maggiore consapevolezza è invece quella della c.d. immersività: dopo essersi dedicata alle funzioni intellettuali legate al linguaggio ([11]) (elaborazione di *input* di parole e testi) e a quelle sensoriali della vista e dell'udito (elaborazioni di *input* di immagini e suoni), la scienza informatica lavora nella direzione della creazione di una *immersività sensoriale completa* allargata agli altri sensi, compresa la propriocezione ([12]).

Questa nuova realtà, in cui l'Umanità si va progressivamente immergendo, è mediata da linguaggi artificiali. Per esser più precisi: è *creata* e *governata* da linguaggi artificiali.

Inoltre, seppure non è possibile affrontare il tema più approfonditamente in questa sede, è necessario aggiungere in questo contesto l'osservazione che i programmi *software* (prodotti da scritture molteplicemente artificiali, come visto), da un lato *rispondono sempre a pratiche proprietarie* e dall'altro lato possono innescare - in alcune applicazioni- *calcoli incalcolabili* (più precisamente, incontrollabili) per ragioni tecniche.

Sotto il primo aspetto, è sufficiente accennare alla logica proprietaria del *copyright*, che pervade sempre ogni *software* (logica cui non si sottraggono le licenze in *open access*, di variabile estensione, proprio perché sono licenze).

---

[11] Tanto il linguaggio naturale, scritto e parlato, quanto i linguaggi artificiali, compreso, come visto, il linguaggio informatico.

[12] Il '*metaverse*' del 2021 di Mark Zuckerberg (https://about.facebook.com/meta/?_ga=2.21626552.247952293.1641562500-477567524.1641562500) è solo l'ultima eco di una novità annunciata da tempo. Cfr. già L. GALLINO, voce "*Virtuale, realtà*", in *Enciclopedia delle Scienze Sociali*, I, Supplemento (2001), accessibile su https://www.treccani.it/enciclopedia/realta-virtuale_%28Enciclopedia-delle-scienze-sociali%29/: "[…] *I sistemi più complessi di realtà virtuale si avvicinano all'ideale d'una completa immersività per quanto concerne la vista, l'udito, la sensibilità propriocettiva (terminazioni muscolotendinee) e la sensibilità epicritica (tatto e sensazioni termiche e dolorifiche). Sono state avviate ricerche ed esperimenti concernenti l'olfatto; più lontana, ma non impossibile, appare la conquista del gusto da parte della realtà virtuale*.".

La *logica proprietaria* riguarda il prodotto *software*, inteso come risultato del processo creativo, come ben noto. Ma, come non si sottolinea abbastanza, essa riguarda anche lo stesso processo creativo del *software*: ed infatti, lo stesso processo di scrittura del *software* è pervaso da pratiche proprietarie, atteso – come abbiamo visto - il necessario e multiforme intervento di programmi *software* nella creazione di altri programmi *software* (*software* di *requirements engineering*, *code completion*, IDE, *editing*, traduzione, *compilers*, *assemblers* etc.).

Così come è pertinente sottolineare che anche gli stessi linguaggi di programmazione (che in sé considerati, ossia nella loro consistenza di sintassi e semantica, non formano oggetto di privative in senso giuridico) sono fatti oggetto nella sostanza di *pratiche proprietarie*: è il tema non soltanto del necessario collegamento ai *software* licenziati di cui sopra (*requirements engineering*, *code completion*, IDE, *editing*, traduzione, *compilers*, *assemblers* etc.), ma anche quello dei corsi di formazione e di aggiornamento e dei relativi materiali a pagamento, rispondenti a circoli più o meno aperti di divulgatori (detentori della relativa conoscenza).

Sotto il secondo aspetto – l'*incalcolabilità* – facciamo riferimento a programmi che istruiscono l'elaboratore a compiere calcoli il cui esito (*output*) talvolta *non è prevedibile a priori né è ricostruibile a posteriori*. È il ben conosciuto tema della c.d. *black box*, che, con particolare riferimento all'intelligenza artificiale, è indagato a proposito delle c.d. reti neurali e dà luogo alla, pure ben nota e per certi aspetti fraintesa, questione della *Explainable AI* (XAI).

In questo contesto di buio, che nasce da ragioni *tecniche*, si inserisce e si assomma una oscurità dovuta a ragioni *giuridiche*, in particolare a privative (invocate più o meno fondatamente ma ancora molto efficacemente), e che si allarga, oltre che al *diritto di autore*, alla protezione del *know-how* e dei *brevetti*.

Quindi una *nuova incalcolabilità di matrice tecnica* e una ben protetta *oscurità di matrice giuridica*.

E mentre per la seconda è immaginabile ed è anche possibile e auspicabile un percorso di emendamento (che cominci con il riconoscere la dimensione giuridica di prodotto dei *software*, e continui con l'abbattere, a partire da quel riconoscimento, certi tabù di intoccabilità e di applicabilità senza riserve, in quest'ambito, delle privative intellettuali ed industriali ([13])), la prima non lo è, almeno non lo è sulla base di quanto si dice

[13] Un segnale in questa direzione è stato di recente dato dalla Corte di Giustizia dell'Unione Europea, affermando il diritto alla decompilazione del *software* da parte

che l'uomo possa oggi conseguire ("lo stato dell'arte"): sulla base, più precisamente, di quanto gli esperti dicono oggi di riuscire a comprendere e spiegare circa l'*output* di certi algoritmi, in particolare relativamente al c.d. *deep learning* e alle c.d. reti neurali.

11.11. Quid iuris?

La previsione di quel tipo particolare di relazioni che chiamiamo conflitti, giustifica e caratterizza essenzialmente il diritto, l'ordinamento giuridico non altro essendo in essenza che un sistema cognitivo di conflitti, che il diritto – per l'appunto - prevede in funzione della loro prevenzione o soluzione.

Come ogni sistema cognitivo, il diritto ha suoi criteri di rilevanza, che sta a dire - *a contrario* - che ciò che non vi si conosce per suo mezzo è irrilevante (è giuridicamente tale).

Ed effettivamente, la singolarità, la verità e la franchezza del diritto consistono proprio nella nudità giuridica dei fenomeni, che il diritto impone di spogliare per cercare (tutti e soltanto) i tratti dei conflitti da offrire alla regola che li prevede.

Così anche la stanza della responsabilità giuridica è uno spogliatoio, nel quale deve esercitarsi il mestiere della sottrazione, alla ricerca di quegli elementi di fatto e di quei nessi logici che caratterizzano determinati tipi di conflitti, siccome originati da comportamenti ritenuti dal diritto antisociali e come tali contrastati.

Dunque proprio nel prisma della responsabilità, uno sguardo franco ci impone di vedere quella nuova realtà, creata da linguaggi molteplicemente artificiali e caratterizzati da pratiche proprietarie ed esiti giuridicamente e spesso anche tecnicamente incalcolabili, nella quale l'Umanità si va sempre più immergendo, per stabilire quali fatti e quali nessi siano da ritenersi giuridicamente rilevanti per i problemi della responsabilità, e prima ancora: *quale idea di socialità* (sintesi tra la società e i comportamenti osservati e accettati nel suo seno) sia realistico ed adeguato immaginare dietro norme funzionalmente intese, per definizione, a contrastare comportamenti antisociali.

---

del legittimo acquirente per correggere errori del codice che incidono sul funzionamento del programma: v. E.M. INCUTTI, *La sentenza della Corte di Giustizia UE del 6 ottobre 2021 sul diritto di decompilazione del software (il caso Top System)*, nella rubrica '*Diritto e nuove tecnologie*', in *Persona e mercato*, 2021, p. 893 ss.

E, naturalmente, *quale idea di uomo*.

È questo – evidentemente - lo spazio della riflessione sul rapporto tra l'uomo, la società e la *ricerca scientifica* (sulla quale ultima poco o niente si trova riflesso nei documenti, i libri bianchi e i progetti normativi della UE relativi all'intelligenza artificiale), e sulla *sintesi di socialità possibile* – e dunque: l'indagine sugli equilibri, i conflitti e i 'rischi' generati dalle applicazioni della ricerca scientifica.

11.12. «… e il verbo era presso l'uomo»

Ma insieme a questo, e proprio per dare un contributo al dibattito sui rischi generati in quest'ambito dalle applicazioni della ricerca scientifica, *sarà necessario fermarsi innanzitutto a riflettere sulla radice molteplicemente artificiale del linguaggio che crea e governa questa nuova realtà*, e così riconoscere con franchezza che la sua creazione è segnata da un *progressivo distacco dal linguaggio naturale*.

Certamente, l'esecuzione automatica, da parte di dispositivi tecnologici, di istruzioni di calcolo espresse in linguaggi artificiali, è *responsabilità* dell'uomo: non solo di singoli "uomini" con riferimento a singoli processi e a singoli sistemi di IA, ma "dell'uomo" in generale, con riferimento alla decisione 'a monte' di vivere in un mondo connotato dall'ubiquità del *software*.

Anche in quest'ambito, come per ogni sfida culturale proposta dagli avanzamenti applicativi della tecnica, è proprio la potenza delle tecnologie digitali ad imporre di assumere consapevolezza circa la necessità di declinazione in forma collettiva della famosa sentenza sul destino: da *homo faber fortunae suae* a *humanitas fabra fortunae suae*.

Consapevolezza e mancanza di consapevolezza, come si sa, evocano scenari per definizione contrapposti, l'esattezza della cui predizione è, a sua volta, e naturalmente, dipendente dal grado di consapevolezza di chi li evoca; e anche dall'equilibrio del giudizio, senza il quale è facile interpretare in maniera manichea, o addirittura caricaturale, la contrapposizione.

Effettivamente, la prospettiva di un'umanità che non assuma un'adeguata consapevolezza critica circa i caratteri dei linguaggi informatici, il loro scarto rispetto al linguaggio naturale, e il loro ruolo esclusivo nella creazione e nel governo delle tecnologie digitali, e dunque nella creazione e nel governo del nuovo mondo connotato dall'immersività e dall'ubiquità di cui dicevamo, può evocare uno scenario di

linguaggi artificiali autopoietici e fuori controllo; ossia di un futuro nel quale - con la verità spiazzante di una battuta – potrebbe, con qualche ragione, tra qualche tempo dirsi: «… e il verbo *era* presso l'*uomo*».

Ma non è davvero per tratteggiare scenari cupi o futuri distopici che abbiamo preso la parola.

Il messaggio conclusivo che vorremmo affidare a questa relazione è, tutto al contrario, positivo e propositivo, e va nella direzione della proposta di assunzione di consapevolezza circa l'importanza fondamentale del linguaggio – che deriva dal suo valore fondativo (ossia creativo ed esplicativo insieme) per ogni comunità.

E dunque sulla necessità di aggiungere all'elenco dei temi del dibattito giuridico sull'innovazione digitale quello dello scarto e del necessario dialogo tra il linguaggio naturale e il linguaggio informatico: ossia i problemi di adattamento e traduttologici che abbiamo sopra abbozzato nei loro tratti essenziali.

Come notavamo prima, nei libri bianchi, negli studi e nei progetti di regolamenti sull'IA dell'Unione Europea, poco o niente è dedicato alla ricerca ([14]). Come ricercatori dovremmo far sentire una voce. Ma, specificamente, proprio come ricercatori *giuristi*, interessati alle strutture fondative e regolative della società intesa come comunità di persone, dovremmo far notare anche l'assenza di un approfondimento sui linguaggi ai quali si affida il disegno dei sistemi e delle applicazioni dell'intelligenza artificiale. E colmare la lacuna.

Da qui la sollecitazione di un dibattito sui profili giuridici dei temi che abbiamo oggi succintamente segnalato. Perché, in definitiva, sarebbe manchevole occuparsi della nascita e della *governance* delle nuove tecnologie digitali senza prestare attenzione ai linguaggi che le creano e le istruiscono.

E anche perché, più profondamente, non può immaginarsi una comunità che non comunica; e tale sarebbe il destino della nostra *societas*, che è (già) oggi una comunità legata da strutture informatiche, laddove essa non maturasse una coscienza dei suoi linguaggi.

---

[14] Ma cfr. da ultimo il *Progress Report* della Presidenza del Consiglio dell'Unione Europea del 22 novembre 2021, recante una proposta di modifica del testo di proposta dell'*Artificial Intelligence Act* del 21 aprile 2021 (COM(2021) 206 final) nel senso, *inter alia*, di far chiaro che l'AIA non si applichi ai sistemi di IA e ai loro *output* usati per il solo scopo di ricerca e sviluppo (13802/1/21 REV 1- *Interinstitutional File*: 2021/0106(COD)).

12. L'intelligenza artificiale nel prisma dell'impresa: evoluzione normativa e prospettive di studio

Francesco Pacileo (Università di Roma La Sapienza)

12.1. Alcuni fra i principali rischi connaturati all'intelligenza artificiale

Le istituzioni europee e la letteratura scientifica hanno evidenziato alcuni rischi connaturati all'impiego dei sistemi di intelligenza artificiale (IA) [1] ed al connesso utilizzo dei *big data* [2].

---

[1] Ad oggi non esiste ancora una definizione univocamente accettata e compiuta di "intelligenza artificiale. Per una definizione, anche con riferimento al *machine learning* ed al *deep learning* cfr., comunque, COMMISSIONE EUROPEA, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, Bruxelles, 25 aprile 2018, pt. 1, secondo cui «"Intelligenza artificiale" (IA) indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi». In dottrina, cfr. M. GUIHOT, A.F. MATTHEW, N.P. SUZOR, *Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence*, in 20 *Vand. J. Ent. & Tech. L.* (2017), da p. 385, pp. 393 ss.; M.U. SCHERER, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, in 29 *Harv. J.L. & Tech.* (2016), da p. 354, pp. 359 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, Study requested by JURI committee, July 2020, p. 9, pp. 15 ss. Per ulteriori definizioni di "electronic agent", S. WETTIG, E. ZEHENDNER, *A legal analysis of human and electronic agents*, in 12 *AI & L.* (2004), da p. 111, pp. 129 ss. Cfr., inoltre, M. HILDEBRANDT, *Law* as *Information in the Era of Data-Driven Agency*, in 79 *Modern L. Rev.* (2016), da p. 1, p. 4.

[2] Per una definizione anche del c.d. *big data analytics* cfr. BANCA D'ITALIA, *Fintech in Italia. Indagine conoscitiva sull'adozione delle innovazioni tecnologiche applicate ai servizi finanziari*, dicembre 2017, in www.bancaditalia.it, 31, secondo cui essi costituiscono un «insieme di dati di enorme dimensione, memorizzati anche in archivi eterogenei, ossia non correlati tra loro, per la cui analisi vengono utilizzati strumenti di statistica inferenziale e concetti di identificazione di sistemi non lineari per dedurre regressioni, effetti causali e relazioni. A differenza dei sistemi gestionali tradizionali, che trattano

Al riguardo si segnalano innanzi tutto il rischio di "contagio", inconsapevole o meno, dai programmatori ed utilizzatori all'algoritmo, di pregiudizi ed elementi ingiustificatamente discriminatori [3]; il rischio di sviluppi dannosi imprevisti ed imprevedibili degli algoritmi soprattutto di *machine learning* [4]; i rischi, strettamente collegati all'ultimo menzionato, conseguenti alla difficoltà se non addirittura all'impossibilità di ricostruire tutti i processi logici che hanno portato ad un determinato *output* (c.d. *black box algorithm*) [5].

Tuttavia, alla maggiore complessità dell'algoritmo e alla mole di dati trattati corrisponde in maniera direttamente proporzionale una maggiore *accuracy* delle previsioni e degli *output* [6].

---

dati strutturati o strutturabili in tabelle tra loro relazionabili, i big data comprendono anche dati semistrutturati o non strutturati (ad es. dati che provengono dal web come i commenti sui social media, documenti di testo, audio, video disponibili in diversi formati, etc.)»; FSB, *Artificial intelligence and machine learning in financial services. Market developments and financial stability implications*, 1 November 2017, in www.fsb.org, 4 ss.

[3] Cfr. S. BAROCAS, A.D. SELBST, *Big Data' s Disparate Impact*, in 104 *Cal. L. Rev.* (2016), da p. 671, p. 677 ss.; M. GUIHOT, A.F. MATTHEW, N.P. SUZOR, *Nudging Robots*, cit., pp. 404 s.; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YUT, *Accountable Algorithms*, in 165 *U. Pa. L. Rev.* (2017), da p. 633, pp. 678 ss.; M. HILDEBRANDT, *Law* as *Information*, cit., pp. 24 s.; L. ENRIQUES, D. ZETZSCHE, *Corporate Technologies and the Tech Nirvana Fallacy*, in 72 *Hastings L. J.* (2020), da p. 55, 66 ss. e *passim* Nella letteratura italiana, cfr. N. ABRIANI, G. SCHNEIDER, *Diritto delle imprese e intelligenza artificiale. Dalla Fintech alla Corptech*, Bologna, 2021, 38 ss.; A. NUZZO, *Algoritmi e regole*, in *AGE*, 1/2019, da p. 39, p. 43.

[4] Cfr. H. EIDENMÜLLER, *The Rise of Robots and the Law of Humans*, Oxford Legal Studies Research Paper No. 27/2017, p. 5, secondo cui detti sistemi «are unpredictable by design»; H. ZECH, *Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken*, in *Intelligente Agenten und das Recht*, Hrsg. S. Gless, K. Seelmann, Baden Baden, 2016, da p. 163, pp. 172 ss.; U. PAGALLO, *Killers, fridges, and slaves: a legal journey in robotics*, in *AI & Society*, January 2011, p. 6.

[5] Sul *black box algorithm* cfr. F. PASQUALE, *The Black Box Society. The secret Algorithms That Control Money and Information*, Cambridge-London, 2015; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YUT, *Accountable Algorithms*, cit., *passim*; M. HILDEBRANDT, *Law* as *Information*, cit., p. 26; Y. BATHAEE, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, in 31 *Harvard Journal of Law & Technology* (2018), da p. 889; E. PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *NLCC*, 2018, da p. 1209, 1209 ss. spec. 1212; A. NUZZO, *Algoritmi e regole*, cit., p. 44; M.L. MONTAGNANI, *Flussi informativi e doveri degli amministratori di società per azioni ai tempi dell'intelligenza artificiale*, in *Persona e Mercato*, 2020/2, da p. 65, pp. 78 ss. Cfr., altresì, COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, Bruxelles, 19 febbraio 2020, COM(2020) 65 final, p. 13.

[6] Cfr. A. MATTHIAS, *Automaten als Träger von Rechten. Plädoyer für eine Gesetzänderung*,

Una trattazione a parte, che non può essere effettuata in questa sede, meriterebbero poi i rischi connessi a chi dispone dei *big data* nonché i rischi connessi a dolose manomissioni e ad attacchi informatici, sintetizzabili nell'espressione *cybersecurity* ovvero connessi alla protezione della riservatezza e dei dati personali.

Nondimeno alcune fra le questioni (anche) giuridiche maggiormente controverse sorgono in relazione alla capacità o meno dei sistemi di IA di assumere "decisioni" (si preferisce il temine *output*) e di assumerle in maniera sostanzialmente autonoma [7] rispetto ai programmatori, fornitori, utilizzatori e tutti i componenti della catena di valore dei sistemi di IA.

In particolare, un'attenta dottrina ha segnalato un potenziale vuoto di responsabilità (*Verantwortungslücke*) che consiste nella difficoltà per gli uomini ad avere un sufficiente controllo sulle macchine autonome, tale da giustificare una responsabilità correlata all'abilità del controllore: in particolare, detta difficoltà discende non solo dalla menzionata imprevedibilità (*Unberechenbarkeit*) di tali macchine ma altresì dalla circostanza che esse si trovano al di là dell'"orizzonte visuale" del produttore, il quale allora si troverebbe nell'impossibilità di evitare il pregiudizio [8].

Berlin, 2008, p. 22, p. 37; P.B. DE LAAT, *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, in 31 *Philos. Techn.* (2018), da p. 525.

[7] Sull'autonomia dell'IA cfr. COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., p. 18; COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, COM(2020) 64 final, Bruxelle, 19 febbraio 2020, pp. 7 s. In dottrina, cfr. A. WIEBE, *Die elektronische Willenserklärung*, Tübingen, 2002, pp. 27 ss. Nella letteratura italiana, cfr. A. BERTOLINI, *Robots as Products: The Case for Realistic Analysis of Robotic Applications and Liability Rules*, in *Law, Innovarion, Technology*, 2013, da p. 213, pp. 220 ss. Sui concetti di indipendenza e controllo cfr., altresì, R. ABBOTT, *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, in 86 *Wash. L. Rev.* (2018), da p. 1, p. 23. Cfr. U. PAGALLO, *Killers, fridges, and slaves*, cit., p. 6; ID., *The Law of Robots: Crimes, Contracts and Torts*, Heidelberg-New York-London, 2013, p. 2, secondo cui sussiste autonomia quanto i robot «sense-think-act» senza l'intervento o il coinvolgimento degli uomini. Nella letteratura giuridica, propendono per la capacità di assumere decisioni R. ABBOTT, *The Reasonable Computer*, cit., p. 23; T. ALLEN, R. WIDDISON, *Can Computers Make Contracts?*, in 9 *Harv. J. L. & Tech.* (1996), da p. 25, p. 27; R. ROMANO, *Intelligenza artificiale, decisioni e responsabilità in ambito finanziario*, cit., p. 325. Di opposto avviso, H. EIDENMÜLLER, *The Rise of Robots and the Law of Humans*, cit., pp. 12 ss.; H.P. BULL, *Sinn und Unsinn des Datenschutzes*, Tübingen, 2015, pp. 118 ss.

[8] Cfr. A. MATTHIAS, *op. loc. cit.*; B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE, *Bridging the Accountability Gap: Rights for New Entities in the Information Society?*, in 11

L'importanza e la serietà del problema è certificata da una risoluzione del Parlamento europeo del 2017 (di seguito anche "Risoluzione del 2017"), che individua, tra un ventaglio di ipotesi di regolamentazione di diritto civile della robotica, anche quella di istituire normativamente una «personalità elettronica» («electronic person») da attribuire all'IA, che in tal modo verrebbe ad avere una propria soggettività giuridica, un proprio patrimonio ed una propria responsabilità [9].

Il rischio più grave, allora, può apparire quello di parificare in qualche modo esseri umani e sistemi di IA e, di conseguenza, di comprimere, e di comprimere eccessivamente, gli affari e le attività umane se non addirittura l'essenza degli esseri umani [10].

12.2. Il difficile inquadramento della natura giuridica dell'IA. Opportunità di un'interpretazione funzionale ed evolutiva

Prendendo parte all'esercizio intellettuale denominato "Gaio digitale" in voga tra i relatori dell'Osservatorio Giuridico sull'Innovazione Digitale, i problemi finora posti in evidenza potrebbero spingere persino a domandarsi ove si collochi l'IA nell'ambito della nota tripartizione gaiana [11]. Nondimeno si crede opportuno seguire un approccio

Minn. J. L. Sci. & Tech. (2010), da p. 497, p. 546, p. 553. Cfr., altresì, G. TEUBNER, *Digitale Rechtssubjekte? Zum privatrechtlichen Status automater Softwareagenten*, in 218 *AcP* (2018), da p. 155, (anche nella versione in italiano *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, a cura di P. Femia, Napoli, 2019), p. 157 ss.

[9] Cfr. PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, (2015/2103(INL), 17 febbraio 2017, P8_TA(2017)0051, ptt. 49 ss. spec. pt. 59, lett. (*f*). In dottrina, cfr. H. EIDENMÜLLER, *The Rise of Robots and the Law of Humans*, cit., critico; B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE, *Bridging the Accountability Gap*, cit., p. 510; G. SCARCHILLO, Corporate Governance *e Intelligenza Artificiale*, in *NGCC*, 2019, da p. 881, p. 884; R. ROMANO, *Intelligenza*, cit., pp. 326 ss.

[10] Cfr., tra i molti che paventano un rischio di sopravvivenza dell'umanità di essere sopraffatta da macchine con intelligenza superiore, B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE, *Bridging the Accountability Gap*, cit., *passim*, spec. pp. 557 ss.; I. OLEKSIEWICZ, M.E. CIVELEK, *From Artificial Intelligence to Artificial Consciousness: Possible Legal Bases for the Human-Robot Relationships in the Future*, in 7 *Int. J. Adv. Res.* (2019), da p. 254. Cfr., altresì, U. RUFFOLO, A. AMIDEI, *Intelligenza Artificiale e diritti della persona: le frontiere del ''transumanesimo''*, in *Giur. it.*, 2019, da p. 1658.

[11] Il riferimento va alla nota massima «Omne autem ius quo utimur, vel ad personas pertinet vel ad res vel ad actiones» (Gai. 1.8). Per l'esercizio intellettuale relativo a

funzionale e allora in questi termini l'impressione è che assuma uno specifico interesse scientifico la prospettiva dell'*impresa* e, specificamente, dell'impresa organizzata in forma societaria, ed in particolare di una società che può permettersi di disporre di simili tecnologie, quindi oggi una società di capitali [12].

La prospettiva dell'impresa, si crede, pur non dovendosi considerare in termini assoluti, è senz'altro centrale nell'analisi giuridica dell'IA, posto che buona parte di produttori, programmatori e degli utilizzatori di questi sistemi sono imprese, e imprese organizzate in forma di società di capitali, o comunque persone fisiche che operano nell'ambito di un'organizzazione imprenditoriale.

Trascurare questo dato di fatto potrebbe implicare criticità non dissimili da quelle riscontrate nel diritto concorsuale, ove la legge fallimentare è impostata sulla crisi e l'insolvenza del debitore imprenditore individuale ma poi la maggior parte dei debitori sottoposti a procedure concorsuali sono società, e società di capitali.

L'indagine circa l'opportunità di un'impostazione incentrata sull'impresa può procedere sulla base di almeno due percorsi, non necessariamente alternativi: l'analisi del dibattito dottrinale in merito alla natura giuridica dell'IA [13] e lo studio dell'evoluzione normativa tuttora in atto, quanto meno nell'UE. Per esigenze di sintesi, le successive pagine si concentreranno su tale ultimo aspetto.

"Gaio digitale" sono debitore di D. IMBRUGLIA, che ringrazio, e che pure ha scritto *L'intelligenza artificiale (IA) e le regole. Appunti*, in *Media Laws*, 2020, da p. 18.

[12] Sul tema dell'IA e della *corporate governance* cfr. M. FENWICK, J.A. MCCAHERY, E. P.M. VERMEULEN, *The End of Corporate Governance*, working paper, in *ECGI*, December 2018; M. FENWICK, E. P.M. VERMEULEN, *Technology and Corporate Governance: Blockchain, Crypto and Artificial Intelligence*, working paper, in *ECGI*, November 2018; F. MÖSLEIN, *Robots in the Boardroom: Artificial Intelligence and Corporate Law*, in W. Barfield, U. Pagallo (Eds.), *Research Handbook on the Law of Artificial Intelligence*, Northampton MA, 2018, da p. 649; L. ENRIQUES, D. ZETZSCHE, *Corporate Technologies*, cit.; J. ARMOUR, H. EIDENMÜLLER, *Self-Driving Corporations?*, in 10 *Harvard Business Law Review* (2020), da p. 87; L. LOPUCKY, *Algorithmic Entities*, in 95 *Wash. U. L. Rev.* (2018), da p. 887. Nella letteratura italiana cfr. G.D. MOSCO, *Roboboard. L'intelligenza artificiale nei consigli di amministrazione*, in *AGE*, 1/2019, da p. 247; N. ABRIANI, G. SCHNEIDER, *Il diritto societario incontra il diritto dell'informazione.* IT, Corporate governance *e* Corporate Social Responsibility, in *Riv. soc.*, 2020, da p. 1326; N. ABRIANI, *La* corporate governance *nell'era dell'algoritmo. Prolegomeni a uno studio sull'impatto dell'intelligenza artificiale sulla* corporate governance, in *NDS*, 2020, da p. 261; G. SCARCHILLO, Corporate Governance *e Intelligenza Artificiale*, in *NGCC*, 2019, da p. 881, M.L. MONTAGNANI, *Flussi informativi*, cit.

[13] Cfr., per tutti, B.-J. KOOPS, M. HILDEBRANDT, D.-O. JAQUET-CHIFFELLE *Bridging the Accountability Gap*, cit., *passim*; G. TEUBNER, *Digitale Rechtssubjekte?*, cit., *passim*.

12.3. Mancanza di una regolamentazione compiuta in tema di IA

Le istituzioni europee hanno promosso e portato avanti numerose ricerche sul tema: in particolare si è preso atto che ad oggi non esiste una normativa che disciplini in maniera soddisfacente l'impiego dell'IA e dei *big data*.

Qualche spunto potrebbe ricavarsi dalla direttiva sui prodotti difettosi (85/374/CEE del Consiglio) [14], ma con risultati parziali, come osservato dalla stessa Commissione europea [15].

Al riguardo, tale ultima direttiva è applicabile limitatamente ai danni materiali patiti dai consumatori, mentre andrebbe chiarito il concetto di "difettosità" dei sistemi di IA e se tali sistemi rientrino nella nozione di "prodotti" o in quella di "servizi" [16]. Significativamente gravoso, inoltre, può risultare l'onere probatorio a carico del danneggiato, che attualmente deve dimostrare il danno patito ed il nesso di

---

[14] Anche nell'ordinamento degli Stati Uniti la disciplina dei prodotti difettosi è stata attentamente presa in considerazione dalla dottrina, ai fini dell'applicabilità alle nuove tecnologie quale regola di responsabilità da *tort*. Cfr. R. ABBOTT, *The Reasonable Computer*, cit., pp. 13 ss., 22 ss.; D.C. VLADECK, *Machines without Principals: Liability Rules and Artificial Intelligence*, in 89 *Wash. L. Rev.* (2014), da p. 117, pp. 127 ss., seppure in chiave critica. Nella letteratura italiana, cfr. A. BERTOLINI, *Robots as Products*, cit., pp. 235 ss.; L. LIGUORI, in M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e* accountability*. Verso nuovi paradigmi?*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, a cura di F. Pizzetti, Torino, 2018, da p. 333, pp. 348 ss., ove numerosi riferimenti giurisprudenziali.

[15] Cfr., sul tema della responsabilità *de qua*, PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica*, cit.; COMMISSIONE EUROPEA, Relazione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo «sull'applicazione della direttiva del Consiglio relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi (direttiva 85/374/CEE)», COM(2018) 246 final, Bruxelles, 7 maggio 2018; COMMISSIONE EUROPEA, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, Bruxelles, 25 aprile 2018; COMMISSIONE EUROPEA, *Liability for emerging digital technologies*, SWD(2018) 137 final; COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., pp. 14 ss.; FSB, *op. cit.*, p. 26, 38. In dottrina, cfr. A. AMIDEI, *Intelligenza Artificiale e* product liability*: sviluppi del diritto dell'Unione Europea*, in *Giur. it.*, 2019, da p. 1715.

[16] Cfr. COMMISSIONE EUROPEA, COM(2018) 246 final, *cit.*, pt. 5.4.; COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., pp. 14 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 50 ss.; H. ZECH, *Zivilrechtliche Haftung*, cit., p. 176, pp. 184 s.; A. AMIDEI, *Intelligenza Artificiale*, cit., pp. 1720 ss.

causalità tra danno e difetto. Occorrerebbe poi aggiornare la nozione di "produttore" [17].

In buona sostanza, rileva il Parlamento europeo che, nonostante l'ambito di applicazione della direttiva sui prodotti difettosi, «l'attuale quadro giuridico non sarebbe sufficiente a coprire i danni causati dalla nuova generazione di robot, in quanto questi possono essere dotati di capacità di adattamento e di apprendimento che implicano un certo grado di imprevedibilità nel loro comportamento, dato che imparerebbero in modo autonomo, in base alle esperienze diversificate di ciascuno, e interagirebbero con l'ambiente in modo unico e imprevedibile» [18].

Altre normative – alcune di carattere generale, altre più specifiche – che in qualche modo possono contribuire a regolamentare l'impiego di sistemi di IA sono la direttiva sulla sicurezza generale dei prodotti (2001/95/CE), la direttiva macchine (2006/42/CE), la direttiva apparecchiature radio (2014/53/UE), la direttiva sui dispositivi medici (93/42/CEE), la direttiva sulla sicurezza dei giocattoli (2009/48/CE), la direttiva sugli strumenti di misura (2014/32/UE) e la normativa sull'omologazione dei veicoli [19].

Va da subito sottolineato che la normativa europea in materia di sicurezza dei prodotti e di responsabilità per i prodotti difettosi è retta dal principio guida per cui, a prescindere dalla complessità della catena del valore, la responsabilità per la sicurezza e la difettosità del prodotto verso gli utilizzatori è posta a carico del produttore che immette il prodotto sul mercato.

Da ultimo, il Parlamento europeo ha pubblicato una Risoluzione recante raccomandazioni alla Commissione europea su un regime di responsabilità civile per l'IA (di seguito anche "Risoluzione del 2020"). Tale Risoluzione contiene lo schema di una correlata Proposta di

---

[17] Cfr. COMMISSIONE EUROPEA, COM(2018) 246 final, *cit.*, pt. 6; COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., pp. 14 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 50 ss.; A. AMIDEI, *Intelligenza Artificiale*, cit., pp. 1723 ss.

[18] Cfr. PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica*, cit., «considerando» AI.

[19] Cfr. COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., pp. 4 ss.; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 47 ss., per un approfondimento. Sempre sulla normativa europea applicabile cfr., altresì, L. LIGUORI, in M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale*, cit., pp. 341 ss.; A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *NGCC*, 2012, da p. 494.

regolamento sulla responsabilità per il funzionamento dei sistemi di IA (di seguito "Schema di proposta di regolamento") [20].

Al riguardo, la fonte normativa regolamentare è stata pensata al fine di porre in essere una piena armonizzazione mediante una normativa uniforme di principio, tale da favorire lo sviluppo di un mercato unico digitale [21]. Il regolamento dovrebbe peraltro coordinarsi ed armonizzarsi con le normative testé menzionate ed in particolare con le direttive sui danni da prodotti difettosi e sulla sicurezza dei prodotti (*ultra*, § 8) [22].

La Risoluzione del 2020 e lo Schema di proposta di regolamento si fondano su una serie di risoluzioni, documenti e studi promossi dalle istituzioni europee negli ultimi anni.

Un rapido cenno, infine, andrà fatto rispetto alla ancor più recente Proposta di regolamento del Parlamento europeo e del Consiglio «che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione» ("AI Act" o "AIA") [23], predisposta dalla Commissione europea e che però si pone in parte al di fuori degli schemi tracciati dal Parlamento europeo.

La legislazione *in fieri* in tema di IA va poi inserita in un più ampio contesto di "costituzionalismo digitale" dell'Unione europea, in cui

---

[20] PARLAMENTO EUROPEO, *Regime di responsabilità civile per l'intelligenza artificiale. Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, (2020/2014(INL) (P9_TA-PROV(2020)0276) e relativo Allegato, contenente *Raccomandazioni dettagliate per l'elaborazione di un regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale*, nonché la *Proposta di regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale*.

[21] Cfr. PARLAMENTO EUROPEO, *Raccomandazioni dettagliate per l'elaborazione di un regolamento*, cit., principio n. 1.

[22] Questa raccomandazione è contestuale ad altri due risoluzioni del Parlamento europeo. Cfr. PARLAMENTO EUROPEO, *Relazione recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate* (2020/2012(INL)) (A9 – 0186/2020), 8 ottobre 2020, su cui si è basata la Proposta di regolamento della Commissione, di cui si accennerà *infra* nel § 8; PARLAMENTO EUROPEO, *Relazione sui diritti di proprietà intellettuale per lo sviluppo di tecnologie di intelligenza artificiale* (2020/2015(INI)) (A9- 0176/2020), che si propone di stabilire a chi appartenga la proprietà intellettuale di qualcosa sviluppato completamente dall'IA. Per un inquadramento sistematico più ampio, cfr. A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Milano, 2020, pur se antecedente alle citate proposte.

[23] COM(2021) 206 final, 21st April 2021.

oltre al GDPR, dovrebbero in futuro aggiungersi il *Data Governance Act*, il *Digital Markets Act* e il *Digital Services Act* [24].

L'indagine, allora, non può che partire dal testo della Risoluzione del 2017, per poi svilupparsi tramite l'analisi di alcuni dei principali documenti delle istituzioni europee che le hanno fatto seguito.

12.4. I principi guida su cui si fonda la Risoluzione del Parlamento europeo in tema di norme di diritto civile sulla robotica: prospettiva antropocentrica e fondata sui diritti e i valori fondamentali dell'UE

Nella Risoluzione del 2017, il Parlamento europeo afferma che la questione legata alla responsabilità civile per i danni causati dai robot «sia una questione fondamentale», da analizzare ed affrontare anche a livello di Unione europea «al fine di garantire il massimo livello di *efficienza*, *trasparenza* e coerenza nell'attuazione della *certezza giuridica* in tutta l'Unione europea nell'interesse tanto dei *cittadini* e dei *consumatori* quanto delle *imprese*» [25].

Già in questo punto della Risoluzione del 2017 sono individuabili almeno tre principi guida per la regolamentazione della responsabilità robotica: *efficienza*, *trasparenza* e *certezza giuridica*.

Altro profilo giuridicamente rilevante è il riferimento non solo ai *consumatori*, alla cui tutela è limitata la direttiva sui prodotti difettosi, ma anche ai *cittadini* e alle *imprese*.

– Quanto all'*efficienza*, i «considerando» E, F ed S della Risoluzione del 2017 tradiscono in qualche modo un'impostazione utilitaristica ma anche attenta a non tarpare la fisiologica *spinta* dell'UE verso

[24] L'espressione "costituzionalismo digitale" è di L. FLORIDI, *The European Legislation on AI: a Brief Analysis of its Philosophical Approach*, in *Phil. & Techn.*, 3 June 2021. Cfr. COMMISSIONE EUROPEA, *Proposal for a regulation of the European Parliament and the Council on European data governance (Data Governance Act)*, 25 November 2020, COM(2020) 767 final; COMMISSIONE EUROPEA, *Proposal for a regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, 15 December 2020, COM(2020) 842 final; COMMISSIONE EUROPEA, *Proposal for a regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, 15 December 2020, COM(2020) 825 final. Cfr., altresì, COMMISSIONE EUROPEA, *Fostering a European Approach to Artificial Intelligence*, 21 April 2021, (COM(3032) 205 Final).

[25] Cfr. PARLAMENTO EUROPEO, *Norme di diritto civile sulla robotica*, cit., pt. 49 (enfasi aggiunte).

l'innovazione tecnologica, con benefici per i cittadini (tra cui in particolare gli anziani e i malati), per l'occupazione e la sicurezza lavorativa, per il settore dei trasporti, manifatturiero, commerciale ed agricolo.

– Quanto alla *trasparenza*, il punto 12 della Risoluzione del 2017, incardinato nell'ambito dei «Principi etici», ne esplica il significato nel senso che (*i*) «dovrebbe sempre essere *possibile indicare la logica alla base di ogni decisione presa con l'ausilio dell'intelligenza artificiale* che possa avere un impatto rilevante sulla vita di una o più persone»; (*ii*) «debba sempre essere possibile ricondurre i calcoli di un sistema di intelligenza artificiale a una *forma comprensibile per l'uomo*»; (*iii*) «i robot avanzati dovrebbero essere dotati di una *"scatola nera" che registri i dati* su ogni operazione effettuata dalla macchina, compresi i passaggi logici che hanno contribuito alle sue decisioni» [26].

Al riguardo è chiaro il riferimento alla problematica degli sviluppi imprevedibili dell'algoritmo e del *black box algorithm*.

– Per quanto concerne la *certezza giuridica*, infine, (*a*) il «considerando» L della Risoluzione del 2017 afferma che «occorre chiarire la responsabilità giuridica per quanto concerne sia il *modello di impresa* sia le caratteristiche dei lavoratori, in caso di emergenza o qualora sorgessero problemi»; (*b*) il «considerando» M sottolinea che «la tendenza all'automazione esige che *i soggetti coinvolti nello sviluppo e nella commercializzazione di applicazioni dell'intelligenza artificiale integrino gli aspetti relativi alla sicurezza e all'etica fin dal principio*, riconoscendo pertanto che devono essere preparati ad accettare di essere legalmente responsabili della qualità tecnologica prodotta»; (*c*) il «considerando» S osserva che l'industria europea potrebbe trarre beneficio da una regolamentazione a livello di UE «che fornisca *condizioni prevedibili e sufficientemente chiare in base alle quali le imprese possano sviluppare applicazioni e pianificare i propri modelli commerciali su scala europea*, garantendo nel contempo che *l'Unione e i suoi Stati membri mantengano il controllo sulle norme regolamentari da impostare* e non siano costretti ad adottare e subire norme stabilite da altri, vale a dire quei paesi terzi che sono anche in prima linea nello sviluppo della robotica e dell'intelligenza artificiale» [27].

Se ne deduce che la *certezza giuridica* concerne, da un lato, la distribuzione della responsabilità tra diverse categorie di soggetti interessati (produttori, distributori, utilizzatori ecc.) e, dall'altro, la possibilità di

[26] Enfasi aggiunte.

[27] Tutte enfasi aggiunte.

sperimentare, produrre e commercializzare nuove tecnologie in un ambiente normativo protetto e armonizzato.

Ancora, la *certezza giuridica* rileva di per sé come strumento di autonomia e di protezione – per cittadini, imprese e istituzioni europee e degli Stati membri – dai principali *players* mondiali in campo di robotica e IA, la maggior parte dei quali, per natura imprenditoriale o per forme di Stato e di governo, possono insidiare il fondamento democratico dell'evoluzione civile e sociale.

– Ad ogni modo, i principi di *efficienza*, *trasparenza* e *certezza giuridica* sembrano disvelare il fondamento originario di comunità economica, ancor prima che di unione sociale, dell'Unione europea.

Ciò nondimeno si crede opportuno precisare da subito che, in una scala di valori – e in una prospettiva *unionale*, anziché comunitaria –, detti principi, seppure maggiormente prossimi alle problematiche segnalate, non debbano essere posti al vertice della regolamentazione in tema di responsabilità civile sulla robotica.

Al riguardo, proprio dall'analisi della stessa Risoluzione del 2017 si evince che (*i*) il «considerando» O pone attenzione a che «gli sviluppi nel campo della robotica e dell'intelligenza artificiale possono e dovrebbero essere pensati in modo da preservare la *dignità*, *l'autonomia e l'autodeterminazione degli individui*»; (*ii*) il punto 3 sottolinea che «lo sviluppo della tecnologia robotica dovrebbe mirare a *integrare le capacità umane e non a sostituirle*», così che «sia fondamentale, nello sviluppo della robotica e dell'intelligenza artificiale, garantire che *gli uomini mantengano in qualsiasi momento il controllo sulle macchine intelligenti*»; (*iii*) il punto 13, anch'esso incardinato nei «Principi etici», precisa che il quadro etico di orientamento dovrebbe essere basato, in primo luogo, sulle cc.dd. "leggi di Asimov", ossia sui «principi di beneficienza, non maleficenza, autonomia e giustizia» nonché, in secondo luogo e soprattutto, «sui *principi sanciti all'art. 2 del trattato sull'Unione europea* e nella *Carta dei diritti fondamentali dell'Unione europea* – quali la *dignità umana*, l'*uguaglianza*, la *giustizia* e l'*equità*, la *non discriminazione*, il consenso informato, la vita privata e familiare e la protezione dei dati, così come sugli *altri principi e valori alla base del diritto dell'Unione* come la *non stigmatizzazione*, la trasparenza, l'*autonomia*, la *responsabilità individuale e sociale* – e sulle *pratiche e i codici etici esistenti*» [28].

[28] Tutte enfasi aggiunte. E cfr. ora, COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit., p. 2, pp. 10 ss.

Al riguardo, il riferimento alle "leggi di Asimov" può far sorridere, trovandosi agevolmente i principi ivi contenuti nei principi fondamentali di tutti gli ordinamenti giuridici evoluti [29].

Gli altri riferimenti citati consentono invece di anticipare sin d'ora che l'ordinamento giuridico dell'Unione europea si caratterizza proprio per la sua *prospettiva antropocentrica* della regolamentazione sull'IA, attenta prima di tutto a tutelare *i diritti ed i valori fondamentali*, su cui si costruisce l'Unione e che accomunano gli Stati membri, nonché a delimitare l'IA quale *strumento d'integrazione* delle capacità umane – tra cui la capacità di autodeterminazione – e *mai di sostituzione* delle stesse.

Si anticipa altresì che l'esplicito riferimento alla Carta dei diritti fondamentali dell'Unione europea e agli «altri principi e valori alla base del diritto dell'Unione» è rilevante per orientare un'interpretazione ampia dell'impostazione appena delineata.

12.5. Il rischio "etico" del dominio dell'IA sull'essere umano. L'approccio procedimentale delle linee guida etiche dell'HLEG

Si è accennato in apertura al rischio di parificare in qualche modo esseri umani e sistemi di IA nonché di comprimere eccessivamente gli affari e le attività umane se non addirittura l'essenza degli esseri umani.

Concentrandosi su un'impresa organizzata in forma societaria, basti pensare alle difficoltà che possono incontrare gli amministratori di una società che adoperi un sistema di IA per ricevere una consulenza in merito ad una "scelta" d'impresa decisiva: in tale ipotesi gli amministratori "consenzienti" potrebbero appiattirsi rispetto all'*output* del sistema, confidando in un'alta aspettativa di *accuracy*; d'altro canto, gli amministratori "dissenzienti" incontrerebbero notevoli difficoltà nel motivare in maniera dialettica le ragioni della loro differente opinione.

Va pertanto accolta con favore la conferma della Commissione europea verso il sostegno a un approccio antropocentrico nei confronti

[29] Sulle tre "leggi di Asimov" cfr. M. BASSINI, in M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale*, cit., pp. 339 s.; G. LEMME, *Gli* smart contracts *e le tre leggi della robotica*, in *AGE*, 1/2019, da p. 19; D. ETZERI, *Liability for operation and damages caused by artificial intelligence – with a short outlook to online games*, in 153 *Studia Iuridica Auctoritate Universitatis Pecs Publicata* (2015), da p. 57.

dell'IA. Al riguardo, detta istituzione ha precisato che la *fiducia* verso l'IA costituisce una condizione indispensabile: in particolare «l'intelligenza artificiale non è fine a se stessa, ma *è uno strumento a servizio delle persone* che ha come fine ultimo quello di migliorare il benessere degli esseri umani» [30].

La strumentalità dell'IA all'uomo aiuta a porre quest'ultima altresì in una prospettiva funzionale al rispetto della dignità umana, anche quale capacità autodeterminazione dell'individuo [31].

La questione sconfina nell'etica e proprio le recenti *Ethic Guidelines for Trustworthy AI* pubblicate dall'*Independent High-Level Expert Group on Artificial Intelligence* (HLEG) forniscono preziosi spunti per una corretta soluzione dei problemi enunciati [32].

Segnatamente le menzionate linee-guida declinano i requisiti del *rispetto dell'autonomia umana*; della *fairness*; dell'*explicability*; dell'*intervento e* della *sorveglianza umani*; della *robustezza*; della *riservatezza* e della *governance dei dati*; della *diversità, non discriminazione* ed *equità*; del *benessere sociale e ambientale*.

Per ciò che qui interessa, riguardo al primo requisito, secondo l'HLEG i sistemi di IA non dovrebbero subordinare, forzare, sviare, manipolare, condizionare gli esseri umani in maniera ingiustificabile. Al contrario tali sistemi dovrebbero *aumentare, completare e rafforzare* le capacità cognitive, sociali e culturali degli esseri umani [33].

Il requisito della *fairness* (tradotto con l'espressione «equità»), (*i*) nell'accezione *sostanziale* si esplica nell'impegno a garantire una distribuzione giusta ed equa di costi e di benefici, in ossequio al principio di proporzionalità, nonché a garantire che sia gli individui sia i gruppi

---

[30] Cfr. COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, COM(2019) 168 final, Bruxelles, 8 aprile 2019, p. 2 (enfasi aggiunta).

[31] Cfr. R. MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr.*, 2019, da p. 861, pp. 868 s., secondo cui «Garantire che l'uomo possa comprendere la macchina persegue infatti una palese finalità: assicurare che l'intelligenza artificiale sia – e rimanga – strumentale rispetto a quella umana. Ciò attiene al nucleo essenziale del concetto filosofico e del principio giuridico della dignità dell'uomo». Sia consentito, inoltre, il rinvio a F. PACILEO, *L'uomo al centro. IA tra etica e diritto nella responsabilità d'impresa*, in *Etica digitale. Verità, responsabilità e fiducia nell'era delle macchine intelligenti*, a cura di M. Bertolaso, G. Lo Storto, Roma, 2021, da p. 83.

[32] Cfr. HLEG, *Ethics Guidelines for Trustworthy AI*, Brussels, 8 aprile 2019, reperibile sul sito *www.europa.eu*.

[33] Cfr. HLEG, *op. cit.*, p. 12, p. 16.

non patiscano distorsioni inique, discriminazioni e stigmatizzazioni; (*ii*) nella sua versione *procedurale*, attiene alla capacità di contestare, di cercare una soluzione effettiva contro, gli *output* prodotti da sistemi di IA: a tal fine, il relativo processo decisionale dovrebbe essere esplicabile. Il contesto di riferimento della *fairness sostanziale* è evidentemente quello già menzionato della *trasparenza*, incardinato nei principi etici [34].

E proprio nel comune senso della trasparenza, il requisito dell'*explicability* prevede che i processi decisionali (*rectius*, di funzionamento dell'IA) dovrebbero essere trasparenti, che le capacità e le funzioni dei sistemi di IA dovrebbero essere apertamente comunicate, ed infine che gli *output* siano il più possibile esplicitabili e comprensibili per coloro che vengono coinvolti, in modo che una decisione possa essere debitamente contestata. In particolare, nel caso dei *black box algorithm* si potrebbero richiedere altre misure di *explicability*, quali ad esempio la tracciabilità, la controllabilità, la verificabilità e la trasparenza nelle comunicazioni sui sistemi nel senso di assicurare che detti sistemi rispettino nel complesso i diritti fondamentali [35].

Le linee-guida hanno poi ben presente il potenziale *trade-off* tra *explicability* e *accuracy* e cercano di risolverlo nel senso che la prima può essere sacrificata a favore della seconda nella misura in cui i conseguenti benefici prevalgano sui singoli prevedibili rischi [36].

Inoltre, l'IA deve essere *robusta* nel senso che gli algoritmi debbono essere idonei a far fronte a errori o incongruenze durante tutte le fasi del ciclo di vita del sistema di IA. Detti algoritmi devono essere altresì capaci di gestire risultati sbagliati ed essere resilienti agli attacchi palesi e occulti tesi alla manipolazione dei dati o degli algoritmi. Deve essere infine garantita l'esistenza di un piano di emergenza. Gli *output*,

---

[34] Cfr. HLEG, *op. cit.*, pp. 12 s. Cfr., altresì, KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YUT, *Accountable Algorithms*, cit., p. 642 e p. 685, ove si distingue tra *individual fairness* e *group fairness* e inoltre si aggiunge che «a fair process will give similar participants a similar probability of receiving each possible outcome».

[35] Cfr. HLEG, *op. cit.*, p. 13; COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., p. 10, secondo cui «Non è necessario che gli esseri umani comprendano ogni singola fase del processo decisionale, ma dato che gli algoritmi di intelligenza artificiale sono sempre più avanzati e sono utilizzati in settori critici, è fondamentale che gli esseri umani possano capire come il sistema ha preso le decisioni algoritmiche».

[36] Cfr. HLEG, *op. cit.*, p. 17.

poi, devono essere accurati, o almeno rispecchiare correttamente il loro livello di accuratezza, e i risultati devono essere riproducibili [37].

I sistemi di IA dovrebbero inoltre contenere meccanismi di *sicurezza fin dalla progettazione* (*by design*), per garantire che siano sicuri in modo verificabile in ogni fase. Ciò comprende anche la possibilità di ridurre al minimo e, ove possibile, rendere reversibili gli effetti involontari o gli errori del funzionamento del sistema. È opportuno, pertanto, prevedere processi in grado di chiarire e valutare i potenziali rischi associati all'uso dei sistemi di IA nei vari settori di applicazione [38].

Strettamente interconnessa a tutti questi requisiti è poi la *sorveglianza umana sin dalla progettazione*.

Secondo la Commissione europea a tale requisito può essere rispettato organizzando meccanismi di *governance* secondo tre possibili approcci: (*a*) con intervento umano ["*human-in-the-loop*" (HITL)], che contempla l'intervento umano in ogni ciclo decisionale del sistema, anche se la Commissione stessa avverte che ciò «in molti casi non è né possibile né auspicabile»; (*b*) con supervisione umana [("h*uman-on-the-loop*" (HOTL)], che implica la capacità di intervento umano durante il ciclo di progettazione del sistema e di monitoraggio del funzionamento del sistema; (*c*) con controllo umano [("*human-in-command*" (HIC)], che include sia la capacità di sorvegliare l'attività complessiva del sistema di IA (tra cui il più ampio impatto economico, sociale, giuridico ed etico) sia la capacità di decidere quando e come utilizzare il sistema in una particolare situazione [39].

Anche per ciò che concerne *la riservatezza e la governance dei dati* le Linee-guida e la Commissione delineano un procedimento per la raccolta e l'elaborazione dei *big data* e per gestire il rischio di discriminazioni. In particolare, la Commissione osserva che deve essere garantita l'integrità dei dati. A tal fine, i processi e i set di dati utilizzati devono essere testati e documentati in ogni fase, ed in particolare nella pianificazione, nell'addestramento, nei test e nella diffusione. Ciò dovrebbe valere altresì per i sistemi di IA che non sono stati sviluppati *in house* ma acquisiti altrove [40].

---

[37] Cfr. HLEG, *op. cit.*, pp. 16 s.; COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit., p. 5.

[38] Cfr. HLEG, *op. cit.*, pp. 16 s.; COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit., p. 5.

[39] Cfr. COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit., p. 5, testo e nt. 13; HLEG, *op. cit.*, p. 16.

[40] Cfr. HLEG, *op. cit.*, p. 17; COMMISSIONE EUROPEA, *Creare fiducia nell'intelligenza artificiale*

La *fairness*, la *sorveglianza umana* e la *riservatezza e governance dei dati*, infine, si coordinano per *evitare discriminazioni e disparità di trattamento*, dovute all'internalizzazione, anche involontaria, di pregiudizi all'interno degli algoritmi e dei sistemi di IA [41].

Ad una visione d'insieme, le menzionate Linee-guida si pongono in una prospettiva che appare coerente ad un'impostazione di ordine *procedimentale*, impostazione, si anticipa, che potrebbe risultare quale migliore soluzione per la regolamentazione e gestione dei rapporti tra innovazione tecnologica e diritto dell'impresa organizzata in forma societaria.

Più in generale, l'opzione del legislatore verso la trasparenza e la sicurezza degli algoritmi *fin dalla progettazione* implica una scelta diversa rispetto alla *neutralità tecnologica* (dal punto di vista del programmatore e del produttore nonché dello stesso sistema di AI), scelta che certamente richiede una seria riflessione circa i conseguenti possibili costi e benefici.

12.5.1. Necessità di un'organizzazione e di professionalità. Probabile impiego del metodo economico. Ergo, importanza dell'impresa

E proprio la complessità applicativa di dette Linee-guida e il loro approccio procedimentale implicano un'*organizzazione*, poi un'organizzazione *adeguata*.

Ne deriva che, lasciando da parte i soggetti di natura pubblicistica tra coloro che in qualche modo hanno a che fare con l'IA, i soggetti privati devono avere un'organizzazione che difficilmente può essere sostenuta da un metodo diverso da quello del rispetto del principio di *economicità*.

Ecco allora che, non potendo mancare il requisito della *professionalità*, la maggior parte dei soggetti privati che operano con l'IA saranno organizzati in forma di *impresa*.

Ciò posto, occorre distinguere tra imprese che *producono* sistemi di IA e imprese che *utilizzano* tali sistemi per effettuare "scelte" imprenditoriali strategiche e suscettibili di incidere su diritti fondamentali di soggetti che per varie ragioni vi si rapportano. Si pensi, per

antropocentrica, cit., pp. 5 s.

[41] Cfr. HLEG, *op. cit.*, pp. 18 s.

semplificare, da un lato a una start-up innovativa che produce ovvero offre al mercato un certo sistema di IA e, dall'altro, a una s.p.a. che utilizzi detto sistema per ottenere informazioni decisive, se non una vera propria consulenza, in merito a una scelta strategica (es., investire o non in una operazione complessa oppure liquidare o meno la società).

Al riguardo, in considerazione dell'orizzonte limitato di controllo sui sistemi di IA, di cui si è detto, occorre comprendere come possa distribuirsi una responsabilità per un suo cattivo funzionamento nell'ambito di una così complessa catena di valore.

12.6. Il Libro bianco sull'intelligenza artificiale e l'approccio basato sul rischio

Ulteriori spunti sul tema della responsabilità da funzionamento dei sistemi di IA si ricavano dal Libro bianco sull'intelligenza artificiale [42].

In tale documento la Commissione europea riprende il percorso istituzionale finora descritto, in merito alla regolamentazione dell'IA.

Limitatamente a ciò che qui interessa, si afferma che le maggiori lacune normative si riscontrano sul tema della trasparenza, della tracciabilità e della sorveglianza umana, nonché sulla difficoltà di distinguere le responsabilità del produttore, dell'utilizzatore per i danni derivanti dalla programmazione o dall'apprendimento/uso dell'algoritmo.

Viene inoltre promosso *un approccio basato sul rischio* nel duplice significato di (*i*) prevedere una regolamentazione più stringente nei settori con rischi significativi o laddove siano gli stessi sistemi di IA a generare rischi significativi; (*ii*) distribuire la responsabilità agli operatori che si trovano nella posizione migliore per affrontare i rischi potenziali.

Riguardo al primo profilo, si può innanzi tutto segnalare la difficoltà di individuare criteri oggettivi di distinzione fra situazioni a rischio significativo e situazioni meno rischiose [43], rinviando poi allo

[42] Cfr. COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, cit.

[43] Su tale distinzione cfr. EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence and Other Emerging Digital Technologies*, commissionato dalla Commissione europea, 2019, pp. 39 ss.; critico verso i suddetti criteri di distinzione A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 77 ss.

Schema di proposta di regolamento e alla Proposta di regolamento (*ultra*, §§ 8 e 9).

Riguardo al secondo, si rinvia a quanto si dirà nei prossimi paragrafi (*ultra*, §§ 7 e 8).

12.7. Principali raccomandazioni della Risoluzione del 2017 del Parlamento europeo, riguardo allo specifico tema della responsabilità civile sulla robotica

Quanto alle principali raccomandazioni fornite dalla Risoluzione del 2017 alla Commissione europea *stricto sensu* riferite alla responsabilità civile sulla robotica (punti 49-59), fissati i principi fondamentali di riferimento (*supra*, § 4), vale la pena di evidenziare i principali profili che emergono dalla lettura della Risoluzione del 2017.

– Così, il punto 50 fa riferimento alla necessità di «una maggiore comprensione per trovare il terreno comune necessario ai fini dell'*attività congiunta umano-robotica* e che dovrebbe basarsi su due relazioni interdipendenti essenziali, quali la *prevedibilità* e la *direzionalità*». Sempre il punto 50 precisa che «queste due relazioni interdipendenti sono cruciali per determinare quali informazioni è opportuno che gli umani e i robot condividano e come individuare una base comune tra umani e robot che consenta un'efficace *azione congiunta umano-robotica*» [44]. L'esplicito riferimento all'*attività/azione congiunta umano-robotica* appare ispirato alla dottrina che, si crede, ad oggi ha fornito alcuni tra gli spunti più interessanti in materia di responsabilità civile sulla robotica [45]. Detta raccomandazione si colloca evidentemente nel solco del principio della *sorveglianza umana* (*supra*, § 5).

– Ancora la Risoluzione del 2017 raccomanda al punto 52 che la responsabilità civile «per danni causati dai robot diversi dai danni alle cose», non dovrebbe limitare (*i*) il tipo e l'entità dei danni risarcibili; (*ii*) le forme di risarcimento che potrebbero essere offerte alla parte lesa «per il semplice fatto che il danno è provocato da un soggetto non umano».

In buona sostanza tale previsione suggerisce di porre al riparo la parte lesa da eventuali lacune normative che non permettano di individuare in modo chiaro il soggetto responsabile e la ripartizione delle

[44] Enfasi aggiunte.

[45] Il riferimento è a G. TEUBNER, *Digitale Rechtssubjekte?*, cit.

responsabilità. Qui il riferimento va al summenzionato principio di *certezza giuridica* (*supra*, § 4).

– Il Parlamento europeo circoscrive la futura regolamentazione della responsabilità *de qua* all'approccio della «responsabilità oggettiva» o a quello della «gestione dei rischi» (punto 53), osservando al riguardo che (*a*) «la responsabilità oggettiva richiede una semplice prova del danno avvenuto e l'individuazione di un nesso di causalità tra il funzionamento lesivo dei robot e il danno subito dalla parte lesa» (punto 54); (*b*) «l'approccio di gestione dei rischi non si concentra sulla persona "che ha agito con negligenza" in quanto responsabile a livello individuale bensì sulla persona che, in determinate circostanze, è in grado di minimizzare i rischi e affrontare l'impatto negativo» (punto 55).

L'approccio di gestione dei rischi (*risk management approach* o RMA) è stato rielaborato dalla Commissione nel Libro bianco, ove si precisa che «in un futuro quadro normativo ciascun obbligo debba essere stabilito a carico dell'operatore o degli operatori che si trovano nella posizione migliore per affrontare eventuali rischi potenziali».

– Soprattutto il RMA impone la distinzione fra (*a*) una responsabilità connessa alle «competenze derivanti dalla "formazione" di un robot» e (*b*) una responsabilità invece connessa alle «competenze che dipendono strettamente dalle sue [del robot, n.d.r.] abilità di apprendimento» (punto 56).

Al riguardo, se nell'ambito della formazione si possono individuare profili di negligenza o di minimizzazione dei rischi da parte dei programmatori, sembra invece più arduo delineare una correlazione fra una condotta quanto meno colposa e le «abilità di apprendimento» del robot. Qui il problema è ancora una volta quello degli sviluppi imprevedibili dell'algoritmo, del *black box algorithm* unitamente a quello della certezza giuridica.

In ogni caso, sempre nel medesimo paragrafo il Parlamento europeo precisa che «una volta individuati i soggetti responsabili in ultima istanza, la loro responsabilità dovrebbe essere *proporzionale* all'effettivo livello di istruzioni impartite ai robot e al grado di autonomia di quest'ultimo, di modo che quanto maggiore è la capacità di apprendimento o l'autonomia di un robot e quanto maggiore è la durata della formazione di un robot, tanto maggiore dovrebbe essere la responsabilità del suo formatore» [46].

[46] Enfasi aggiunta.

Su questo aspetto, soprattutto per i sistemi di IA e/o robotici che sono il frutto di una catena complessa di valore, è difficile individuare colui che si trova nella posizione migliore per gestire i rischi potenziali. A tal proposito, la Commissione europea promuove il principio della "responsabilità condivisa". In buona sostanza occorrono disposizioni normative esplicite che impongano la cooperazione tra gli operatori economici nella catena di approvvigionamento e gli utilizzatori, al fine di creare certezza giuridica, anche in termini di *accountability*. In base a tale principio ogni partecipante alla catena di valore avente un impatto sulla sicurezza del prodotto (ad esempio i produttori di *software*) e sugli utilizzatori (ad esempio, se modificano il prodotto) dovrebbe assumersi la propria responsabilità e fornire al partecipante successivo nella catena le informazioni e le misure necessarie [47].

– Il Parlamento europeo osserva che, *de iure condito* e allo stato dell'arte, «la responsabilità deve essere imputata ad un essere umano e non a un robot» (punto 56).

Tale assunto dovrebbe essere scontato ma, alla luce della possibilità di attribuire *de iure condendo* una responsabilità ai robot più autonomi, è bene tenere fermo questo punto di partenza d'indagine.

12.8. La Risoluzione del Parlamento europeo sul regime di responsabilità civile per l'intelligenza artificiale e l'allegato Schema di proposta di regolamento

Si è accennato precedentemente alla Risoluzione del 2020 del Parlamento europeo e all'allegato Schema di proposta di regolamento (*supra*, §§ 2 e 3).

– Al riguardo, il Parlamento europeo innanzi tutto sembra escludere l'ipotesi della "personalità elettronica", dallo stesso formulata, nonché sottolineare la strumentalità dei sistemi di IA all'uomo. Il «considerando» n. 6 dello Schema di proposta di regolamento prevede infatti che «Qualsiasi cambiamento richiesto riguardante il quadro giuridico esistente dovrebbe iniziare con il chiarimento che i *sistemi di IA*

[47] Cfr. COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., pp. 12 s. Cfr., altresì, G. COMANDÉ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *AGE*, 1/2019, da p. 169.

non possiedono né una personalità giuridica né una coscienza umana e che *il loro unico compito consiste nel servire l'umanità*» [48].

È questo un punto di riferimento davvero importante per uno studio sulle implicazioni giuridiche dell'impiego dei sistemi di IA.

– L'art. 3 dello Schema di proposta di regolamento *definisce* poi (*i*) *il sistema di IA* come «un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici»; (*ii*) *il sistema di IA "autonomo"* come quello che «che opera interpretando determinati dati forniti e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione».

Ad una prima lettura, colpisce subito la puntualizzazione circa il comportamento del sistema autonomo di IA comunque connesso al perseguimento di *obiettivi ed interessi di un soggetto, altro*, nonché alle *scelte operate dallo sviluppatore in sede di progettazione*. Ciò evidenzia la descritta prospettiva antropocentrica. E vale la pena di anticipare che, significativamente, l'art. 3 della proposta di AIA, sempre nel definire un "sistema di intelligenza artificiale", fa riferimento a «una determinata serie di obiettivi *definiti dall'uomo*» [49].

– Lo Schema di proposta di regolamento pone anch'esso attenzione alla distinzione tra *i diversi soggetti che compongono la catena di valore dei sistemi di IA* – produttore, operatori, persone interessate e qualsiasi terzo coinvolto [50] – e dà seguito alla condivisione delle responsabilità di tali soggetti, promossa nel Libro bianco, secondo il criterio del RMA.

In particolare, sempre nell'ambito delle definizioni di cui all'art. 3, si distingue (*a*) la nozione di "operatore di front-end", quale «persona fisica o giuridica *che esercita un certo grado di controllo su un rischio connesso* all'operatività e al funzionamento del sistema di IA e che *beneficia* del suo funzionamento»; (*b*) la nozione di "operatore di back-end",

[48] Enfasi aggiunta.

[49] Enfasi aggiunta.

[50] Cfr. PARLAMENTO EUROPEO, *Raccomandazioni dettagliate per l'elaborazione di un regolamento*, cit., principio n. 2; nonché l'art. 3 dello Schema di proposta di regolamento, ove si definisce "persona interessata" «qualsiasi persona che subisca i danni o pregiudizi causati da un'attività, dispositivo o processo fisico o virtuale guidato da un sistema di IA e che non sia l'operatore di tale sistema».

quale «persona fisica o giuridica che, su base continuativa, *definisce le caratteristiche della tecnologia e fornisce i dati e il servizio di supporto* di back-end essenziale e pertanto *esercita anche un elevato grado di controllo su un rischio connesso* all'operatività e al funzionamento del sistema di IA» [51].

Entrambe le fattispecie di "operatore" sono accomunate dall'"esercizio" di un «controllo su un rischio connesso all'operatività e al funzionamento del sistema di IA»: un «certo grado di controllo» per l'operatore di front-end e un «elevato grado di controllo» per l'operatore di back-end.

E sempre l'art. 3 definisce il "controllo" come «qualsiasi *azione di un operatore* che *influenza* il funzionamento di un sistema di IA e quindi *il grado in cui l'operatore espone terzi ai potenziali rischi associati all'operatività e al funzionamento del sistema di IA*; tali azioni possono avere un impatto sul funzionamento *in qualsiasi fase* determinando gli input, gli output o i risultati, o possono modificare funzioni o processi specifici all'interno del sistema di IA; *il grado* in cui tali aspetti del funzionamento del sistema di IA sono determinati dall'azione *dipende dalla misura in cui l'operatore può influenzare il rischio* connesso all'operatività e al funzionamento del sistema di IA» [52].

In particolare, il «considerando» n. 10 dello Schema di proposta di regolamento puntualizza che «Maggiore è il grado di sofisticazione e di autonomia di un sistema, maggiore sarà l'impatto dato dal fatto di definire e influenzare gli algoritmi, ad esempio attraverso continui aggiornamenti».

Già da questa prima analisi del testo emerge subito una stretta correlazione – una sorta di "spina dorsale" della normativa *in fieri* – tra *operatori-controllo-grado di rischio*.

– Il Capo IV dello Schema di proposta di regolamento (artt. 10 ss.) disciplina poi la *ripartizione delle responsabilità* dei soggetti facenti parte della catena di valore, secondo il criterio della *solidarietà* tra gli operatori ma anche di un *regresso proporzionale* al grado di controllo sul rischio.

Ancora nell'ambito della responsabilità condivisa, qualora non sia possibile o sia eccessivamente oneroso individuare il singolo soggetto

---

[51] Enfasi aggiunte. Per un approfondimento sulla nozione di "operatore", cfr. EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 39 ss.

[52] Enfasi aggiunte.

responsabile, al punto n. 7 della Risoluzione del 2020 si osserva che «è tuttavia possibile aggirare tale ostacolo considerando responsabili le varie persone nella catena del valore che creano il sistema di IA, ne eseguono la manutenzione o ne controllano i rischi associati».

L'impostazione dello Schema di proposta di regolamento appare paragonabile a quella adottata nella direttiva sulla responsabilità per danno da prodotti difettosi. Tale ultima direttiva, peraltro è più volte presa in considerazione dal Parlamento europeo (unitamente alla direttiva sulla sicurezza generale dei prodotti), che suggerisce anche di aggiornarla all'evoluzione delle tecnologie digitali e di armonizzarla con il regolamento *in fieri*. In particolare, il ruolo dell'*operatore* (*rectius*, degli operatori) quale soggetto *accountable* è comparabile a quello del *produttore* nell'ambito delle direttive sui danni da prodotti difettosi e sulla sicurezza dei prodotti [53].

– In ossequio al RMA vengono delineate distinte *fattispecie di sistemi di IA*, a cui poi si dovrebbero applicare distinte discipline di responsabilità: occorre invero individuare se il *sistema di IA* sia *"ad alto rischio" o meno*.

Sempre l'art. 3 dell Schema di proposta di regolamento definisce "ad alto rischio" «un potenziale significativo in un sistema di IA che opera in modo autonomo di causare danni o pregiudizi a una o più persone in modo casuale e che va oltre quanto ci si possa ragionevolmente aspettare; l'importanza del potenziale dipende dall'interazione tra la gravità dei possibili danni o pregiudizi, dal grado di autonomia decisionale, dalla probabilità che il rischio si concretizzi e dalla modalità e dal contesto di utilizzo del sistema di IA».

---

[53] Cfr. PARLAMENTO EUROPEO, *Regime di responsabilità civile per l'intelligenza artificiale*, cit., «considerando» n. 8, ove (*i*) si esorta la Commissione europea «a valutare se la direttiva sulla responsabilità per danno da prodotti difettosi debba essere trasformata in un regolamento, a chiarire la definizione di "prodotti" determinando se i contenuti e i servizi digitali rientrino nel suo ambito di applicazione, nonché a esaminare l'adeguamento di concetti quali "pregiudizio", "difetto" e "produttore"»; (*ii*) si esprime il parere «che, ai fini della certezza giuridica nell'intera Unione, in seguito alla revisione della direttiva sulla responsabilità per danno da prodotti difettosi, il concetto di "produttore" dovrebbe includere i produttori, gli sviluppatori, i programmatori, i prestatori di servizi e gli operatori di back-end». Cfr., altresì, COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, cit., pp. 17 s.; EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 55, circa la responsabilità solidale della *commercial or technological unit*.

Riguardo all'*importanza del potenziale di danni e pregiudizi*, il «considerando» n. 13 della medesimo Schema precisa i criteri con cui può individuarsi (*a*) il *livello di gravità dei danni o pregiudizi*, i cui fattori rilevanti sono «l'entità del danno potenziale derivante dal funzionamento sulle persone interessate, inclusi in particolare gli effetti sui diritti fondamentali, il numero di persone interessate, il valore totale del danno potenziale e il pregiudizio inflitto alla società nel suo insieme»; (*b*) *la probabilità che il danno o il pregiudizio si verifichi*, i cui fattori rilevanti sono «il ruolo dei calcoli algoritmici nel processo decisionale, la complessità della decisione e la reversibilità degli effetti; (*c*) *la modalità di utilizzo*, i cui fattori rilevanti sono «il contesto e il settore in cui opera il sistema di IA, eventuali effetti giuridici o reali su diritti importanti della persona interessata tutelati dalla legge e l'eventuale e ragionevole possibilità di evitare gli effetti».

Ad ogni modo, l'art. 4.2 dello Schema di proposta di regolamento prevede un *elenco* dei sistemi di IA "ad alto rischio" e dei settori fondamentali in cui essi vengono utilizzati. Si conferisce inoltre alla Commissione europea il potere di *aggiornare* l'elenco, anche a cadenza periodica, (*i*) inserendo nuovi tipi di sistemi di IA "ad alto rischio" e settori fondamentali in cui vengono utilizzati; (*ii*) eliminando tipi di sistemi di IA non più qualificabili "ad alto rischio"; (*iii*) modificando i settori fondamentali per i sistemi di IA "ad alto rischio" esistenti.

– Orbene, riguardo alla *disciplina della responsabilità*, per i sistemi di IA "ad alto rischio" lo Schema di proposta di regolamento prevede la *responsabilità oggettiva* dell'operatore in controllo (art. 4), laddove per gli altri sistemi di IA è prevista invece la *responsabilità* per colpa, *aggravata* dall'inversione dell'onere probatorio (art. 8).

In ogni caso, l'approccio è legato all'immissione di un *rischio* nel mercato e/o tra il pubblico ed alla capacità o meno di controllarlo [54].

Riguardo alla responsabilità oggettiva è individuato il limite della *forza maggiore* (art. 10.3).

Per quanto concerne la responsabilità aggravata, invece, l'*inversione dell'onere probatorio* impone all'operatore di dimostrare (*a*) che il

[54] Cfr. il «considerando» n. 8 dello Schema di proposta di regolamento, ove si legge che «chiunque crei un sistema di IA, ne esegua la manutenzione, lo controlli o interferisca con esso dovrebbe essere chiamato a rispondere del danno o pregiudizio che l'attività, il dispositivo o il processo provoca. Ciò discende da concetti di giustizia generali e ampiamente accettati in materia di responsabilità, secondo i quali la persona che crea o mantiene un rischio per il pubblico è responsabile se il rischio causa un danno o un pregiudizio e pertanto dovrebbe minimizzarlo ex ante o risarcirlo ex post».

sistema di IA si è attivato senza che egli ne fosse a conoscenza e sono state adottate tutte le misure ragionevoli e necessarie per evitare tale attivazione al di fuori del suo controllo, o (*b*) che è stata rispettata la dovuta diligenza, o (*c*) la forza maggiore (art. 8.2).

Segnatamente, l'*obbligo di diligenza* è connesso (*i*) alla selezione di un sistema di IA idoneo al compito e alle competenze; (*ii*) alla debita messa in funzione del sistema di IA; (*iii*) al monitoraggio delle attività e al mantenimento dell'affidabilità operativa mediante la periodica installazione di tutti gli aggiornamenti disponibili.

Nel «considerando» n. 18 dello Schema di proposta di regolamento, poi, si aggiunge che «La diligenza che ci si può attendere da un operatore dovrebbe essere commisurata i) alla natura del sistema di IA, ii) al diritto giuridicamente tutelato potenzialmente interessato, iii) al danno o pregiudizio potenziale che il sistema di IA potrebbe causare e iv) alla probabilità di tale danno».

Il medesimo «considerando» contiene due criteri *presuntivi*, rispettivamente afferenti (*a*) la *diligenza* richiesta *durante il funzionamento* del sistema di IA, la cui sussistenza si dovrebbe presumere «laddove l'operatore possa dimostrare di avere effettivamente e regolarmente monitorato il sistema di IA durante il funzionamento e di avere notificato al costruttore le possibili irregolarità riscontrate nel corso del funzionamento»; (*b*) la *diligenza* richiesta riguardo al *mantenimento dell'affidabilità operativa* del sistema di IA, la cui sussistenza si dovrebbe presumere «laddove [l'operatore, n.d.a.] abbia installato tutti gli aggiornamenti disponibili forniti dal produttore del sistema di IA».

Sempre il «considerando» n. 18 puntualizza che «Poiché il livello di sofisticazione degli operatori può variare a seconda che si tratti di semplici consumatori o professionisti, è opportuno adeguare di conseguenza gli obblighi di diligenza».

Tornando alla distribuzione delle responsabilità tra i soggetti coinvolti, il «considerando» n. 11 dello Schema di proposta di regolamento prevede che l'*utilizzatore* di un sistema di IA coinvolto in un evento dannoso dovrebbe essere qualificato *responsabile* a norma del regolamento «*solo laddove si qualifichi anche come operatore*. In caso contrario, l'entità del contributo al rischio da parte dell'utente, per negligenza grave o intenzionale, potrebbe comportare la responsabilità *per colpa* dell'utente nei confronti del ricorrente». In buona sostanza, l'utilizzatore-operatore dovrebbe essere assoggettato a un regime di responsabilità oggettiva o aggravata – a seconda che controlli un sistema di IA

"ad alto rischio" o meno – laddove l'utilizzatore-non operatore dovrebbe essere in qualche modo tutelato mediante assoggettamento ad un regime di responsabilità circoscritto alla colpa grave o al dolo.

Vengono poi fissati *massimali* per i risarcimenti e *prescrizioni ad hoc*.

Anche in correlazione agli accennati massimali, è prevista una disciplina di *assicurazione obbligatoria* quanto meno per gli operatori dei sistemi di IA "ad alto rischio".

Orbene, riprendendo l'esemplificazione precedentemente effettuata (*supra*, § 6), la start-up innovativa che produce ovvero offre al mercato un certo sistema di IA potrebbe essere agevolmente qualificata come persona giuridica-operatore di back-end.

È più complicato, invece, stabilire se la s.p.a. che utilizzi detto sistema per "scelte" strategiche, così come i suoi amministratori, possano essere qualificati come operatori di front-end. La questione qui può essere solo accennata, ma (*i*) occorrerebbe comprendere che cosa si intenda per "beneficio" ai sensi dell'art. 3, facilmente attribuibile alla s.p.a. ma di più ardua attribuzione per gli amministratori; (*ii*) quale possa essere il «controllo» dell'utilizzatore e quali siano i «potenziali rischi associati all'operatività e al funzionamento del sistema di IA»; (*iii*) l'importanza dei danni e dei pregiudizi legati al processo decisionale e il correlativo ruolo degli algoritmi.

Immaginando allora un possibile scenario d'indagine, si crede che potrebbero svolgere un ruolo significativo (*a*) la *due diligence* effettuata nei confronti del produttore (in *outsourcing*)-operatore di back-end e del sistema di IA prodotto, prendendo spunto anche dai criteri di diligenza indicati dallo Schema; (*b*) il corretto impiego del sistema di IA da parte della s.p.a. utilizzatrice, pure in termini di aggiornamento e di manutenzione; (*b*) la valutazione critica dell'*output* dell'algoritmo da parte dell'utilizzatore, anche in comparazione con altri elementi funzionali alla decisione effettuata, cercando di evitare una sorta di *ipse dixit*.

12.9. La proposta di regolamento c.d. "*AI Act*", apparentemente scollegata con i pregressi lavori

Si è fatto cenno in apertura alla Proposta di regolamento predisposta dalla Commissione europea, c.d. *Artificial Intelligence Act* (AIA), che però si pone in parziale discontinuità con gli altri documenti precedentemente analizzati.

Il tema non può essere qui approfondito, ma va segnalato, in primo luogo, il criterio non chiaro e piuttosto rigido con cui l'AIA distingue sistemi di IA "ad alto rischio" da sistemi di IA "non ad alto rischio" [55].

In secondo luogo, e soprattutto per ciò che qui interessa, l'AIA prevede una serie obblighi di *compliance* a carico degli operatori che impiegano sistemi di IA "ad alto rischio", chiaramente ispirati alle Linee-guida etiche. Nondimeno, detti obblighi di *compliance* non sono previsti per gli operatori che impiegano sistemi di IA "non ad alto rischio". Manca, inoltre, qualsiasi riferimento al regime di responsabilità civile [56].

Da tutto ciò consegue un evidente scollamento tra lo Schema di proposta del Parlamento e la Proposta dell'AIA della Commissione: non è facilmente riscontrabile la compatibilità tra un regime di responsabilità oggettiva e la previsione dei menzionati obblighi di *compliance*, per

---

[55] Cfr., in particolare, l'art. 6 AIA. Al riguardo, i sistemi di IA "ad alto rischio" concernerebbero tecnologie di IA che possono avere un impatto significativo sulla salute, la sicurezza o i diritti fondamentali delle persone fisiche; ovvero che possono essere componenti di sicurezza di un prodotto; ovvero che possano essere essi stessi un prodotto (*i*) regolato dalla legislazione dell'UE in tema di sicurezza dei prodotti e che richieda una valutazione di conformità da parte di un terzo, al fine di essere collocato sul mercato o messo in funzione secondo una normativa dell'UE, ovvero (*ii*) incluso in un'ulteriormente ristretta lista tassonomica. Per una prima analisi critica dell'AIA, cfr. M. EBERS, V.R.S. HOCH, F. ROSENKRANZ, H. RUSCHEMEIER, B. STEINRÖTTER, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, in 4 *J* (2021) https://doi.org/10.3390/j4040043, pp. 589 ss., spec. pp. 593 ss.; M. VEALE, F. ZUIDERVEEN BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act Analysing the good, the bad, and the unclear elements of the proposed approach*, in J. of Information L. and Tech., 4/2021, pp. 97 ss., spec. 102 ss.; N. SMUHA, E. AHMED-RENGERS; A. HARKENS, W. LI, J. MACLAREN, R. PISELLI, K. YEUNG, *How the EU can achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 5 August 2021, in https://ssrn.com/abstract=3899991.

[56] La *ratio legis* di tali previsioni consisterebbe nel promuovere un mercato unico in tema di IA, nonché di incentivare l'innovazione, evitando i cc.dd. *chilling effects* dovuti ad un eccesso di regolamentazione e all'incertezza giuridica. Ma l'obiettivo principale è quello di rendere l'UE competitiva con gli Stati Uniti e la Cina nell'evoluzione delle tecnologie digitali. Cfr. i «considerando» (23) e (24) della Proposta. In dottrina, cfr. L. FLORIDI, *The European Legislation on AI*, cit.; A. BRADFORD, *Effetto Bruxelles. Come l'Unione Europea regola il mondo*, trad. it. P. Micalizzi, Milano, 2021. Sull'approccio etico, economico e normativo dell'UE in tema di IA, rispetto a U.S.A. e Cina, cfr., altresì. E. HINE, L. FLORIDI, *Artificial Intelligence with American Values and Chinese Characteristics: A Comparative Analysis of American and Chinese Governmental AI Polici*es, in https://ssrn.com/abstract=4006332, 2022; R. RIBERA D'ALCALÀ, *La bussola etica dell'intelligenza artificiale. Visioni e prospettive dell'Unione europea*, in *Etica digitale*, cit., da p. 101.

quanto concerne l'impiego di sistemi di IA "ad alto rischio". D'altro canto, l'impiego dei sistemi di IA "ad alto rischio" parrebbe soggetto a un rischio di *deregulation* eccessivo.

La sensazione è allora che tale Proposta dovrà essere significativamente rivista nella sua stessa struttura.

12.10. Impostazione per una responsabilità da organizzazione d'impresa

Il rapido *excursus* sull'evoluzione normativa in corso in tema di regolamentazione europea sull'IA permette di esporre alcune riflessioni che possono essere utili ai fini di uno studio *ex professo* del tema.

Si crede che l'utilizzo della "personalità elettronica", quand'anche in una prospettiva funzionale, non costituisca la soluzione più opportuna da adottare. Alcune tra le principali ragioni possono essere qui solo accennate: il veloce progresso tecnologico e l'inserimento di un (ulteriore) diaframma nell'interrelazione fra esseri umani, danni cagionati dall'impiego dell'IA e connessa responsabilità potrebbero favorire abusi, elusioni e frodi alla legge, o peggio, progetti criminali [57]; adottare una prospettiva "a soggetto" nei confronti dei sistemi di IA, pensando che essi decidano/agiscano e rispondano dei danni, rischierebbe, in ogni caso, di disincentivare e de-responsabilizzare coloro che devono rendere sicuro il sistema di IA; allo stesso tempo aumenterebbero le probabilità di innescare l'idea di attribuire diritti proprietari o addirittura diversi diritti della personalità ad entità inanimate, con rischi etici e di deriva dei diritti umani; sorgerebbero poi notevoli difficoltà di inserimento della "persona elettronica" nell'ambito dell'ordinamento vigente, soprattutto se si condivide l'idea che già per le persone giuridiche il rapporto tra diritti della personalità, diritti di proprietà industriale e impresa collettiva vadano regolati secondo principi diversi da quelli delle persone fisiche [58]. E d'altronde lo stesso Parlamento europeo (che, si ricorda, aveva formulato l'ipotesi della "personalità elettronica"), insieme a numerosi esponenti del mondo scientifico ed all'evoluzione normativa di importanti Stati membri, si è mostrato contrario a tale soluzione nello Schema di proposta di

[57] Su tale criticità, cfr. L. LOPUCKY, *Algorithmic Entities*, cit.

[58] Cfr., su tale ultimo aspetto e in termini generali, A. ZOPPINI, *I diritti della personalità*, cit., pp. 864 s., 884 s.

regolamento [59]. Nello stesso Schema di proposta di regolamento oltre che nel Libro Bianco, inoltre, l'attenzione posta alla correlazione tra responsabilità e *rischio* si sposa perfettamente con la responsabilità dell'imprenditore commisurata a come venga gestito il rischio d'impresa assunto tramite l'*organizzazione* d'impresa.

Seguendo l'impostazione dei documenti finora menzionati, appare preferibile tener ferma la prospettiva secondo cui un sistema di IA deve essere inteso *come un mero strumento a disposizione dell'uomo*: in tal senso, la tripartizione gaiana (*supra*, § 2) porterebbe a classificare l'IA quanto meno come *res*, seppure con un'anomala vicinanza alle *actiones*. Tuttavia, tale schema elementare non contempla l'*impresa* come *organizzazione* produttiva e come *attività* organizzata.

E allora si può proseguire il discorso, limitatamente a ciò che qui interessa, intendendo l'IA come strumento a disposizione di un uomo-imprenditore. Che poi detto imprenditore sia organizzato in forma di società di capitali, specie se imprenditore collettivo, non implica una minore centralità dell'uomo [60].

Al contrario, lo studio delle dottrine tradizionali e più recenti in tema di personalità giuridica può confermare l'imprescindibilità e la

---

[59] Per una critica all'ipotesi della "personalità elettronica" cfr. EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 37 ss.; OPEN LETTER TO THE EUROPEAN COMMISSION, *Artificial Intelligence and Robotics*, redatta da un gruppo di intellettuali, reperibile sul sito http://www.robotics-openletter.eu (ultimo accesso 10 settembre 2020). Cfr., altresì, in Francia la *Proposition de loi constitutionnelle* n. 2585 del 15 gennaio 2020, relativa alla *Charte de l'intelligence artificielle et des algorithmes*, la quale prevede espressamente, a protezione dei diritti dell'Uomo, che «Un système [«qui se compose d'une entité qu'elle soit physique (par exemple un robot) ou virtuelle (par exemple un algorithme) et qui utilise de l'intelligence artificielle», n.d.r.] *n'est pas doté de la personnalité juridique et par conséquent inapte à être titulaire de droits subjectifs*. Cependant les obligations qui découlent de la personnalité juridique incombent à la personne morale ou physique qui héberge ou distribue ledit système devenant de fait son représentant juridique» (enfasi aggiunta). Tra coloro che sono invece possibilisti verso l'impiego della "personalità elettronica" cfr. A. BERTOLINI, *Artificial Intelligence and Civil Liability*, cit., pp. 34 ss., seppure in una prospettiva funzionale e circoscritta ad alcuni casi di sistemi di IA e/o robotici particolarmente complessi e di cui appare difficile ricostruire profili individuali di responsabilità di programmatori, fornitori, utilizzatori ecc., come ad esempio l'autovettura a guida autonoma. Cfr., altresì, l'importante tesi autopoietica di G. TEUBNER, *Digitale Rechtssubjekte?*, cit., secondo cui l'agente digitale potrebbe essere inquadrato come un "ibrido", consistente in un'associazione uomo-macchina percepita unitariamente dall'ambiente sociale; *adde* C.P. CIRILLO, *I soggetti giuridici digitali*, in *Contr. impr.*, 2020, da p. 573.

[60] Cfr., in tal senso, MÖSLEIN, *Robots in the Boardroom*, cit., pp. 650 ss.

centralità del fattore umano anche in tale ambito [61]. Ciò, si crede, va tenuto ben presente laddove si paventi l'impiego di meccanismi analoghi alla persona giuridica per regolare la responsabilità per danni cagionati dall'impiego dell'IA.

Sempre esaminando le dottrine generali civilistiche ed anche autorevole dottrina giuscommercialistica in tema di società, si possono trovare invece importanti argomenti per inquadrare l'impiego di sistemi di IA nella prospettiva, oggettiva, dell'*organizzazione dell'attività* imprenditoriale [62].

In buona sostanza, si può immaginare *un sistema di IA come un'articolazione dell'organizzazione dell'impresa societaria* o comunque come *parte dell'attività* il cui (specifico) *rischio* deve essere gestito nell'ambito dell'organizzazione imprenditoriale ed in qualche modo garantito dal patrimonio dell'imprenditore.

Secondo tale prospettiva – concentrando l'attenzione sulle imprese che *utilizzano* sistemi di IA [63] – anche *de iure condito* si può individuare una regolamentazione della responsabilità civile per l'impiego di queste nuove tecnologie traendo spunto dagli istituti della responsabilità in qualche modo connessi ad un'organizzazione d'impresa non conforme ai criteri testé menzionati. Nell'ordinamento giuridico italiano è il caso della responsabilità per danni cagionati da cose in custodia (art.

---

[61] La letteratura al riguardo è vastissima, a partire dalla pandettistica tedesca. Cfr., per tutti, T. ASCARELLI, *Considerazioni in tema di società e personalità giuridica*, in *Riv. dir. comm.*, 1954, I, da p. 245 e da p. 333; ID., *Personalità giuridica e problemi delle società*, in *Riv. Soc.*, 1957, da p. 981; M. BASILE, A. FALZEA, voce «Persona giuridica (dir. priv.)», in *Enc. Dir.*, XXIII, Milano, 1983, da p. 234.; A. FALZEA, *Il soggetto nel sistema dei fenomeni giuridici*, Milano, 1939, pp. 171 ss.; ID., voce «Capacità (teoria gen.)», in *Enc. Dir.*, VI, Milano, 1960, da p. 8; F. D'ALESSANDRO, *Personalità giuridica e analisi del linguaggio*, rist. a cura di N. Irti, Padova, 1991; N. IRTI, *Sul concetto di titolarità (persona fisica e obbligo giuridico)*, in *Riv. dir. civ.*, 1970, I, da p. 501, pp. 519 ss.; R. ORESTANO, *Diritti soggettivi e diritti senza soggetto*, in *Jus*, 1960, da p. 142; ID., *Il « problema delle persone giuridiche » in diritto romano*, Torino, s.d. ma 1968, pp. 55 ss.; G.G. SCALFI, *L'idea di persona giuridica e le formazioni sociali titolari di rapporti nel diritto privato*, Milano, 1968; P. ZATTI, *Persona giuridica e soggettività*, Padova, 1975. Cfr., altresì, F. RANIERI, *L'invenzione della persona giuridica*, Milano, 2020.

[62] Cfr., in termini generali, P. FERRO-LUZZI, *I contratti associativi*, Milano, 1971, spec. pp. 170 ss.; C. ANGELICI, *La società per azioni. Principi e problemi*, vol. I, in *Trattato di diritto civile e commerciale*, a cura di P. Schlesinger, Milano, 2012, pp. 126 ss., pp. 139 ss., pp. 345 ss.; P. ZATTI, *Persona giuridica e soggettività*, cit., pp. 172 s.

[63] Relativamente più semplice può essere il discorso per le imprese che programmano ovvero pongono sul mercato sistemi di AI, quale *prodotto* o *servizio*. In tale ipotesi, seppure con i dovuti *distinguo*, si può ragionare prendendo spunto dalla responsabilità da prodotto difettoso o non sicuro.

2051 c.c.) ma anche della responsabilità per fatto di dipendenti/ausiliari (artt. 1228 e 2049 c.c.) o comunque institoria o legata alla rappresentanza, legale o volontaria. Il discorso può valere persino per la responsabilità da rischio (art. 2050 c.c.), a seconda di come vada collocato lo sviluppo inatteso o il mal funzionamento del sistema di IA nell'ambito del rischio d'impresa.

Al riguardo, traendo spunto anche dall'evoluzione normativa in tema di responsabilità da reato delle persone giuridiche, la dottrina che ha approfondito il tema propende per una *responsabilità da organizzazione scorretta e inadeguata*, da preferire alla responsabilità oggettiva [64]. Tale impostazione non è estranea neppure all'evoluzione di altri ordinamenti giuridici europei o di *common law* [65] ed è ulteriormente avvalorata dalla codificazione dei principi di corretta gestione imprenditoriale e societaria, anche sotto il profilo dell'adeguatezza degli assetti organizzativi (artt. 2381, 2403, 2497, 2086 2° co., c.c.), avvenuta con la riforma del diritto societario del 2003 e con la recente riforma del diritto della crisi d'impresa.

Ed allora si può pensare, in primo luogo, che un simile approccio valorizzi e incentivi opportunamente le imprese che si organizzano in maniera adeguata per un corretto impiego dei sistemi di IA. Adottando il criterio della responsabilità oggettiva si rischierebbe invero di provocare una selezione avversa a svantaggio delle imprese più efficienti, che pagherebbero due o persino tre volte (in caso di assicurazione obbligatoria con rivalsa) i costi di tale impiego. In tal modo si disincentiverebbero l'efficienza ed il progresso tecnologico, a discapito dell'utilità sociale dell'iniziativa economica (artt. 3, 2° co. e 41, 2° co., Cost.) [66].

In secondo luogo, tale approccio individua un modello giuridico consolidato di riferimento che consente di chiarire non solo i *criteri di imputazione della responsabilità* ma anche *i criteri di imputazione di*

---

[64] Cfr. F. GUERRERA, *Illecito e responsabilità nelle organizzazioni collettive*, Milano, 1991; M. CAMPOBASSO, *L'imputazione di conoscenza nelle società*, Milano, 2002; A. ZOPPINI, *Imputazione dell'illecito penale e «responsabilità amministrativa» della persona giuridica*, in *Riv. soc.*, 2005, da p. 1314; E. GINEVRA, *Identità e rilevanza della persona giuridica alla luce del d.lgs. n. 231/2001*, in *Riv. soc.*, 2020, da p. 72. Cfr., altresì, C. ANGELICI, *op. loc. ult. cit.*

[65] Per un approfondimento sul tema, anche con riferimenti dottrinali, cfr. M. CAMPOBASSO, *op. cit.*, pp. 37 ss., pp. 80 ss.; F. GUERRERA, *op. cit.*, pp. 303 ss. Cfr., altresì, EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES, *Liability for Artificial Intelligence*, cit., pp. 19 ss.

[66] Circa il rilievo giuridico dell'utilità sociale dell'iniziativa economica nella responsabilità da organizzazione imprenditoriale, cfr. E. GINEVRA, *Identità*, cit.

conoscenza e della volontà negoziale. Sempre al fine di risolvere l'opzione fra responsabilità per colpa, aggravata od oggettiva – se si condividono i risultati della dottrina che propende per la responsabilità da scorretta/inadeguata organizzazione – si crede che sarebbe pregiudizievole per l'imprenditore che impiega sistemi di IA adoperare un criterio d'imputazione di responsabilità più severo (la responsabilità oggettiva) rispetto a quello previsto per gli imprenditori che utilizzano rappresentanti/ausiliari o cose meno evolute [67].

12.10.1. (segue) Riflessi nel diritto societario: il ruolo dell'adeguatezza degli assetti societari

Nell'ambito di questa impostazione, l'organizzazione imprenditoriale in forma di società, e in particolare di società di capitali, permette di inquadrare il dovere di corretta organizzazione dell'impresa per l'impiego dell'IA nell'ambito del dovere degli amministratori di istituire un assetto imprenditoriale e societario adeguato alla natura ed alle dimensioni dell'impresa (artt. 2086, 2° co., 2381 e 2403 c.c.).

Al riguardo, esigenze di sintesi impongono di accennare solamente che tale ultimo dovere, da un lato, richiede che gli amministratori dispongano in qualche modo (direttamente o indirettamente) di competenze specifiche in tema di di IA [68] e, dall'altro, l'adozione di una prospettiva *procedimentale* [69] non dissimile da quella contemplata nei documenti menzionati nei precedenti paragrafi. In particolare, la codificazione normativa dei doveri di corretta gestione imprenditoriale (art. 2497 c.c.) consente di attribuire un rilievo giuridico significativo all'osservanza delle migliori prassi e norme tecniche esistenti, da

[67] In termini non dissimili sul punto, G. TEUBNER, *Digitale Rechtssubjekte?*, cit., pp. 187 s.

[68] Una spia normativa in tal senso si rinviene nell'art. 2392 c.c. ove è previsto che gli amministratori di una s.p.a. devono adempiere ai doveri imposti dalla legge e dallo statuto «con la diligenza richiesta *dalla natura dell'incarico e dalle loro specifiche competenze*» (enfasi aggiunta). E sul problema delle competenze degli amministratori cfr., altresì, il «considerando» n. 18 dello Schema di proposta di regolamento, ove si legge che «l'operatore potrebbe avere una conoscenza limitata degli algoritmi e dei dati utilizzati nel sistema di IA. Si dovrebbe presumere che l'operatore abbia osservato la dovuta diligenza che ci si può ragionevolmente attendere da questi nel selezionare un sistema di IA idoneo, laddove l'operatore abbia scelto un sistema di IA certificato».

[69] Cfr. C. ANGELICI, *La società per azioni*, cit., p. 417 *sub* nt. 140; ID., *Interesse sociale e business judgment rule*, in *Riv. dir. comm.*, 2012, I, da p. 573.

canalizzare entro sistemi di controllo interno e di procedure di gestione dei rischi.

In tale ambito, si crede, *possono essere annoverati i documenti precedentemente citati ed anche le linee guida etiche*. Il risultato è degno di nota già per il solo fatto che si individua una cornice giuridica anche a prescrizioni *prima facie* meramente etiche.

E sempre all'interno dei principi di corretta gestione imprenditoriale e di adeguatezza degli assetti, l'osservanza, da parte degli amministratori di società, di una *due diligence* verso le controparti contrattuali nonché verso gli strumenti adottati per l'esercizio dell'impresa, può contribuire in maniera decisiva a sviluppare la cooperazione tra i vari operatori economici nella catena di approvvigionamento e tra gli utilizzatori. Detta cooperazione, si ricorda, è auspicata dalla Commissione europea al fine di conseguire l'obiettivo della *certezza giuridica* mediante i principi della "responsabilità condivisa" e dell'*accountability* e inoltre è parte dello Schema di proposta di regolamento (*supra*, § 8) [70].

A tal proposito, la contrattazione tra le varie componenti, prevalentemente imprenditoriali, della catena di valore può contribuire a regolamentare chiaramente i confini di ciascuna responsabilità, con opportune clausole di salvaguardia, ad esempio tese a chiarire i rispettivi doveri di monitoraggio e aggiornamento del *software*, specie se indipendente.

12.11. Impressioni di sintesi: una normativa in costruzione che può incentivare il progresso, favorire una corretta organizzazione d'impresa e tutelare i diritti fondamentali

Il *rilievo centrale* che l'approccio dell'Unione europea attribuisce all'*essere umano* e all'osservanza dei *diritti fondamentali* costituisce certamente un fattore decisivo per impedire l'appiattimento, o peggio la

[70] Cfr., altresì, art. 8.4 dello Schema di proposta di regolamento, ove si legge che «Il produttore di un sistema di IA è tenuto a cooperare con l'operatore o con la persona interessata, su loro richiesta, e a fornire loro informazioni, nella misura giustificata dall'importanza della pretesa, al fine di consentire l'individuazione delle responsabilità».

sudditanza, nei confronti degli *output* dei sistemi di IA e quindi di una società o di un'economia *data driven*.

Un segnale, inquietante, dell'importanza del tema si scorge nell'epigrafe della *Proposition de loi constitutionnelle* n. 2585 del 15 gennaio 2020, relativa alla *Charte de l'intelligence artificielle et des algorithmes*, ove si legge che « Au même titre que les virus s'intègrent au long cours au patrimoine génétique des humains, les technologies du quotidien entrent de fait dans les réflexions».

Volendo seguire l'impostazione incentrata sulla *responsabilità, aggravata, da scorretta o inadeguata organizzazione d'impresa*, la prima impressione corre nel senso di auspicare che il futuro quadro normativo in tema di responsabilità civile per il funzionamento di sistemi di intelligenza artificiale consideri in maniera in qualche modo "transitoria" la responsabilità oggettiva dei sistemi di IA. Si vuol dire che, al di fuori di casi eccezionali particolarmente rischiosi, si potrebbe immaginare che vengano inclusi nell'elenco dei sistemi di IA "ad alto rischio" soprattutto quelli più innovativi e che proprio a causa della loro innovatività non consentono in una fase iniziale di governare del tutto i rischi connessi.

D'altronde le principali innovazioni tecnologiche in tema di sistemi di IA dovrebbero svilupparsi in un ambiente normativo protetto, in stretta collaborazione con le autorità di vigilanza competenti. In tal senso depone il «considerando» L della Risoluzione del 2020, ove si legge che «sarebbe opportuno adottare un approccio in cui si ricorra a sperimentazioni, progetti pilota e spazi di sperimentazione normativa per trovare soluzioni proporzionate e basate su dati concreti che affrontino, ove necessario, situazioni e settori specifici».

Detto approccio è particolarmente condiviso nell'ambito dell'intero fenomeno del *fintech*, ove la Commissione europea intende favorire l'aggiornamento delle autorità di vigilanza nonché il dialogo fra queste, le imprese vigilate e le imprese *fintech*, mediante «facilitatori *fintech*» (*innovation hub*, *sandbox* o *incubator*) istituiti presso le autorità di vigilanza nazionali nonché tramite istituzione di laboratori per le tecnologie finanziarie e la costituzione di un gruppo di esperti che valutino la compatibilità tra il quadro normativo regolamentare, attuale e *in fieri*, ed il progresso tecnologico [71].

[71] Cfr. COMMISSIONE EUROPEA, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, Bruxelles, 8 marzo 2018, COM(2018) 109 final; ESAS, *FinTech: Regulatory sandboxes and innovation hubs*, 2018, in

I rischi non governabili dovrebbero allora essere minimi e in ogni caso il problema del *black box* dovrebbe essere presto superato perfezionando il sistema di IA innovativo o la sua applicazione innovativa.

Inoltre, i vantaggi per la collettività devono notevolmente oltrepassare i pregiudizi, anche potenziali, come chiaramente espresso dal principio di *efficienza* (*supra*, § 4), dalle Linee-guida etiche riguardo al *trade-off* tra *accuracy* e trasparenza (*supra*, § 5) nonché dal «considerando» n. 4 dello Schema di proposta di regolamento, ove si puntualizza che «i vantaggi della diffusione dei sistemi di IA saranno di gran lunga superiori agli svantaggi».

A favore della tendenziale temporaneità della situazione di "alto rischio" e della connessa responsabilità oggettiva giovano, nella Schema di proposta di regolamento, (*i*) l'art. 4.2, che delega alla Commissione il potere anche di *eliminare* sistemi di IA dall'elenco di quelli "ad alto rischio", così assoggettandoli ad un regime responsabilità aggravata in luogo della responsabilità oggettiva; (*ii*) il «considerando» n. 2, ove si legge che «*Specialmente all'inizio del ciclo di vita di nuovi prodotti e servizi*, dopo che questi hanno superato i test preliminari, per l'utente e per i terzi è presente un certo grado di rischio che qualcosa non funzioni correttamente» [72].

D'altra parte, pur sempre ad una prima sensazione, l'approccio procedimentale promosso soprattutto attraverso le Linee guida etiche e il Libro bianco sembra non trovare piena realizzazione nei sistemi di IA "ad alto rischio", così come definiti e disciplinati. Così, nel «considerando» n. 3 dello Schema di proposta di regolamento si avverte la consapevolezza di un possibile affievolimento, tra gli altri, della *fairness*, dell'*explicability*, dell'*intervento e sorveglianza umani* oltre che della *robustezza* [73].

Tutto ciò potrebbe essere interpretato come una *tensione proattiva al raggiungimento di tutti i requisiti previsti dalle Linee-guida e dal Libro*

www.europa.esma.eu.

[72] Enfasi aggiunta.

[73] Ed infatti vi si legge che «L'uso di sistemi di IA nella vita quotidiana porterà a situazioni in cui la loro opacità (elemento "scatola nera") e la pluralità di soggetti che intervengono nel loro ciclo di vita renderanno estremamente oneroso o addirittura impossibile identificare chi avesse il controllo del rischio associato all'uso del sistema di IA in questione o quale codice o input abbia causato l'attività pregiudizievole. Tale difficoltà è aggravata dalla connettività tra un sistema di IA e altri sistemi, di IA e non di IA, dalla sua dipendenza dai dati esterni, dalla sua vulnerabilità a violazioni della cibersicurezza e dalla crescente autonomia di sistemi di IA attivati dall'apprendimento automatico e dalle capacità di apprendimento profondo».

bianco, promossa dal legislatore *in fieri*. Uno dei principali strumenti per raggiungere tale risultato sarebbe costituito proprio dalla responsabilità oggettiva, da intendersi allora come sprone al perfezionamento delle innovazioni tecnologiche immesse nel mercato e tra il pubblico, al fine di beneficiare del più clemente strumento della responsabilità aggravata.

Se così fosse, quest'ultimo regime andrebbe a costituire la regola, laddove l'assunzione di un "alto rischio" e la connessa responsabilità oggettiva potrebbero essere l'eccezione.

* Postilla. Nelle more della pubblicazione di questo scritto la Commissione europea ha pubblicato due proposte di direttiva molto rilevanti rispetto ai temi qui trattati. Si fa riferimento alla Proposta di direttiva del Parlamento europeo e del Consiglio «on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)» [COM(2022) 496 final (di seguito "AILD")] e alla Proposta di direttiva del Parlamento europeo e del Consiglio «on liability for defective products» [COM(2022) 495 final (di seguito "PLD")], entrambe del 28.09.2022.
Al riguardo, l'AILD prevede una serie di incentivi di *disclosure* verso i soggetti danneggiati da sistemi di IA nonché di presunzioni *iuris tantum* a favore di questi ultimi, al fine di non rendere più onerosa la loro azione di responsabilità extracontrattuale, rispetto a chi abbia subìto un danno derivante da diverse circostanze.
La stessa AILD si coordina poi con la PLD per agevolare l'individuazione del responsabile nell'ambito della catena di valore dei sistemi di IA, con particolare attenzione al produttore.
A tal proposito, la PLD mira a colmare i limiti della normativa originaria in tema di danno da prodotti difettosi, limiti che sono stati segnalati nelle pagine che precedono.

13. Trattamento dei dati personali e tutela dei minori

Federico Ruggieri (Università di Palermo)

13.1. Contesto dei nuovi media ed esigenze di tutela

Con l'affermazione del web 2.0 gli utenti di Internet sono divenuti i protagonisti della c.d. società dell'informazione: tutti, in modo sostanzialmente indistinto, hanno la possibilità e gli strumenti per compiere in prima persona attività di creazione e condivisione di contenuti digitali[1]. Così, la diffusione e il successo dei più diversi *social network*, ciascuno caratterizzato da specifiche funzionalità e rivolto a particolari categorie di utenti[2], come anche il sempre più abituale ricorso da parte dei consumatori di piattaforme digitali di acquisto e di valutazione di beni e servizi, hanno trasferito nella dimensione virtuale aspetti e momenti tipici delle relazioni interpersonali.

Ciò appare tanto più evidente e comprensibile se si considera l'utilizzo quotidiano e costante che ormai generalmente si fa dei c.d. nuovi media, ovvero di tutti quei mezzi di comunicazione che funzionano proprio perché connessi alla rete. E che, in quanto tali, costituiscono strumenti di fruizione, elaborazione e condivisione di informazioni in tempo reale, oltre che in assenza di qualsivoglia impedimento di

---

[1] Sulla rivoluzione di Internet «caratterizzata dall'avvento dei *social network* e dalla diffusione del Web 2.0», G.M. RICCIO, Social networks *e responsabilità civile*, in *Diritto dell'informazione e dell'informatica*, 6, 2010, pp. 859 ss. Il riferimento a Internet 2.0 si ritrova già in S. RODOTÀ, *Tecnologie e diritti*, Seconda edizione a cura di G. ALPA, M.R. MARELLA, G. MARINI, G. RESTA, Il Mulino, Bologna, 2021, pp. 119 ss.

[2] A.R. POPOLI, Social Network *e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Diritto dell'informazione e dell'informatica*, 6, 2014, pp. 982 ss.

carattere spaziale che ne ostacoli materialmente la circolazione.

Dispositivi di uso comune, come gli *smartphone* o i computer, permettono al giorno d'oggi di essere perennemente connessi e in grado di entrare in contatto con altre persone: i rapporti di famiglia, di amicizia o professionali, o anche le attività di svago, di studio o di lavoro, sono a immediata portata di un semplice *clic*.

In questo contesto, ci si interroga inevitabilmente su quali possano essere le conseguenze giuridicamente rilevanti dell'accesso, spesso non sufficientemente consapevole, alla rete, in particolare per quanto concerne il trattamento dei dati personali.

L'utilizzo di tutti questi *device* implica infatti una tanto inevitabile quanto consistente circolazione di dati riferiti alla propria persona, cui viene comunemente richiesto di indicare le proprie generalità, di condividere la propria posizione o anche di acconsentire all'accesso ai contatti inseriti in rubrica, alla fotocamera, al microfono, alle immagini in galleria o a qualsiasi altra informazione disponibile sullo strumento utilizzato per fruire di determinati servizi *online*. Circolazione che, come appare intuibile, presenta particolari profili di rischio per la tutela dei diritti della persone fisiche e, in particolare, del diritto alla privacy, ovvero al corretto trattamento dei dati personali[3].

Tale circostanza richiede peraltro una specifica riflessione quando

[3] Di autonoma rilevanza rispetto al diritto alla riservatezza, sebbene siano entrambi storicamente riconducibili all'elaborazione, di derivazione statunitense, del diritto ad essere lasciati soli, c.d. *right to be let alone*, generalmente ricondotto al celebre saggio di S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, vol. 4, n. 5, 1890, pp. 193 ss. Tale diritto si qualificava per un contenuto negativo, di esclusione dei terzi dalla conoscenza dei fatti privati e di opposizione a qualsiasi indesiderata altrui ingerenza nella propria sfera fisica e morale. Questa particolare connotazione caratterizza oggi quello che definiamo diritto alla riservatezza. Diversamente, il diritto alla privacy costituisce un diritto autonomo, dal contenuto opposto, positivo, in quanto diritto alla autodeterminazione informativa, di libera scelta e di pieno controllo rispetto alla circolazione dei propri dati personali. In ciò il diritto alla privacy presenta dunque una portata nettamente più ampia rispetto all'affine diritto alla riservatezza, proiettando la tutela di questo aspetto della personalità anche nei confronti degli attori del mercato, che del patrimonio informativo riferito a una persona possono fare un utilizzo mirato all'influenza delle scelte di consumo. In questo senso, si dice che tale diritto presenta una natura al contempo privatistica e pubblicistica. Di tale distinzione prende peraltro atto, già nel 2000, la Carta dei diritti fondamentali dell'Unione europea, che opportunamente distingue, all'art. 7, il diritto al rispetto della vita privata e familiare e, all'art. 8, il diritto alla privacy quale diritto al corretto trattamento dei propri dati personali (M. BIANCA, *Il minore e i nuovi media*, in R. SENIGAGLIA (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pacini Giuridica, Pisa, 2020, pp. 151 ss.).

ad esserne interessate sono persone particolarmente esposte e vulnerabili come i soggetti minori di età[4].

Infatti, sebbene le insidie inerenti alla fruizione di servizi in rete incombano in egual misura su tutti gli utenti del web, indipendentemente dal fattore anagrafico, l'impiego diffuso dei nuovi media da parte dei più giovani desta nei loro confronti specifiche esigenze di attenzione e tutela[5].

La ragione di tanto riguardo si ritiene ravvisabile nell'incidenza che l'utilizzo di tali strumenti può avere nel processo di formazione della propria identità personale[6]. A maggior ragione con riferimento a soggetti che si trovano nel pieno di una fase di crescita e di primo sviluppo di idee e convincimenti propriamente personali, specificamente sotto il profilo culturale, politico, religioso o sessuale. E la cui identità digitale[7] appare difficilmente distinguibile da quella della vita di relazione *offline*, pur affermandosi in un mondo virtuale in cui trovano realizzazione autonome situazioni di pericolo. In questo contesto, infatti, il diradamento dei contatti reali con altre persone rischia di non far riconoscere i limiti alla condivisione di informazioni di carattere personale[8].

In questo senso, un'eventuale circolazione incontrollata dei dati personali che li riguardano potrebbe generarne l'esposizione a specifiche situazioni di pericolo – ad esempio rispetto alle persone con cui

---

[4] Per un inquadramento complessivo delle situazioni giuridiche c.d. di vulnerabilità, si rimanda a E. BATTELLI, *I soggetti vulnerabili: prospettive di tutela della persona*, in *Il diritto di famiglia e delle persone*, 1, 2020, pp. 283 ss.

[5] Sul punto, già ampiamente il Libro Bianco "Media e minori" 2.0, pubblicato dall'Autorità Garante per le Comunicazioni (AGCOM) nel 2016, nonché il documento "La tutela dei minorenni nel mondo della comunicazione", del 2017, ad opera dell'Autorità Garante per l'Infanzia e l'Adolescenza (AGIA).

[6] Sull'evoluzione del diritto all'identità personale, in particolare, G. PINO, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Il Mulino, Bologna, 2003; G. FINOCCHIARO, (voce) *Identità personale (diritto alla)*, in *Digesto delle discipline privatistiche – Sezione civile*, Aggiornamento, V, Utet, Torino, 2010, pp. 721 ss.

[7] In argomento si veda G. RESTA, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica*, 3, 2007, pp. 511 ss. Più recentemente, G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 3, 2017, pp. 723 ss.

[8] A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo*, in *Le nuove leggi civili commentate*, 2, 2017, p. 424. Si veda anche G. PEDRAZZI, *Minori e* social media*: tutela dei dati personali, autoregolamentazione e privacy*, in *Informatica e diritto*, 1-2, 2017, pp. 437 ss.

possono accidentalmente entrare in contatto ovvero accedendo a contenuti inappropriati o divenendo destinatari di pubblicità commerciali mirate[9] –, capaci di incidere (negativamente) sulla loro personalità *in fieri*.

Le questioni sottese a tali considerazioni sono in sostanza di primaria importanza ed attualità, interessando intere generazioni di nativi digitali, nati e cresciuti in un mondo già altamente informatizzato e interconnesso tramite Internet[10], ma non per questo meno vulnerabili nella formazione di sé e nello sviluppo della propria identità. E in quanto tali meritevoli di attenzioni mirate, oltre che di appositi strumenti di tutela da parte dell'ordinamento[11].

13.2. I principali riferimenti normativi interni

L'esigenza di tutela della dimensione personale privata dei minori trova un primo riconoscimento formale già nella Convenzione di New York sui diritti del fanciullo del 20 novembre 1989, ratificata in Italia con la l. 27 maggio 1991, n. 176.

L'art. 16 della Convenzione sancisce al primo comma che «[n]essun fanciullo sarà oggetto di interferenze arbitrarie o illegali nella sua vita privata, nella sua famiglia, nel suo domicilio o nella sua corrispondenza, e neppure di affronti illegali al suo onore e alla sua reputazione», garantendo, al secondo comma, il «diritto alla protezione della legge contro tali interferenze o tali affronti». Gli Stati aderenti si impegnavano in questo modo ad adoperarsi per contrastare comportamenti

---

[9] G. CAPILLI, *La tutela dei dati personali dei minori*, in R. PANETTA, *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d. lgs. n. 196/2003 (Codice Privacy)*, Giuffrè, Milano, 2019, p. 249.

[10] Per usare l'espressione di S. SICA, V. ZENO-ZENCOVICH, *Legislazione, giurisprudenza e dottrina nel diritto dell'Internet*, in *Diritto dell'informazione e dell'informatica*, 3, 2010, p. 384, «[l]e generazioni che sono nate digitando una tastiera prima che tenendo in mano una penna».

[11] I. GARACI, *Il «superiore interesse del minore» nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, in *Le nuove leggi civili commentate*, 4, 2021, pp. 800 ss. Sulla duplice prospettiva, fisiologica e patologica, attraverso cui indagare al problema, C. PERLINGIERI, *La tutela dei minori di età nei* social networks, in *Rassegna di diritto civile*, 4, 2016, pp. 1325 ss.

e strumenti potenzialmente lesivi della sfera più intima della vita dei minori. E che tra tali situazioni di rischio per il loro sviluppo si pensasse già allora anche a quelle riconducibili all'utilizzo dei mezzi di comunicazione si evince dal successivo art. 17, che, promuovendo l'accesso delle nuove generazioni ai media e alle nuove tecnologie, trasmette un'immagine particolarmente moderna del minore quale protagonista del proprio percorso educativo e formativo e in quanto tale anche inevitabilmente esposto a una possibile pregiudizievole ingerenza da parte di terzi[12].

A livello interno, il legislatore italiano si è anzitutto occupato di protezione del minore dalle indebite intromissioni nella propria vita privata nell'ambito del processo penale. Il sesto comma dell'art. 114 c.p.p. vieta infatti la pubblicazione delle generalità e dell'immagine dei minorenni che siano testimoni, persone offese ovvero danneggiati dal reato finché non raggiugano la maggiore età; nonché la pubblicazione di qualsiasi elemento che, anche indirettamente, possa comunque provocarne l'identificazione. La disposizione incontra però un limite applicativo nel caso in cui il tribunale per i minorenni ritenga che proprio tale pubblicazione realizzi invece l'interesse esclusivo del minore ovvero qualora sia lo stesso minore ad acconsentirvi, purché si tratti di un minore ultrasedicenne. Tale regime, previsto per il processo penale e ulteriormente specificato dall'art. 13 del d.P.R. 22 settembre 1988, n. 448, concernente il processo a carico di imputati minorenni, è stato poi esteso dall'art. 50 del Codice della privacy (d. lgs. 20 giugno 2003, n. 196) a ogni «caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale».

Occorre rilevare che il Codice della privacy, come anche la precedente legge di disciplina della materia, l. 31 dicembre 1996, n. 675 (di recepimento della direttiva 95/46/CE[13]), abrogata proprio con l'entrata

---

[12] M. NITTI, *La pubblicazione di foto di minori sui* social network *tra tutela della riservatezza e individuazione dei confini della responsabilità genitoriale*, in *Famiglia e diritto*, 4, 2018, p. 388. V. CORRIERO, *Privacy del minore e potestà dei genitori*, in *Rassegna di diritto civile*, 4, 2004, p. 1006, che ripercorre le tappe del processo di valorizzazione dei diritti della personalità del minore innanzitutto a livello sovranazionale, sottolinea espressamente che «la violazione della sfera intima della persona aumenta con il progresso tecnologico degli strumenti di informazione».

[13] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

in vigore del Codice, non conteneva alcuna altra norma espressamente rivolta alla protezione dei dati personali dei minori. Vi erano tuttavia delle disposizioni che, implicitamente, potevano sopperire a tale lacuna.

L'ormai abrogato art. 24 del Codice prevedeva in particolare la possibilità di effettuare il trattamento dei dati anche in mancanza della manifestazione di un apposito consenso laddove fosse «necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato». Ebbene, la mancanza di una norma specificatamente dedicata all'ipotesi di trattamento dei dati dei minori conduceva a due possibili interpretazioni di tale disposizione, dal senso diametralmente opposto. Da un lato, si argomentava che, al di fuori delle ipotesi di salvaguardia della vita o dell'incolumità fisica, il consenso potesse anche venire espresso direttamente dal soggetto minore di età[14]; dall'altro, che la mancata previsione di una norma *ad hoc* andasse necessariamente intesa ravvisando nel raggiungimento della maggiore età un limite imprescindibile per la valida prestazione del consenso[15]. Le stesse considerazioni erano peraltro rivolte anche all'art. 82 del Codice, in materia di somministrazione dell'informativa e richiesta del consenso circa il trattamento dei dati sanitari nell'ambito di una prestazione medica[16].

Alla tutela del minore è poi dedicato l'art. 7 del Codice di deontologia dei giornalisti, allegato al Codice della privacy e approvato con apposito provvedimento dell'Autorità Garante per la protezione dei

---

[14] S. PATTI, *Commento all'art. 23*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, 1, Cedam, Padova, 2007, pp. 544 ss. Nella stessa ottica sembra porsi anche E. LA ROSA, *Tutela dei minori e contesti familiari. Contributo allo studio per uno statuto dei diritti dei minori*, Giuffrè, Milano, 2005, p. 166, riconoscendo valore alla capacità di discernimento del minore nel caso concreto.

[15] V. CUFFARO, *Il consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997, pp. 201 ss.

[16] F. NADDEO, *Il consenso al trattamento dei dati personali del minore*, in *Diritto dell'informazione e dell'informatica*, 1, 2018, pp. 40-41.

dati personali datato 29 luglio 1998. In tale sede, viene stabilito che al giornalista è fatto divieto di pubblicare i nomi dei minori coinvolti in fatti di cronaca e di fornire particolari utili ad identificarli, riconoscendosi espressamente, nel bilanciamento degli interessi coinvolti, la preminenza del diritto del minore «alla riservatezza» sul diritto di critica e di cronaca, con il solo limite della presenza di un oggettivo interesse del minore[17].

All'interno di questa cornice normativa si colloca il nuovo regolamento europeo n. 679 del 2016[18], cui ci si riferisce generalmente con l'acronimo GDPR (*General Data Protection Regulation*), che ad oggi costituisce il principale riferimento normativo in materia di trattamento dei dati personali in tutti gli Stati membri, nell'intenzione dichiarata del legislatore comunitario di uniformare quanto più possibile la disciplina di una materia che, per sua natura, non concepisce l'esistenza o la previsione di confini geografici[19].

L'entrata in vigore del GDPR il 25 maggio 2018 ha richiesto ai legislatori nazionali di adeguare la disciplina interna preesistente, peraltro già parzialmente armonizzata in forza della direttiva del 1995. Il legislatore italiano è così intervenuto per mezzo del d. lgs. 10 agosto 2018, n. 101, che ha abrogato gran parte del contenuto del vigente Codice della privacy, attuando il necessario coordinamento normativo con la nuova disciplina di derivazione europea, cui di volta in volta viene fatto apposito rinvio.

---

[17] In tal senso, l'art. 7 in oggetto compie espresso rimando alla Carta di Treviso. Si tratta di un documento, firmato il 5 ottobre 1990 dall'Ordine dei Giornalisti, dalla Federazione Nazionale della Stampa Italiana e dall'associazione Telefono Azzurro, volto a riconoscere espressamente e in senso vincolante il preminente interesse del minore nello svolgimento dell'attività giornalistica, anche a scapito dell'esercizio del diritto all'informazione.

[18] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

[19] Tra i primi significativi contributi alla nuova normativa europea, si vedano F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, *passim*; G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le nuove leggi civili commentate*, 1, 2017, pp. 1 ss.; F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civili commentate*, 2, 2017, pp. 369 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contratto e impresa*, 1, 2018, pp. 106 ss.

In questo senso, il Codice della privacy nazionale mantiene dunque una propria autonomia, in particolare per quanto non sia direttamente previsto dalle norme del regolamento e per quanto lo stesso GDPR abbia preferito rimettere alla volontà dei singoli ordinamenti, anche a costo dell'auspicata uniformazione.

13.3. La minore età nella nuova disciplina privacy

Quando l'art. 1 GDPR individua lo scopo della nuova disciplina in materia di privacy nella protezione «[de]i diritti e [del]le libertà fondamentali delle persone fisiche», naturalmente con specifico riferimento al diritto alla protezione dei dati personali, sembra volersi ragionevolmente rivolgere a ciascun soggetto di diritto, indipendentemente dalla sussistenza dei requisiti della capacità di agire[20].

Alla tutela dei minori è così appositamente dedicato l'art. 8 GDPR, di cui si dirà diffusamente nei paragrafi che seguono, tuttavia si vuole evidenziare da subito quanto già i considerando del regolamento permettano di riconoscere un approccio innovativo nell'attenzione prestata loro da parte del legislatore europeo.

È innanzitutto il considerando 38 a mostrare come, con riferimento ai minori di età, si sia di fronte a dei soggetti inevitabilmente meno consapevoli, rispetto agli adulti, delle peculiari insidie della rete. In particolare, si afferma che «[i] minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore».

Il riferimento alla consapevolezza ritorna anche al considerando 65,

[20] C. CAMARDI, *Minore e privacy nel contesto delle relazioni familiari*, in R. SENIGAGLIA (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pacini Giuridica, Pisa, 2020, p. 122.

dedicato al diritto all'oblio[21]. Rispetto al quale si dice che «l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano» o quando, più in generale, questo avvenga con modalità non conformi al GDPR. E tale diritto, si aggiunge, risulterebbe ulteriormente rilevante in particolar modo quando «l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet».

Si richiama da ultimo il considerando 58, anch'esso modellato sul presupposto che l'incapace minore di età possa riscontrare particolari difficoltà nella comprensione di quanto si riferisca ad attività aventi ad oggetto il trattamento di dati personali. Il principio di trasparenza, in ogni caso, impone infatti che «le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione». Ma, a maggior ragione, «[d]ato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente».

Si tratta in sostanza di riferimenti, questi, utili a comprendere quanto sia significativa questa nuova centralità che il legislatore europeo ha finalmente riconosciuto alla figura del minore nell'ambito delle dinamiche di circolazione dei dati personali, proprio in considerazione di quelle peculiarità e fragilità che lo caratterizzano e che lo rendono destinatario necessario di specifiche forme di tutela.

---

[21] In argomento, R. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Le nuove leggi civili commentate*, 5, 2017, pp. 1023 ss.; nonché già G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, RomaTr*E-Press*, Roma, 2015, *passim*.

13.3.1. I minori e l'offerta di servizi della società dell'informazione

L'art. 8 GDPR rappresenta attualmente la norma di riferimento in tema di consenso al trattamento di dati personali riferiti a minori di età.

Che la norma abbia una sfera di applicazione limitata, e non pretenda di definire delle condizioni generali di validità del consenso del minore al trattamento dei dati che lo riguardano, si evince già dalla rubrica. Il riferimento diretto ai «servizi della società dell'informazione», per la cui definizione occorre rinviare all'art. 1, § 1, lett. b) della direttiva (UE) 2015/1535[22], circoscrive infatti la portata della norma in questione, così potendosi riconoscere il fondamento di tale intervento di modernizzazione della disciplina privacy nell'esigenza di adeguare la normativa in materia all'attuale contesto sociale, in cui i minori fanno un uso sempre più ampio dei più diversi strumenti di tipo telematico. E, in questo modo, riconoscere finalmente loro una forma di autonomia nella gestione di sé e della propria identità digitale[23].

Peraltro, nell'ambito di questa categoria di servizi, il primo paragrafo dell'art. 8 GDPR precisa ulteriormente che la sfera applicativa della norma è limitata soltanto a quelli offerti *direttamente* a soggetti minori di età. Di conseguenza, laddove un prestatore di servizi della società dell'informazione renda evidente ai suoi potenziali utenti di volersi rivolgere a un pubblico composto esclusivamente da persone maggiorenni, e ciò non venga smentito da ulteriori elementi, il servizio

---

[22] Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione). La disposizione richiamata li definisce come quei servizi prestati «normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi», così riferendosi in particolare a quei servizi che consentono l'accesso a determinate informazioni, come banche dati o *newsletter*, o a strumenti di comunicazione, quali i servizi di posta elettronica o i *social network*.

[23] F. RESTA, *Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*, in G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, IPSOA, Milano, 2018, pp. 84-85.

offerto non potrà essere considerato come fornito *in modo diretto* ai minori e pertanto la norma non potrà trovare applicazione[24].

Anche questa scelta del legislatore europeo si spiega nell'esigenza di prestare tutela ai minori esposti ai rischi della rete e, al contempo, garantire loro un certo livello di autonomia. L'utilizzo generalizzato dei nuovi media consente infatti di considerarli destinatari diretti di offerte di beni e servizi, specie da parte delle grandi piattaforme di vendita *online* che, tramite i dati raccolti anche attraverso il semplice accesso alle loro pagine web, sono in grado di sfruttare a loro vantaggio le vulnerabilità di qualsiasi utente, a maggior ragione se minore. In questo senso, delle insidie particolarmente rilevanti discendono dall'attuazione di pratiche di profilazione, utili a ricostruire l'identità e le preferenze commerciali individuali di un determinato utente e, in forza di tale elaborazione, finalizzate a rivolgergli annunci pubblicitari personalizzati che sappiano incentivarne in modo soddisfacente le scelte di consumo[25].

L'opportunità di prevedere adeguate misure di protezione in ragione della indubbia vulnerabilità del minore nel contesto digitale è dunque evidente.

Tuttavia, al contempo, sarebbe irrealistico immaginare di non lasciare uno spazio di autonomia nella gestione di sé ai minori di oggi, nativi digitali, il cui utilizzo dei dispositivi connessi alla rete non è certamente limitato a mere attività ricreative[26]. Ed è quindi nell'ottica del bilanciamento tra esigenze di tutela e libertà di autodeterminazione operato dal legislatore europeo che occorre leggere la nuova disciplina

---

[24] F. NADDEO, *cit.*, p. 42. Questa precisazione non appare tuttavia sufficiente, di per sé, ai fini di risoluzione pratica dei problemi che potrebbero porsi in sede applicativa. In questo senso, un utile punto di riferimento sembra potersi individuare nella corrispondente disciplina vigente negli Stati Uniti, ove dal 1998 è in vigore il *Children's Online Privacy Protection Act* (COPPA), che al fine di verificare se un servizio è realmente diretto a un pubblico di minori di età, prende in considerazione al § 312.2 una precisa serie di fattori, quali l'oggetto del sito o del servizio proposto; i suoi contenuti visivi e audio; la rappresentazione di personaggi animati; l'immagine di personaggi famosi a loro volta minorenni o che, in ogni caso, si rivolgono ai bambini; il tipo di pubblicità che compare sul sito.

[25] Sul punto si rinvia a un recente documento elaborato dal Garante Privacy irlandese, che tratta l'argomento in maniera organica: DATA PROTECTION COMMISSION, *Fundamentals for a Child-Oriented Approach to Data Processing*, 2021, pp. 49 ss.

[26] Nello stesso senso, I. GARACI, *cit.*, p. 804, specie nella necessaria considerazione dell'attuale contesto di emergenza sanitaria.

relativa alla prestazione del consenso al trattamento dei dati personali del minore.

13.3.2. Consenso del minore e questioni in tema di capacità

Il primo paragrafo dell'art. 8 GDPR sancisce la validità del consenso prestato personalmente dal minore ultrasedicenne. Di contro, ove il minore abbia meno di sedici anni, il trattamento dei suoi dati personali è lecito soltanto se e nella misura in cui il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale.

In questo modo, la norma intende distinguere la posizione e il grado di autonomia del minore che fruisce di servizi in rete sulla base del raggiungimento di un certo anno di età[27]. E, all'interno di un disegno che in questo contesto sostanzialmente anticipa l'acquisto della capacità di agire probabilmente riconoscendo una forma di "maggiore età digitale", l'art. 1, § 2, GDPR ha concesso ai legislatori nazionali di stabilire un'età soglia diversa, benché non inferiore a tredici anni[28].

Con il nuovo art. 2-*quinquies* del Codice della privacy, aggiunto dal richiamato d. lgs. 101/2018, il legislatore italiano ha pertanto stabilito il limite di quattordici anni. Alla luce di tale scelta di sistema è allora possibile dare una nuova lettura al primo paragrafo dell'art. 8 GDPR e affermare che, nel nostro ordinamento nazionale, il trattamento dei dati personali di un minore è lecito se ad acconsentirvi personalmente sia un minore ultraquattordicenne. In caso contrario, la liceità del

---

[27] Sembra così volersi individuare diverse fasi della minore età: quella dei c.d. *petits enfants*, i bambini per così dire in senso stretto, per i quali prevalgono logiche di protezione; e quella dei c.d. *grands enfants*, i "grandi minori", ai quali riconoscere invece specifiche esigenze di libertà e autodeterminazione. Cfr. M. NITTI, *cit.*, p. 390.

[28] Tale previsione del regolamento rappresenta evidentemente una rinuncia da parte del legislatore europeo ad un maggior grado di uniformità della disciplina. Gli Stati membri, infatti, in sede di coordinamento della legge nazionale con la disciplina derivata, hanno utilizzato tutte le diverse opzioni di età compresa tra i tredici e i sedici anni, realizzandosi un'evitabile frammentazione che non giova al processo di integrazione europeo, né tantomeno agli stessi minori, trattati diversamente in base alla loro nazionalità, o ai titolari del trattamento dei dati personali, che di tale eterogeneità devono necessariamente tenere conto. Per alcuni riferimenti sulle scelte compiute dai principali Paesi europei, si veda G. CAPILLI, *cit.*, pp. 258-259.

consenso è subordinata all'intervento di chi ne abbia la responsabilità genitoriale, compreso il tutore[29].

Tale previsione, evidentemente, introduce nel nostro sistema normativo una nuova eccezione alla regola generale *ex* art. 2 c.c. per cui la capacità d'agire si acquista con il raggiungimento della maggiore età, e dunque con il compimento dei diciotto anni. E attribuisce così nuovo valore alla capacità di autodeterminazione del minore nello sviluppo della personalità, anche alla luce di quanto già sancito dalle Carte sovranazionali[30].

In quest'ottica, l'art. 2-*quinquies* del Codice della privacy sembra confinare la portata dell'art. 2 c.c. ai soli rapporti a contenuto patrimoniale, lasciando invece ampio spazio alla libertà decisionale del minore nel campo dei rapporti non patrimoniali e dell'esercizio dei diritti fondamentali[31]. D'altronde lo stesso art. 8 GDPR, nel legittimare il minore ultrasedicenne alla prestazione del consenso al trattamento dei propri dati personali, fa espressamente salve le disposizioni generali del diritto interno concernenti la validità e l'efficacia dei contratti stipulati dai minori di età. E tale previsione andrebbe intesa come intenzione di distinguere il consenso negoziale riferito agli atti a contenuto patrimoniale in senso stretto dal consenso al trattamento dei dati personali, da includere piuttosto nella sfera di esercizio dei diritti personali fondamentali[32].

Allo stesso modo, l'art. 8 GDPR non sembrerebbe peraltro rappresentare una completa anomalia del sistema, inserendosi in quel gruppo di norme che, ormai da tempo, hanno scardinato e reso in un certo senso più fluida la nozione civilistica della capacità d'agire[33]. Vi sono infatti diversi – e noti – esempi normativi di valorizzazione dell'autodeterminazione del minore rispetto a scelte che costituiscono forme di estrinsecazione della sua personalità. Si pensi alla capacità del

---

[29] F. NADDEO, *cit.*, p. 45.

[30] Cfr. V. BARBA, *Persone con disabilità e capacità. Art. 12 della Convenzione sui diritti delle Persone con Disabilità e diritto civile italiano*, in *Rassegna di diritto civile*, 2, 2021 pp. 441-442.

[31] C. IRTI, *Persona minore di età e libertà di autodeterminazione*, in *Giustizia civile*, 3, 2019, p. 644. In argomento, M. CINQUE, *Il minore contraente. Contesti e limiti della capacità*, Cedam, Padova, 2007.

[32] C. CAMARDI, *cit.*, p. 124.

[33] Sul «superamento del dogma dell'incapacità» del minore, si vedano già le riflessioni di G. RESTA, *Autonomia privata e diritti della personalità*, Jovene, Napoli, 2005, pp. 307 ss.

minore emancipato di contrarre matrimonio nei limiti e con i presupposti di cui all'art. 84 c.c.; in tema di riconoscimento del figlio minorenne, all'art. 250, comma 2, c.c., che ne richiede l'assenso quando questi abbia più di quattordici anni; al riconoscimento del diritto d'autore in capo al minore ultrasedicenne (art. 108 l. 22 aprile 1941, n. 633); alla disciplina sull'interruzione volontaria della gravidanza da parte della minorenne (art. 12 l. 22 maggio 1978, n. 194); alla richiesta del minore tossicodipendente di essere sottoposto ad accertamenti diagnostici e di definire un programma terapeutico e socio-riabilitativo (art. 120 d.P.R. 9 ottobre 1990, n. 309); alla scelta dello studente minorenne di scuola secondaria di avvalersi o meno dell'insegnamento della religione cattolica (art. 1, comma 1, l. 18 giugno 1986, n. 281).

Ebbene, il riconoscimento della maggiore autonomia del minore nel contesto digitale si ascrive in sostanza in un orientamento generale che ha caratterizzato importanti settori del diritto civile, comunemente riconducibili agli atti di estrinsecazione della personalità, nonché di partecipazione alla vita di relazione. Un processo anche culturale che, peraltro, attraverso il nuovo art. 315-*bis* c.c., introdotto dalla più recente l. 10 dicembre 2012, n. 219 di riforma del diritto della filiazione, ha portato a comprendere nell'impianto del Codice civile un diritto del minore ad autodeterminarsi, da ricondurre al concetto generale ed indeterminato della capacità di discernimento del minore quale capacità esclusiva di un soggetto che sta progressivamente pervenendo all'acquisizione del pieno esercizio di tutti i diritti soggettivi[34].

Rispetto al trattamento dei dati, nello specifico, può però rilevarsi ancora una volta una peculiare caratteristica. Ovvero che la rete enfatizza più che mai la contraddizione in cui si trovano minori di oggi: sempre più autonomi, da un lato; sempre più esposti al rischio, dall'altro. Indipendenti, ma vulnerabili; alla ricerca di libertà, ma bisognosi di tutela, nella vita virtuale ormai forse più che in quella reale[35].

---

[34] R. SENIGAGLIA, «*Consenso libero e informato» del minorenne tra capacità e identità*, in *Rassegna di diritto civile*, 4, 2018, p. 1324.

[35] Cfr. M. BIANCA, *cit.*, p. 158.

13.3.3. Consenso e autorizzazione genitoriale

La formulazione dell'art. 8 GDPR permette peraltro ulteriori considerazioni con riferimento alla posizione del minore – in Italia – infraquattordicenne. La norma pone infatti un'alternativa tra l'ipotesi di manifestazione di una volontà affermativa al trattamento dei dati del minore da parte dell'esercente la responsabilità genitoriale e il caso in cui questi si limiti ad autorizzare il minore stesso alla prestazione del consenso.

Si tratta evidentemente di due modelli distinti: il primo non attribuisce alcun ruolo al minore, che viene integralmente rappresentato da chi, nei suoi confronti, esercita la responsabilità genitoriale; il secondo subordina la validità del suo consenso all'autorizzazione del genitore o tutore, avente funzione integrativa di una capacità di agire del minore in parte effettivamente riconosciuta[36].

Nella pratica, tuttavia, non può non immaginarsi che un nativo digitale sia facilmente in grado di aggirare la richiesta, rivolta ai genitori, di prestazione del consenso in via sostitutiva o complementare della volontà del figlio. In assenza di strumenti di controllo, a tutela dei dati personali del minore, questi potrebbe senza difficoltà dichiarare da sé che i genitori non sono contrari al trattamento dei suoi dati.

Si pone in sostanza un problema di carattere pratico, ovvero di concreto accertamento dell'esistenza dei requisiti di validità del consenso, per la cui soluzione la norma in oggetto si affida apertamente al titolare del trattamento, ossia al soggetto che determina le finalità e gli strumenti del trattamento di dati personali[37].

L'art. 8, § 2, GDPR, richiede infatti proprio a quest'ultimo di adoperarsi «in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili», senza però precisare quali possano essere, almeno a titolo

---

[36] F. RESTA, *cit.*, p. 87. In entrambi i casi rileva peraltro la necessità che la decisione genitoriale venga sempre adottata nel rispetto del principio del *best interest of the child*, sul quale si rinvia *amplius* a V. SCALISI, *Il superiore interesse del minore ovvero il fatto come diritto*, in *Rivista di diritto civile*, 2, 2018, pp. 405 ss.

[37] A. ASTONE, *L'accesso dei minori d'età ai servizi della c.d. Società dell'informazione: l'art. 8 del Reg. (UE) 2016/679 e i suoi riflessi sul Codice per la protezione dei dati personali*, in *Contratto e impresa*, 2, 2019, pp. 632 ss.

esemplificativo, le modalità pratiche per l'acquisizione del consenso o dell'autorizzazione dei genitori[38].

Un tentativo, invero non sufficientemente definito, di dare maggiore nitidezza a tale disposizione è contenuto nelle Linee guida di accompagnamento al GDPR dedicate al consenso[39]. In questa sede viene generalmente raccomandata l'adozione di un approccio, in linea con il principio di minimizzazione dei dati, che miri ad ottenere una quantità di informazioni limitata (ad esempio i dettagli di contatto di un genitore), ma sempre in proporzione ai rischi inerenti al trattamento dei dati e alla tecnologia a disposizione del titolare. Così, sostanzialmente al fine di riconoscere la *ragionevolezza* degli sforzi compiuti dal titolare, si suggerisce, nei casi a basso rischio per la tutela del minore, una verifica a mezzo posta elettronica della volontà del genitore o tutore; nei casi ad alto rischio, invece, la richiesta di ulteriori prove, così che il titolare del trattamento possa non solo accertare il reale consenso genitoriale, ma anche conservare la relativa documentazione.

Tali raccomandazioni appaiono tuttavia piuttosto deboli, di limitata utilità per il titolare del trattamento dei dati personali chiamato ad adottare misure concrete ed efficaci a tutela dei minori. Il quale avrebbe forse avuto bisogno, in questo caso, di un maggior grado di determinatezza, per potersi muovere entro confini più certi. Se infatti i metodi di verifica più contenuti, come quelli fondati sulla posta elettronica, sono facilmente eludibili dal minore, quelli più rigorosi, ad esempio la richiesta di utilizzo delle carte di credito, possono essere poco graditi ai genitori, oltre che costosi per il gestore del servizio. Dall'indicazione almeno parziale di tali meccanismi, insomma, avrebbero tratto beneficio tanto i destinatari quanto i titolari del trattamento

[38] Anche sotto questo profilo, la prospettiva comparatistica può agevolare concretamente il compito del giurista in sede applicativa. La corrispettiva disciplina vigente negli Stati Uniti permette infatti di immaginare alcune soluzioni pratiche di verifica del consenso o dell'autorizzazione genitoriale al trattamento dei dati di un minore (§ 312.5 COPPA). In particolare: fornendo ai genitori un modulo per il consenso da compilare e inviare al titolare del trattamento via fax o mail; chiedendo loro di utilizzare carte di credito o di debito o altri sistemi di pagamento elettronico; o di confermare direttamente il proprio consenso a personale qualificato del titolare del trattamento, tramite una telefonata a un numero verde o un collegamento via *webcam*; o di presentare una copia di un documento di identità; o di rispondere a domande specifiche cui solo un genitore può essere in grado di rispondere; impiegando appositi applicativi digitali di riconoscimento facciale attraverso l'accostamento di immagini.

[39] Si tratta delle Linee guida sul consenso ai sensi del regolamento (UE) 2016/679 adottate dal Gruppo di lavoro Articolo 29 (in particolare, pp. 29-30).

dei dati.

In questa situazione di incertezza, un ruolo fondamentale appare dunque rimesso al Garante Privacy, chiamato a valutarne di volta in volta l'adeguatezza in concreto a tutela dei minori[40].

Da ultimo, ancora con riferimento al minore infraquattordicenne, preme rilevare che, al compimento del quattordicesimo anno di età, il consenso al trattamento dei dati prestato dall'esercente la responsabilità genitoriale deve essere necessariamente confermato, modificato o revocato da parte del minore stesso. Il raggiungimento dell'età del consenso digitale comporta infatti il conseguimento di un controllo pieno sul trattamento che lo interessa personalmente e richiede pertanto una sua decisione libera e diretta. A tal fine, in conformità con i principi di correttezza e *accountability*, il titolare del trattamento è tenuto ad informare il minore di tali possibilità, nonché di quella di esercitare il diritto all'oblio ai sensi dell'art. 17, § 1, lett. f), GDPR e pretendere la cancellazione «senza ingiustificato ritardo» dei dati personali che lo riguardano.

13.3.4. Consenso privacy e diritto dei contratti

Alcune osservazioni conclusive sul terzo e ultimo paragrafo dell'art. 8 GDPR, ai sensi del quale la nuova disciplina sulla prestazione del consenso «non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore»[41].

In questo senso, può infatti emergere la necessità di un

---

[40] Si pensi, da ultimo, al provvedimento del Garante del 22 gennaio 2021, riferito al caso TikTok. L'Autorità ha infatti vietato al *social network* cinese «l'ulteriore trattamento dei dati degli utenti che si trovano sul territorio italiano per i quali non vi sia l'assoluta certezza dell'età e, conseguentemente, del rispetto delle disposizioni collegate al requisito anagrafico», spingendolo all'utilizzo di sistemi di intelligenza artificiale di "*age verification*". Il riferimento a tali strumenti di verifica è presente anche nel citato documento (*supra*, nota 25) della Data Protection Commission, p. 46.

[41] Sulla disciplina di alcuni ordinamenti nazionali europei in materia, si veda P. STANZIONE, *I contratti del minore*, in *Europa e diritto privato*, 4, 2014, pp. 1263 ss. Cfr. anche D. DI SABATO, *Le relazioni economiche del minore*, in *Diritto delle successioni e della famiglia*, 3, 2015, p. 711.

coordinamento della disciplina sui requisiti del consenso privacy con quella – di diritto interno – sui presupposti di validità ed efficacia del contratto, in tutti quei casi in cui il trattamento dei dati personali costituisca, almeno in parte, l'oggetto della prestazione dedotta nel contratto. Ad esempio, quando l'accesso a un servizio telematico postuli la prestazione del consenso al trattamento dei dati personali per finalità promozionali[42]. Ebbene, se il minore ha compiuto l'età del consenso digitale, ma non quella richiesta dalla legge nazionale in materia contrattuale, la liceità del trattamento non potrà che essere travolta dal vittorioso esperimento dell'azione di annullamento del contratto[43].

Potrebbe invero verificarsi anche l'ipotesi opposta di un minore in grado di concludere validamente un contratto, in particolare se relativo al soddisfacimento dei bisogni della vita quotidiana[44], ma che non abbia ancora raggiunto l'età del consenso digitale. Ciò in quanto il trattamento non sia necessario all'esecuzione del contratto (art. 6, § 1, lett. b), GDPR). Sicché può dirsi che l'autonoma rilevanza dei due consensi, quello privacy, da un lato, e quello negoziale, dall'altro, comporti che il trattamento dei dati personali non possa essere considerato lecito per il solo fatto di essere riferito all'esecuzione di un contratto valido[45].

---

[42] E. BATTELLI, *Il contratto di accesso ad Internet*, in *Medialaws*, 1, 2021, pp. 147 ss.

[43] F. NADDEO, *cit.*, p. 50.

[44] Cfr. G. ALPA, *Il contratto in generale. Fonti, teorie, metodi*, in P. SCHLESINGER (diretto da), *Trattato di diritto civile e commerciale*, Giuffrè, Milano, 2014, pp. 752-753.

[45] I.A. CAGGIANO, *Privacy e minori nell'era digitale. Il consenso al trattamento dei dati dei minori all'indomani del Regolamento UE 2016/679, tra diritto e tecno-regolazione*, in *Familia*, 1, 2018, pp. 3 ss.

14. Gli *smart contracts* nel settore finanziario: questioni irrisolte e prospettive regolatorie fra diritto nazionale e sovranazionale

Emanuele Tuccari (Università di Pavia)

14.1 Il problema

La diffusione degli *smart contract*[1], delle *ICO* (*Initial Coin Offering*) e delle *IEO* (*Initial Exchange Offering*) nel settore finanziario fornisce una

[1] Per alcune considerazioni di carattere generale sull'argomento, con impostazioni fisiologicamente anche molto diverse fra loro, cfr., *ex multis*, I. MARTONE, *Gli* smart contracts. *Fenomenologia e funzioni*, Napoli, 2022, p. 13 ss.; M. MAUGERI, voce Smart contracts, in *Enc. dir., I Tematici – Il contratto*, I, Milano, 2021, p. 1132 ss.; EAD., Smart contracts *e disciplina dei contratti*, Bologna, 2021, p. 15 ss.; EAD., Smart contracts *e disciplina dei contratti*, in *Oss. dir. civ. comm.*, 2020, p. 375 ss.; S. ORLANDO, *Gli* smart contracts *come prodotti* software, in S. ORLANDO e G. CAPALDO (a cura di), *Annuario 2021 – Osservatorio Giuridico sulla Innovazione Digitale*, Roma, 2021, p. 235 ss.; ID., *Profili definitori degli "smart contracts"*, in AA.VV., *Internet, contratto e persona: quale futuro?*, a cura di R. CLARIZIA, Pisa, 2021, p. 41 ss.; A.U. JANSSEN, F.P. PATTI, *Demistificare gli* smart contracts, in *Oss. dir. civ. e comm.*, 2020, p. 31 ss.; F. RAMPONE, Smart contract*: né* smart*, né* contract, in *Riv. dir. priv.*, 2020, p. 241 ss.; A. STAZI, *Automazione contrattuale e «contratti intelligenti»*, Torino, 2019; F. DELFINI, Blockchain, smart contracts *e innovazione tecnologica: l'informatica e il diritto dei contratti*, in *Riv. dir. priv.*, 2019, p. 176 ss.; G. SALITO, voce *Smart contracts*, in *Dig. disc. priv., sez. civ.*, agg. XII, Torino, 2019, p. 393 ss.; G. CASTELLANI, Smart contracts *e profili di diritto civile*, in *Comparazione e diritto civile*, 2019, p. 1 ss.; T. PELLEGRINI, *Prestazioni auto-esecutive.* Smart contract *e dintorni*, in *Comparazione e diritto civile*, 2019, p. 843 ss.; C. PERNICE, Smart contract *e automazione contrattuale: potenzialità e rischi della negoziazione algoritmica nell'era digitale*, in *Dir. mercato ass. e fin.*, 2019, p. 117 ss.; L. PAROLA, P. MERATI, G. GAVOTTI, Blockchain *e* smart contract*: questioni giuridiche aperte*, in *I Contratti*, 2018, p. 681 ss.; D. DI SABATO, *Gli* smart contracts*:* robot *che gestiscono il rischio contrattuale*, in *Contr. impr.*, 2017, p. 378 ss.; P. CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in *Nuova giur. civ. comm.*, 2017, II, p. 107 ss. Sull'applicazione (più specifica) degli *smart contract* nell'ambito bancario e finanziario, cfr. G. ALPA, Fintech*: un laboratorio per i giuristi*, in *Contr. e impr.*, 2019, p. 377 ss.; A. CINQUE, *Gli* smart contract *nell'ambito del*

prospettiva privilegiata (e ricca di spunti di riflessione) sui controversi rapporti fra diritto (pubblico e privato) e tecnologia[2].

Le *ICO* servono a raccogliere rapidamente risorse economiche in cambio di rappresentazioni digitali di valori (cc.dd. «token»). Le principali caratteristiche delle *ICO*, seppur in assenza, ancor oggi, di condivise definizioni normative, sono rintracciabili nella pubblicazione sul sito dell'emittente di una sorta di prospetto (c.d. «white paper») – contenente la descrizione (più o meno dettagliata) del progetto imprenditoriale (dal programma d'investimento, alle caratteristiche del prodotto e dei *token*, passando per la composizione del *team* che lavora sul progetto e per i tempi di svolgimento) – e dell'offerta – diretta ad un numero indefinito di destinatari. Quest'offerta è funzionale, più specificamente, proprio a finanziare il progetto presentato attraverso l'acquisto, in moneta o criptovaluta (per esempio, *bitcoin*)[3], di un certo numero di *token* (che possono, di volta in volta, dare diritto a servizi, azioni od obbligazioni oppure operare come mezzo di scambio fra gli investitori oppure ancora svolgere una pluralità delle suddette funzioni). La sottoscrizione dei *token* avviene attraverso un processo automatizzato e compiuto all'interno di un sistema *DLT* (*Distributed Ledger Technology*); se, alla scadenza del termine, la raccolta raggiunge l'ammontare minimo prefissato, si attribuiscono i *token* ai sottoscrittori attraverso l'attivazione degli *smart contract* collegati alla *ICO*; se, invece,

---

FinTech *e dell'*InsurTech, in *Jus civile*, 2021, p. 187 ss.; E. BATTELLI, E.M. INCUTTI, *Gli* smarts contracts *nel diritto bancario tra esigenze di tutela e innovativi profili di applicazione*, in *Contr. e impr.*, 2019, p. 925 ss.

[2] Sulle problematiche specifiche delle *ICO*, cfr. G. GITTI, M. MAUGERI, *Blockchain – Based Financial Service and Virtual Currencies in Italy*, in *EuCML*, 2020, p. 43 ss.; G. GITTI, M. MAUGERI, C. FERRARI, *Offerte iniziali e scambi di cripto-attività*, in *Oss. dir. civ. comm.*, 2019, p. 95 ss.; C. SANDEI, *Le* Initial Coin Offering *nel prisma dell'ordinamento finanziario*, in *Riv. dir. civ.*, 2020, p. 391 ss.; A. SCIARRONE ALIBRANDI, *Offerte iniziali e scambi di cripto attività: il nuovo approccio regolatorio della Consob*, aprile 2019, in *dirittobancario.it*; G. GITTI, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca borsa tit. cred.*, 2020, p. 13 ss.

[3] Per un approfondimento sul fenomeno delle criptovalute (con una particolar attenzione anche ai *bitcoin*), si rinvia alle riflessioni, caratterizzate da approcci metodologici ed esiti anche significativamente diversi fra loro, di M. CIAN, *La criptovaluta – Alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca, borsa, tit. cred.*, 2019, p. 315 ss.; M. F. CAMPAGNA, *Criptomonete e obbligazioni pecuniarie*, in *Riv. dir. civ.*, 2019, p. 183 ss.; A. CALONI, Bitcoin*: profili civilistici e tutela dell'investitore*, in *Riv. dir. civ.*, 2019, p. 159 ss.; C. PERNICE, Digital currency *e obbligazioni pecuniarie*, Napoli, 2018, p. 199 ss.; N. VARDI, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei* bitcoin, in *Dir. inf. informatica*, 2015, p. 443 ss.

l'offerta (e, quindi, la raccolta) fallisce, i fondi vengono automaticamente restituiti ai singoli sottoscrittori[4].

A seguito però di (numerose) truffe – rese possibili anche dalle difficoltà d'identificare i soggetti coinvolti nell'operazione – gli investitori preferiscono recentemente orientarsi spesso verso scambi più sicuri perché realizzati tramite siti di negoziazione (cc.dd. «exchanges»), che, perlomeno in parte, dovrebbero amministrare la raccolta fondi e provvedere all'identificazione delle parti (cc.dd. «IEO»).

14.2. Necessarie premesse "tecnologiche" e "metodologiche"

Nell'ottica non soltanto di comprendere le specifiche problematiche degli *smart contract* nel settore finanziario, ma anche d'ipotizzarne un'eventuale disciplina, sembra però necessario chiarire, seppur in estrema sintesi, taluni profili preliminari.

Se l'idea di *smart contract* poteva ridursi, in origine, soltanto a protocolli computerizzati capaci di eseguire i termini di un contratto[5], l'odierna descrizione dei caratteri fondamentali di uno *smart contract* risulta decisamente più complessa e presuppone, a sua volta, perlomeno un'essenziale definizione di alcuni concetti tecnologici.

Si tratta di chiarire, in particolare, cosa s'intenda per *DLT* (e per *blockchain*)[6].

Le *DLT* – ai sensi dell'art. 8-*ter*, comma 1, del decreto legge 14 dicembre 2018, n. 135, come convertito dalla legge 11 febbraio 2019, n. 12 (c.d. «Decreto Semplificazioni») – sono tecnologie e protocolli informatici «che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non

---

[4] Per un inquadramento chiaro del fenomeno delle *ICO*, cfr., per tutti, C. SANDEI, *Le* Initial Coin Offering *nel prisma dell'ordinamento finanziario*, cit., spec. 392 ss.

[5] Cfr., per tutti, N. SZABO, *Smart contracts*, 1994, reperibile *online*: *https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html*.

[6] Per una panoramica su tali profili tecnologici (e poi sulle loro possibili conseguenze giuridiche), cfr., *ex multis*, F. P. PATTI, Blockchain, smart contracts *e criptovalute*, in AA.VV., *Manuale di diritto privato delle nuove tecnologie*, a cura di G. MAGRI, S. MARTINELLI e S. THOBANI, Torino, 2022, p. 255 ss.; A. SARDINI, *La «moneta» contrattuale*, in *Nuovo dir. civ.*, 2020, p. 167 ss., spec. p. 172.

alterabili e non modificabili»[7]. S'identifica così una tecnologia che consente la registrazione e la conservazione di dati attraverso archivi multipli (*ledger*), ognuno dei quali contiene contemporaneamente gli stessi dati che sono conservati e controllati da una rete di *computer* (che finiscono così per costituire una sorta di «nodi» della «rete»). La *blockchain* (letteralmente «catena di blocchi») è, a sua volta, una *species* (decisamente la più conosciuta e diffusa) del *genus DLT*.

Nell'attuale panorama, tenuto conto dell'odierna evoluzione tecnologica (e normativa), gli *smart contract* – definiti, a loro volta, dallo stesso art. 8-*ter*, comma 2, del c.d. «Decreto Semplificazioni» – si avvalgono spesso (ma non sempre) di una *DLT* (e, in particolare, di una *blockchain*)[8]. Nonostante pertanto gli *smart contract* rappresentino, com'è stato autorevolmente sostenuto, perlopiù dei prodotti *software* (e siano solitamente così identificati e considerati anche dai tecnici del settore)[9], talvolta – quando (come legislativamente previsto)[10] operano su *DLT* e riguardano accordi, comprensibili ad entrambe le parti (che decidono così specificamente di vincolarsi), sullo scambio o mere esecuzioni o altro ancora (per esempio, l'iscrizione di domini) – finiscono

[7] La definizione, in apparenza molto semplice e lineare, rischia però di risultare semplicistica. V., per tutti, E. LABELLA, *Gli* smart contract*: riflessioni sulle prestazioni "autoesecutive" nel sistema di* blockchain, in *Media Laws*, 2020, p. 34 ss.

[8] Cfr., *ex multis*, G. REMOTTI, Blockchain smart contract*. Un primo inquadramento*, in *Oss. dir. civ. comm.*, 2020, p. 189 ss.; G. ALHARBY E A. VAN MOORSEL, *Blockchain-Based Smart Contracts: A Systematic Mapping Study*, in *Computer Science & Information Technology*, 2017, p. 125 ss., spec. p. 127.

[9] Così S. ORLANDO, *Gli* smart contracts *come prodotti* software, cit., p. 249 ss.; ID., *Profili definitori degli "smart contracts"*, cit., p. 51 ss.

[10] Lo stesso art. 8-*ter*, comma 2, del c.d. «Decreto Semplificazioni» sembra, dapprima, metter in dubbio la natura contrattuale dello *smart contract* (descritto come «un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse»), per considerarla, subito dopo, presunta a proposito dell'identificazione delle parti interessate per soddisfare il requisito della forma scritta («gli *smart contract* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con le linee guida da adottare […]»).

per assumere – secondo la posizione oggi prevalente in dottrina[11] – natura contrattuale[12].

Alle premesse, per così dire, "tecnologiche" devono però affiancarsi delle considerazioni, anch'esse preliminari, di carattere "metodologico".

Nell'odierno scenario – contraddistinto non soltanto dalle conseguenze della crisi finanziaria del 2008, ma anche dalle difficoltà derivanti dalla pandemia da *COVID-19* – sembra difficile riaffermare con assoluta certezza (tanto sul piano teorico quanto su quello pratico) la generale capacità del mercato (e, a maggior ragione, del mercato finanziario) di auto-regolarsi. Si ripropongono pertanto ricette caratterizzate dalla centralità dell'azione pubblica senza però riassegnare

[11] Nell'ormai ampio dibattito dottrinale sembrano favorevoli a sostenere, seppure con alcune rilevanti (e opportune) distinzioni fra le diverse figure di *smart contract*, la natura contrattuale M. MAUGERI, voce Smart contracts, cit., p. 1139 ss., spec. p. 1142; EAD., Smart contracts *e disciplina dei contratti*, cit., p. 15 ss.; EAD., Smart contracts *e disciplina dei contratti*, cit., p. 375 ss.; G. REMOTTI, Blockchain smart contract*. Un primo inquadramento*, cit., p. 189 ss.; E. PERNICE, Software *o contratto? Tentativo di applicazione delle norme sulla teoria generale del contratto*, in *Ciberspazio e diritto*, 2022, 49 ss. Sollevano significative perplessità (riconducibili, fra l'altro, alla c.d. «asimmetria informatica») sulla natura contrattuale "generale" degli *smart contracts* S. ORLANDO, *Gli* smart contracts *come prodotti* software, cit., spec. p. 249 ss.; ID., *Profili definitori degli "smart contracts"*, cit., spec. p. 51 ss.; F. RAMPONE, Smart contract*: né* smart*, né* contract, cit., p. 241 ss. Per una prospettiva sovranazionale, cfr. L.A. DI MATTEO, M. CANNARSA, C. PONCIBÒ, *Smart contracts and Contract law*, in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, Cambridge, 2019, p. 3 ss.; M. DUROVIC, A.U. JANSSEN, *The formations of Blockchain-based Smart Contracts in the Light of Contract Law*, in 26 *European Review of Private Law*, 2018, p. 756 ss.

[12] Anche S. ORLANDO (*Gli* smart contracts *come prodotti* software, cit., p. 254) riconosce, però, come talvolta, seppur eccezionalmente, gli *smart contract* possano assumere natura contrattuale ("Fermo restando quanto sopra, ed anzi a conferma del valore generale della superiore conclusione, dovrà riconoscersi anche che, se non può deviarsi in termini generali dalla medesima conclusione (per la valenza a sua volta generale dell'asimmetria informatica, nel senso illustrato), ciò non vale ad escludere anche l'ipotesi che una conclusione diversa, che ammetta la possibilità della conclusione di smart contracts intesi come contratti (…), possa rinvenirsi in casi particolari, da asseverarsi di volta in volta. In particolare, laddove sia possibile riscontrare l'assenza di una asimmetria informatica e la volontà di entrambi i contraenti di vincolarsi esattamente al contenuto contrattuale come espresso da un programma per elaboratore. Simili accordi possono per il vero perseguire finalità di certezza, senz'altro meritevoli di tutela"). Per un'altra recente riflessione sulla qualificazione giuridica degli *smart contract*, cfr., I. MARTONE, *Gli* smart contracts*. Fenomenologia e funzioni*, cit., 71 ss.

un'assoluta (e rinnovata) centralità al c.d. «Stato-imprenditore» per almeno tre fondamentali ordini di ragioni[13].

Innanzitutto, la crisi ha dimostrato che la regolazione dei fenomeni finanziari dev'essere coerente con l'integrazione dei mercati e, pertanto, coordinata non soltanto a livello nazionale, ma anche sovranazionale[14].

Il secondo ordine di ragioni attiene alle modalità dell'intervento pubblico che si risolve recentemente in un insieme complesso di provvedimenti graduati e strategici che vedono lo Stato nella veste talvolta di prestatore di ultima istanza, di assuntore di garanzie e di rischi, talaltra di socio o di sottoscrittore di strumenti finanziari[15].

Il terzo ordine di ragioni riguarda, infine, la tecnica normativa, che risulta anch'essa sensibilmente diversa dal passato. Emergono modelli normativi complessi, affidati normalmente ad autorità indipendenti, «che importano un coacervo articolato e dinamico di rimedi, cui appartengono norme asimmetriche tra operatori, regole procedurali, sanzioni interdittive»[16]. La regolazione del mercato risulta pertanto, sempre più spesso, frutto non più soltanto della disciplina marcatamente pubblicistica, ma anche del ricorso a diversi strumenti di natura privatistica.

---

[13] Cfr. A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020, p. 243 ss. (recensito da A. M. BENEDETTI in *Riv. dir. civ.*, 2021, p. 608 ss.). Per altre affascinanti (e recenti) riflessioni sull'argomento, seppur alla luce dell'applicazione di metodi piuttosto diversi fra loro, si rinvia a B. SORDI, *Diritto pubblico e diritto privato. Una genealogia storica*, Bologna, 2020, p. 211 ss.; G. AMATO, *Bentornato Stato, ma*, Bologna, 2022, p. 9 ss., 57 ss., 93 ss.

[14] Nella stessa direzione si muovono, anche con riferimento ai profili più civilistici, le considerazioni di A.M. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari*, in *Riv. dir. civ.*, 2021, p. 411 ss., spec. pp. 425-426.

[15] L'intervento pubblico nell'economia ha di recente trovato, fra l'altro, nuova linfa attraverso l'ampiamento delle funzioni della Cassa Depositi e Prestiti. Per una primissima panoramica, può rinviarsi al sito istituzionale di CDP: *https://www.cdp.it/*. Qui possono trovarsi, fra l'altro, la ricostruzione dell'attività (passata, presente e futura) svolta dall'istituto (compresi diversi *report* annuali e semestrali nonché il Piano Strategico 2022-2024). In letteratura, per un'interessante analisi, cfr., *ex multis*, P. BRICCO, *Cassa Depositi e Prestiti. Storia di un capitale dinamico e paziente da 170 anni*, Bologna, 2020; A. DONATO, *Il ruolo di* holding *di Cassa depositi e prestiti S.p.A.: profili giuridici attuali della gestione di partecipazioni come strumento di politica industriale*, in *AGE*, 2015, p. 367 ss.

[16] A. ZOPPINI, *Il diritto privato e i suoi confini*, cit., p. 243.

14.3. Prospettive nazionali

Nell'intento di cominciare a comprendere le caratteristiche fondamentali di modelli normativi complessi – e perlopiù ancor oggi *in fieri* – sembra necessario monitorare con attenzione soprattutto l'attività delle diverse autorità (indipendenti) di vigilanza dei mercati finanziari dei singoli Paesi.

In Italia, l'attività della CONSOB (Commissione Nazionale per le Società e la Borsa) si è finora sviluppata in una duplice direzione: l'autorità di vigilanza, per un verso, ha ventilato la riconduzione di talune criptoattività nell'insieme degli strumenti finanziari (ai sensi della disciplina *MiFID II*) o dei prodotti d'investimento (le cui relative attività di emissione, negoziazione e post-negoziazione sono, come noto, soggette alle disposizioni europee di armonizzazione previste per gli strumenti finanziari e per i prodotti di investimento), per un altro, ha ventilato l'eventualità di una prossima specifica regolazione *ad hoc* per investimenti diversi da strumenti finanziari e da prodotti di investimento assicurativi e preassembleati. Quest'ultima prospettiva poggia, a sua volta, prevalentemente su due ragioni che sembrano tali da suggerire un'attenzione particolare: la prima è data proprio dai significativi elementi di similitudine dei fenomeni interessati con le offerte pubbliche di strumenti e prodotti finanziari; la seconda ragione è fornita dalla rappresentazione dei rapporti giuridici in *token*, presentando così profili di analogia con l'incorporazione dei diritti del sottoscrittore in un certificato, che costituisce titolo di legittimazione per il loro esercizio, ma anche uno strumento per una più agevole trasferibilità dei medesimi[17].

Si è così assistito all'elaborazione di un originario documento della CONSOB (19 marzo 2019)[18], poi seguito da un'ampia fase di consultazioni – aperta a numerosi esperti del settore e conclusasi il 5 giugno 2019 – ed infine dalla predisposizione di un Rapporto finale (2 gennaio 2020)[19].

---

[17] Sulle ragioni d'interesse per il fenomeno può leggersi direttamente l'originario documento predisposto dalla CONSOB (cfr. *Le offerte iniziali e gli scambi di cripto-attività*, Documento per la discussione, 19 marzo 2019, in *https://www.consob.it/documents/46180/46181/doc_disc_20190319.pdf/64251cef-d363-4442-9685-e9ff665323cf*, p. 2).

[18] Cfr. CONSOB, *Le offerte iniziali e gli scambi di cripto-attività*, Documento per la discussione, cit.

[19] Cfr. CONSOB, *Le offerte iniziali e gli scambi di cripto-attività*, Rapporto finale, 2 gennaio 2020, in *https://www.consob.it/documents/46180/46181/ICOs_rapp_fin_20200102.pdf/70466207-edb2-4b0f-ac35-dd8449a4baf1*.

Tale rapporto, seppur ancora lontano dall'essere considerato diritto vigente, contribuisce sicuramente ad intuire possibili sviluppi dei contenuti fondamentali della disciplina. S'intende procedere ad una regolazione non vincolante delle *ICO*, delle *IEO* e (più genericamente) degli scambi di criptoattività mediante una disciplina basata sul meccanismo dell'*opt-in*. A tal fine, una forma d'incentivo ad accedere (e, pertanto, a sottoporsi alla disciplina regolatoria) potrebbe essere rappresentata dalla previsione, in corrispondenza dell'applicazione del regime speciale ad offerte di cripto-attività che siano idonee ad integrare la nozione domestica di prodotto finanziario, di una deroga, di carattere premiale, rispetto alla disciplina dell'offerta al pubblico e dell'offerta a distanza di prodotti finanziari.

L'esigenza di regolare rapidamente il fenomeno delle criptoattività, soprattutto per evitare frodi (addebitabili spesso anche all'insufficiente sicurezza delle piattaforme di *trading*), risulta peraltro confermata dal rapporto del 3 agosto 2021 dell'autorità di vigilanza («Congiuntura e rischi del sistema finanziario italiano in una prospettiva comparata»)[20].

Quest'attenzione crescente – normativa e regolamentare – nei confronti delle criptoattività sembra trovare conferma nei principali sistemi giuridici nazionali del continente europeo[21].

Nel Regno Unito, la *task force* congiunta fra *HM Treasury*, *Financial Conduct Authority* (FCA) e *Bank of England* – costituita in materia di

[20] Il rapporto è reperibile *online* sul sito ufficiale della CONSOB: *https://www.consob.it/documents/46180/46181/Congiuntura2021.pdf/2984d324-f20e-47a6-96b1-92fa53f88c32* (v. spec. pp. 8-9, p. 103 ss.). L'attenzione costante della CONSOB all'applicazione delle nuove tecnologie (e, in particolar modo, delle *DLT*) nelle materie di sua competenza è dimostrata, fra l'altro, dalla pubblicazione di uno specifico «Quaderno giuridico» nel maggio 2022: AA.VV., *Gli sviluppi tecnologici del diritto societario*, a cura di M. BIANCHINI, G. GASPARRI, G. RESTA, G. TROVATORE, A. ZOPPINI, Roma, 2022 (anch'esso reperibile *online* sul sito ufficiale della CONSOB: *https://www.consob.it/documents/46180/46181/qg23.pdf/657d5505-966c-421f-a8a8-2b12581ebd35*).

[21] Le medesime problematiche, seppure non affrontabili esaustivamente in questa sede, si sono poste chiaramente anche in altri Paesi. Per una prima panoramica, per esempio, sull'evoluzione del sistema statunitense (anch'esso in costante sviluppo), cfr. L.A. DI MATTEO, J.C. JIANG, *Blockchain-Based Financial Services and Virtual Currencies: United States*, in *EuCML*, 2019, p. 251 ss.; e, nella nostra letteratura, M. MAUGERI, voce Smart contracts, cit., spec. p. 1137 ss. Anche l'approccio del Governo cinese, che ha proibito lo scambio di criptovalute e l'*ICO*, sembra poter assumere un ruolo non indifferente nell'evoluzione futura del fenomeno (e della sua regolazione sovranazionale) (cfr. D. I. OKORIE, B. LIN, *Did China's ICO ban alter the Bitcoin market?*, in *International Review of Economics & Finance*, 2020, p. 977 ss.).

crypto-asset – ha elaborato, già a partire dall'ottobre 2018[22], dei rapporti (aperti a diverse consultazioni degli operatori del mercato) nei quali, dopo avere esaminato rischi e potenziali benefici dei *crypto-asset* e dell'uso di tecnologia *distributed ledger*, ha esposto piano di azione e prese di posizione delle Autorità (soprattutto della FCA). Ancor oggi, però, il Regno Unito risulta privo di un'espressa disciplina legislativa: l'attività regolatoria sembra caratterizzata da un approccio pragmatico, orientato, al contempo, ad incentivare il *business* legato alla "finanza digitale" – come desumibile dalle prese di posizione pubbliche dell'ex Cancelliere dello Scacchiere (oggi Primo Ministro) Rishi Sunak[23] e dalla documentazione ufficiale prodotta dal Ministero del Tesoro all'esito della consultazione pubblica su *cryptoassets*, *stablecoins* e *distributed ledger technology* nei mercati finanziari[24] – e a declinare – alla luce, di volta in volta, dei possibili soggetti e delle diverse funzioni esercitate dai singoli *token* concretamente scambiati – il principio generale del «same risk, same regulatory outcome»[25].

Anche l'approccio regolamentare dell'Autorità di vigilanza tedesca (*Bundesanstalt für Finanzdienstleistungsaufsicht*, *BaFin*) ha lungamente fatto a meno di un espresso intervento legislativo nazionale, preferendo valutare la specifica funzione svolta dal *token* scambiato nel caso concreto. Già una circolare del 20 febbraio 2018 (poi confermata da una successiva del 18 agosto 2019) dell'Autorità faceva però rientrare – nonostante talune pronunce giurisprudenziali contrarie[26] – i *token* d'investimento nella nozione di «strumento finanziario», classificando peraltro contestualmente le *ICO* come operazioni capaci di creare delle

[22] Per il testo del primo rapporto della *task force* dell'ottobre 2018, cfr. *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf*.

[23] Sul punto, v. il *Mansion House speech 2021* (ancor oggi reperibile *online* nella sua trascrizione originale: *https://www.gov.uk/government/speeches/mansion-house-speech-2021-rishi-sunak*).

[24] Il documento del Ministero del Tesoro, stilato nell'aprile 2022, risulta regolarmente reperibile *online*: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088774/O-S_Stablecoins_consultation_response.pdf.

[25] Per una puntuale (e, al contempo, sintetica) panoramica dell'evoluzione della disciplina britannica sulle criptoattività con i principali documenti elaborati, negli ultimi anni, dalla *task force* e dalla FCA, cfr. *https://www.fca.org.uk/firms/cryptoassets*. In letteratura, cfr. M. DUROVIC, F. LECH, *The enforceability of smart contract*, in *Italian Law Journal*, 2019, p. 493 ss.

[26] V. App. Berlino 25 Settembre 2018 (cfr. *https://www.morganlewis.com/pubs/2019/09/the-regulation-of-icos-in-germany*).

securities e gli *exchange* come sistemi multilaterali di negoziazione[27]. Ne derivava l'esigenza di prevedere un prospetto e, più genericamente, di osservare la (già preesistente) disciplina finanziaria. Quest'impostazione ha poi trovato conferma legislativa, a partire dall'inizio del 2020, con l'introduzione di nuove regole, di matrice eurounitaria[28], di contrasto al riciclaggio di denaro (tramite l'approvazione della *Gesetz zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie*) nonché di modifiche della legge bancaria tedesca (*Kreditwesengesetz – KWG*). Sono stati così, fra l'altro, legislativamente definiti e classificati i *crypto-asset* – considerati complessivamente come strumenti finanziari[29] (non è così, invece, per i cc.dd. "utility token")[30] – ed è stata prevista una nuova di disciplina per i servizi di custodia[31]. Ai *crypto-asset*

---

[27] Per una riflessione sull'approccio regolatorio tedesco, prima delle modifiche legislative riportate poi nel testo, cfr. E. M. INCUTTI, «Initial Coin Offering» *ed il mercato delle cripto-attività: riflessioni sugli* «utility token», in S. ORLANDO e G. CAPALDO (a cura di), *Annuario 2021 – Osservatorio Giuridico sulla Innovazione Digitale*, Roma, 2021, pp. 193-194; ID., «Initial Coin Offering» *ed il mercato delle cripto-attività: l'ambiguità degli* «utility token», in *Riv. dir. priv.*, 2022, p. 86; E. RULLI, *Incorporazione senza res e dematerializzazione senza accentratore: appunti sui token,* in *Orizzonti del diritto commerciale,* 2019, p. 136 e ss.

[28] Si tratta, in particolare, del recepimento nell'ordinamento tedesco della direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018, che, a sua volta, modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/138/CE e 2013/36/UE. Il testo ufficiale della direttiva è reperibile *online*: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32018L0843*.

[29] Secondo la sezione 1, § 1, 11, della legge bancaria tedesca (*KWG*) i *crypto-asset* sono rappresentazioni digitali di un valore che non è stato emesso o garantito da una banca centrale o da un ente pubblico e non ha lo *status* giuridico di una valuta o di una moneta, ma è accettato da persone fisiche o giuridiche come *mezzo di scambio o di pagamento o serve a scopi di investimento* sulla base di un accordo o di un esercizio effettivo e che è trasmesso elettronicamente, potendo essere liberamente memorizzato e negoziato. Tali *crypto-asset*, ai sensi sempre della sez. 1, § 1, 11, n. 10 *KWG*, si qualificano genericamente come *strumenti finanziari*.

[30] I cc.dd. «utility token» forniscono al titolare, secondo la recente normativa tedesca, diritti di accesso o di utilizzo di determinati servizi o prodotti e possono essere paragonati a biglietti o *voucher*. Non sono pertanto considerati strumenti finanziari. Ne deriva l'esigenza di distinguere con esattezza (ma spesso con difficoltà) nella prassi, di volta in volta, i cc.dd. «utility token» dagli altri *crypto-asset* (poiché vi si applica inevitabilmente una diversa disciplina).

[31] L'inclusione tedesca dei *crypto-asset*, anche di pagamento, nella definizione di strumenti finanziari ha comportato l'istituzione di un nuovo servizio finanziario per la loro custodia. Quest'attività è stata descritta e regolata dettagliatamente dalla *BaFin*: *https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_krypto-verwahrgeschaeft_en.html*.

(di pagamento e d'investimento) si applica così, in quanto "strumenti finanziari" ai sensi del *KWG*, la disciplina eurounitaria *MiFID II* e – anche all'esito dell'approvazione della legge sui titoli elettronici (*eWPG*) (entrata in vigore il 10 giugno 2021) – la disciplina in materia di valori mobiliari, ossia il Regolamento sul prospetto, la Legge tedesca sul prospetto dei valori mobiliari (*WpPG*) e la Legge tedesca sul commercio dei valori mobiliari (*WpHG*) o, se concepiti come quote di fondi di investimento, il Codice tedesco degli investimenti di capitale (*KAGB*). L'Autorità federale di vigilanza finanziaria (*BaFin*) ha poi fatto seguire all'intervento legislativo la pubblicazione di documenti e linee guida che mirano a chiarire e precisare ulteriormente la disciplina[32].

L'*Autorité des marchés financiers* (*AMF*) ha pubblicato, a sua volta, un *discussion paper*, con specifico riferimento alle *ICO*, e successivamente un documento di sintesi delle risposte pervenute ad esito della consultazione del mercato. L'Autorità francese ha individuato un approccio regolamentare basato su uno schema di autorizzazione opzionale: i promotori dell'*ICO* possono decidere di richiedere l'autorizzazione all'*AMF*, che rilascerà (o meno) un visto attestante l'eventuale rispetto della disciplina (normativa e regolamentare), oppure, al contrario, di non richiedere autorizzazione all'AMF. Offerte formalmente non autorizzate non sarebbero pertanto vietate, ma dovrebbero, se presentate in Francia, contenere un avvertimento che indichi chiaramente l'assenza di visto della *AMF*[33]. Quest'approccio regolatorio s'inserisce peraltro in un panorama normativo ormai completo: alla disciplina legislativa del *Code monétaire et financier* – recentemente rivista ad opera della c.d. «Loi PACTE», n. 2019-486 del 22 maggio 2019[34] – si affianca, infatti, quella regolamentare di primo livello (modifiche al *Réglement*

[32] Si tratta di documenti pubblici facilmente reperibili anche *online* sul sito ufficiale dell'Autorità di vigilanza (v. *https://www.bafin.de/*): *BaFin – Advisory Letter (WA) - GZ: WA 11-QB 4100-2017/0010*; *BaFin – Guidance Notice: Second Advisory Letter - GZ: WA 51-Wp 7100-2019/0011 and IF 1-AZB 1505-2019/0003*; *BaFin – Guidance notice: Guidelines concerning the statutory definition of crypto custody business*.

[33] Quest'ultima opzione – seppur ammessa – risulta però, secondo i primi commentatori, poco realistica: v. P. Carrière, *Initial Coin Offerings (ICOs): Italia-Francia due approcci regolatori a confronto*, 15 gennaio 2020, in *dirittobancario.it*.

[34] Il fenomeno, collocato nell'ambito dell'ordinamento finanziario, è pertanto attualmente regolato *ad hoc* nel nuovo Capitolo II ("Emetteurs de jetons") del Titolo V ("Intermédiaires en biens divers et émetteurs de jetons") del Libro V ("Les prestataires de services") del "Code monétaire et financier".

général de l'Autorité des marchés financiers)[35] e quella di secondo livello (adozione della *Instruction DOC-2019-06: Procédure d'instruction et établissement d'un document d'information devant être déposé auprès de l'AMF en vue de l'obtention d'un visa sur une offre au public de jetons*)[36].

Già così – sorvolando su altre, pur interessanti, discipline ed esperienze nazionali (si pensi, per esempio, a quella di Malta[37] o di San Marino[38]) – sembra possibile constatare non soltanto una maggior attenzione nei confronti delle *ICO* e, più genericamente, dello scambio di criptoattività, ma anche una pluralità di possibili metodi e soluzioni regolamentari. All'approccio del c.d. «wait and see» (sostenuto finora da Paesi come l'Italia e l'Inghilterra) – che, monitorando lo sviluppo delle nuove tecnologie, preferisce non intervenire a livello legislativo, ma, tutt'al più, soltanto regolamentare tramite l'adozione di provvedimenti (perlopiù interpretativi) delle Autorità nazionali di vigilanza (applicando, nelle more, le disposizioni legislative preesistenti) – si affiancano, infatti, posizioni meno attendiste (fatte proprie, per esempio,

---

[35] Per una versione aggiornata del "Réglement général de l'Autorité des marchés financiers" è possibile consultare direttamente il sito ufficiale dell'*AMF*: *https://www.amf-france.org/sites/default/files/pdf/68793/fr/RG-en-vigueur-au-20210731_notes.pdf?1628676408*.

[36] Il testo ufficiale della "Instruction DOC-2019-06: Procédure d'instruction et établissement d'un document d'information devant être déposé auprès de l'AMF en vue de l'obtention d'un visa sur une offre au public de jetons" è reperibile *online* (sempre sul sito dell'*AMF*): *https://www.amf-france.org/sites/default/files/doctrine/fr/Instruction/DOC-2019-06/1.1/Procedure%20d%27instruction%20et%20etablissement%20d%27un%20document%20d%27information%20devant%20etre%20depose%20aupres%20de%20l%27AMF%20en%20vue%20de%20l%27obtention%20d%27un%20visa%20sur%20une%20offre%20au%20public%20de%20jetons.pdf.*

[37] Un'interessante normativa nazionale è contenuta, infatti, nel "Virtual Financial Assets Act" della Repubblica di Malta (per reperire e consultare il testo ufficiale, come successivamente modificato ed integrato, cfr. *https://legislation.mt/eli/cap/590/eng/pdf*). Cfr. E. M. INCUTTI, «Initial Coin Offering» *ed il mercato delle cripto-attività: riflessioni sugli* «utility token», cit., pp. 192-193; ID., «Initial Coin Offering» *ed il mercato delle cripto-attività: l'ambiguità degli* «utility token», cit., p. 84 ss.

[38] Anche la Repubblica di San Marino ha prestato una particolar attenzione alla disciplina delle criptoattività, delineando una normativa *ad hoc* delle *ICO* (qui denominate "ITO", Offerta Iniziale dei Token, v. artt. 7 ss.) mediante il Decreto Delegato 27 febbraio 2019, n. 37, poi abrogato e sostituito dal Decreto Delegato 23 maggio 2019, n. 86 ("Norme sulla tecnologia Blockchain per le imprese"). Il testo dell'abrogato Decreto Delegato 27 febbraio 2019, n. 37 (*https://www.consigliograndeegenerale.sm/on-line/home/scheda17162023.html*) e dell'attualmente vigente Decreto Delegato 23 maggio 2019, n. 86 (*https://www.consigliograndeegenerale.sm/on-line/home/archivio-leggi-decreti-e-regolamenti/scheda17163165.html*) sono entrambi reperibili e consultabili *online* sul sito ufficiale del Consiglio Grande e Generale della Repubblica di San Marino.

dalla Germania e dalla Francia) – che preferiscono predisporre specifiche soluzioni nazionali tanto di carattere legislativo quanto di carattere regolamentare. Questo panorama normativo – caratterizzato da una significativa frammentarietà di metodo e di merito – finisce per imporre all'interprete di volgere lo sguardo nella direzione delle possibili prospettive di disciplina sovranazionale delle *ICO* e, più genericamente, dello scambio di criptoattività.

14.4. Una prospettiva eurounitaria

Nell'intento di sviluppare la possibile prospettiva di una disciplina sovranazionale – ormai considerata l'unica capace di fronteggiare fenomeni, per loro natura, transnazionali – si propone una chiave di lettura diretta ad affiancare all'analisi della normativa di diritto finanziario (§ 4.1) anche un ripensamento circa problematiche (e soluzioni) di carattere più strettamente privatistico (§ 4.2).

Nell'evoluzione del panorama eurounitario, in particolare, è la competente Autorità di vigilanza – cioè l'ESMA (*European Securities and Markets Authority*) – a svolgere, ancor una volta, un ruolo centrale nell'ottica di suscitare, dapprima, e alimentare, poi, curiosità ed interesse nei confronti delle criptoattività attraverso la pubblicazione di *advice* rivolti alla Commissione europea.

L'ESMA – dopo aver evidenziato l'incerta evoluzione del dato normativo nel panorama continentale – ha, infatti, sollevato, a più riprese (nel 2017 e nel 2019)[39], problematiche nell'applicazione della disciplina sui servizi di investimento per i *token* qualificabili come strumenti finanziari, affrontando, seppur in forma sintetica, anche il tema dei *token* che non si qualificano come strumenti finanziari e raccomandando una regolamentazione *ad hoc* senza, tuttavia, proporre univoche scelte normative.

L'autorità di vigilanza europea non ha poi mancato, anche di recente, di avvertire chiaramente i consumatori sui rischi derivanti dalle criptoattività[40].

---

[39] Cfr. ESMA Advice su *Initial Coin Offrings and Crypto-Assets*, 9 gennaio 2019 (reperibile *online*: *https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf*), che fa seguito all'intervento precedente *The Distributed Ledger Technology Applied to Securities Markets*, febbraio 2017 (anch'esso reperibile *online*: *https://www.esma.europa.eu/system/files_force/library/dlt_report_-_esma50-1121423017-285.pdf*).

[40] Sul punto, cfr. *https://www.esma.europa.eu/press-news/esma-news/eu-financial-regulators-warn-consumers-risks-crypto-assets.*

14.4.1. Un panorama in evoluzione: la «Proposta MiCAR»

Il 24 settembre 2020, sull'onda anche dei *report* prodotti dall'ESMA, la Commissione UE pubblica un interessante pacchetto di proposte per la finanza digitale diretto ad agevolare la creazione e lo sviluppo di un mercato unico funzionale, da un lato, ad offrire prodotti finanziari migliori ai consumatori e, dall'altro, ad aprire nuovi canali di finanziamento alle imprese[41].

Fra le proposte della Commissione meritano una particolar attenzione quella avente ad oggetto alcuni adattamenti alle disposizioni vigenti, che hanno recentemente portato all'introduzione di un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito (*Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology – COM/2020/594 final*; oggi c.d. «Regolamento DLT»)[42], e soprattutto quella avente ad oggetto l'emanazione di un regolamento europeo sui Mercati di Cripto-attività (*Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 – COM(2020) 593 final-2020/0265(COD)*; c.d. «Proposta MiCAR»), che mira a dotare l'Unione Europea di norme uniformi in materia di emittenti di cripto-attività, nonché di prestatori di servizi in cripto-attività, superando così l'attuale frammentazione dei singoli regimi nazionali[43].

La c.d. «Proposta MiCAR» (approvata dal Consiglio dell'Unione Europea nell'ottobre 2022) – dopo avere scelto di regolare soltanto le

---

[41] Per una ricostruzione dei profili fondamentali della disciplina di matrice eurounitaria, cfr. M. SCOPSI, *La proposta della Commissione europea del 24 settembre 2020 avente ad oggetto l'emanazione di un Regolamento Europeo sui Mercati di Cripto-attività*, in *Pers. merc.*, 2020, pp. 504-505.

[42] Nell'art. 2 del Regolamento 2022/858/UE sono peraltro contenute delle definizioni di «tecnologia a registro distribuito (DLT)» («una tecnologia che consente il funzionamento e l'uso dei registri distribuiti») e di «registro distribuito» («archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso»), poi riprese anche nella Proposta di Regolamento MiCAR. Tale «Regolamento DLT» è destinato ad entrar in vigore (tranne che per alcune disposizione specificamente richiamate all'art. 19, paragrafo 2) a partire dal 23 marzo 2023.

[43] L'originario documento ufficiale è *online*: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593*. Nel testo si riporta chiaramente la versione aggiornata delle disposizioni richiamate.

criptoattività non rientranti già nella definizione di *non fungible token* (NFT), strumenti finanziari, moneta elettronica, depositi, depositi strutturati o cartolarizzazioni – definisce «criptoattività» ogni «rappresentazione digitale di un valore o un diritto che utilizza la crittografia a scopo di sicurezza e si presenta sotto forma di moneta o token o qualsiasi altro supporto digitale e che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga» (art. 3, paragrafo 1, n. 2), prevedendo, per un verso, l'eventuale rilascio di un passaporto europeo per consentire agli operatori del settore di offrire prodotti e servizi su cripto-attività nell'intero territorio dell'Unione e, per un altro, delle regole molto diverse a seconda che ciascuna criptoattività sia configurabile come (i) «token collegato ad attività», (ii) «token di moneta elettronica» e (iii) «utility token».

Nella disciplina, più specifica, dell'emissione di criptoattività (contenuta specificamente nei Titoli II, III, IV e V della «Proposta MiCAR»)[44], si recepiscono pratiche di mercato consolidatesi nel tempo (a partire, per esempio, dalla pubblicazione dei *white paper*), riadattando, al contempo, previsioni già radicate nella disciplina eurounitaria del mercato dei capitali al mercato delle cripto-attività.

Tale proposta – non ancora entrata in vigore – rischia, però, di sollevare significative perplessità non soltanto sulla tassonomia tripartita dei *token*, ma soprattutto sull'incerta delimitazione dei confini definitori che rischia di comportare rilevanti conseguenze sulla disciplina poi concretamente applicabile alle varie tipologie di *token* (potenzialmente rientranti in uno od in un altro regolamento oppure riconducibili ad una o ad un'altra disposizione nell'ambito del medesimo testo normativo)[45]. Non a caso le più recenti modifiche della proposta – oltre a rivedere parzialmente l'originale definizione dei «token collegati ad

[44] La «Proposta MiCAR» è composta, però, da ulteriori quattro titoli. Si tratta, in particolare, del Titolo VI («Prevenzione degli abusi di mercato relativi alle cripto-attività»), VII («Autorità competenti, ABE ed ESMA»), VIII («Atti delegati e atti di esecuzione»); IX («Disposizioni transitorie e finali»).

[45] Per alcune perplessità (elaborate, per la verità, a partire dall'originaria formulazione della «Proposta MiCAR», ma sostanzialmente condivisibili anche oggi nonostante talune modifiche testuali sopravvenute), specie sui cc.dd. «utility token», v. E. M. Incutti, «Initial Coin Offering» *ed il mercato delle cripto-attività: riflessioni sugli* «utility token», cit., p. 194 ss.; Id., «Initial Coin Offering» *ed il mercato delle cripto-attività: l'ambiguità degli* «utility token», cit., spec. p. 87 ss.

attività», dei «token di moneta elettronica» e degli «utility token»[46] – riconoscono significativi poteri all'ESMA per elaborare progetti di norme tecniche di regolamentazione, da presentare alla Commissione entro 18 mesi dall'entrata in vigore del futuro regolamento, funzionali ad individuare criteri e condizioni tali da stabilire quando una cripto-attività debba essere ritenuta sostanzialmente equivalente a uno strumento finanziario a prescindere dalla sua forma (art. 2, paragrafo 3)[47].

14.4.2. Il ruolo del diritto privato

L'odierna riflessione sull'evoluzione della disciplina eurounitaria non sembra, però, potere tralasciare questioni (e, di conseguenza, soluzioni) di carattere più strettamente privatistico.

Emergono così due ordini di riflessioni.

Il primo coinvolge problemi – di carattere (forse) più generale – riguardanti l'applicabilità o meno al contratto di compravendita dei *token* della disciplina dei contratti conclusi «a distanza» (direttiva 2011/83/UE) e, più in generale, del commercio elettronico (d.lgs. 9 aprile 2003, n. 70) e del Codice del consumo (d.lgs. 6 settembre 2005, n. 206, artt. 49-59 cod. cons.) nonché dei contratti di fornitura di contenuto e di servizi digitali (direttiva 2019/770/UE). Significative problematiche di coordinamento della disciplina applicabile sembrano poi emergere, fra l'altro, con riferimento all'interferenza con la normativa "speciale" di contrattazione a distanza dei servizi finanziari (direttiva 2002/65/CE, che, con ogni probabilità, sarà a breve abrogata all'esito dell'entrata in vigore della proposta di una nuova direttiva sui contratti finanziari a distanza con i consumatori, pubblicata nel maggio del 2022 e destinata a modificare significativamente anche la suddetta

[46] Queste le tre definizioni tratteggiate dalla «Proposta MiCAR»: «*"asset-referenced token" means a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing to any other value or right or a combination thereof, including one or more official currencies; "electronic money token" or "e-money token" means a type of crypto-asset that purports to maintain a stable value by referencing to the value of one official currency; "utility token" means a type of crypto-asset which is only intended to provide access to a good or a service supplied by the issuer of that token*» (art. 3, paragrafo 1, nn. 3, 4 e 5).

[47] Peraltro, un ruolo centrale, al di là delle suddette funzioni di normazione secondaria e di vigilanza, è stato riconosciuto all'ESMA anche sul fronte dell'attività periodica di rendicontazione sull'andamento del mercato e sull'applicazione della disciplina eurounitaria (v. Titolo IX «Disposizioni transitorie e finali»).

direttiva 2011/83/UE)[48]. A tale panorama, già così decisamente articolato e frammentato, si aggiungono poi le incertezze (di coordinamento e, di conseguenza, di disciplina applicabile) derivanti dalla disciplina (in vigore e *in itinere*), sempre di matrice eurounitaria, sulle clausole abusive e sulle pratiche commerciali scorrette.

Non stupisce pertanto che già la Risoluzione del Parlamento europeo del 20 ottobre 2020 abbia chiesto alla Commissione «di aggiornare il suo documento orientativo esistente sulla direttiva 2011/83/UE del Parlamento europeo e del Consiglio, del 25 ottobre 2011, sui diritti dei consumatori al fine di chiarire se ritiene che i contratti intelligenti siano contemplati dall'eccezione di cui all'articolo 3, paragrafo 3, lettera l) di tale direttiva ["la presente direttiva non si applica ai contratti (…) conclusi mediante distributori automatici o locali commerciali automatizzati"], e, in caso affermativo, in quali circostanze»[49]. Si tratta di un tentativo per iniziare a riflettere più concretamente sui margini per un'applicabilità o meno (nonché per un eventuale riadattamento) della disciplina consumeristica nell'ambito degli *smart contract*, sollevando così, proprio alla luce della derivazione eurounitaria delle disposizioni, perplessità e problemi di livello non soltanto nazionale, ma anche continentale[50].

Il secondo ordine di riflessioni non può che riguardare alcune emblematiche questioni di carattere più specifico.

Mentre, secondo il Rapporto finale della CONSOB, l'identificabilità dei titolari dei diritti – causa spesso di truffe a danno degli investitori

---

[48] Il testo della proposta di direttiva è reperibile *online*, cfr. *https://eur-lex.europa.eu/resource.html?uri=cellar:e7cebe9a-d208-11ec-a95f-01aa75ed71a1.0021.02/DOC_1&format=PDF*. Altre possibili problematiche di coordinamento della disciplina applicabile possono emergere poi con riferimento alla normativa della contrattazione a distanza dei servizi finanziari di cui all'art. 67-*bis* ss. del codice del consumo (con annessa normativa secondaria della CONSOB sulla raccolta di capitali di rischio tramite portali *online*).

[49] Si tratta della *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione sulla legge sui servizi digitali: adeguare le norme di diritto commerciale e civile per i soggetti commerciali che operano* online, pubblicata (anche nella sua versione in lingua italiana) sul sito ufficiale del Parlamento europeo: *https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_IT.html*, spec. § 36. Per un'analisi delle possibili conseguenze della richiamata Risoluzione, cfr., per tutti, M. MAUGERI, voce Smart contracts, cit., p. 1138 ss.

[50] Sulle problematiche sollevate con riferimento specifico al diritto dei consumatori, cfr. M. MAUGERI, *ICO and consumer protection*, in Liber amicorum *per Paolo Police*, I, Scritti raccolti da C. FABRICATORE, A. GEMMA, G. GUIZZI, N. RASCIO, A. SCOTTI, Torino, 2020, p. 515 ss.

– andrebbe, per esempio, accertata e garantita, nei limiti consentiti dall'odierna tecnologia, «rispettivamente dal gestore della piattaforma per il lancio delle offerte di prima emissione e dall'organizzatore di scambi di cripto-attività»[51], nessuna indicazione (legislativa o regolamentare) è stata fornita ad oggi con riferimento ai (pur estremamente rilevanti) problemi ascrivibili alla lingua «informatica» degli *smart contract*[52] (fino a dubitare, come si è detto, della stessa configurabilità, nel caso di accordi non comprensibili ad entrambe le parti per via di un'incolmabile «asimmetria informatica», della natura contrattuale dei suddetti strumenti)[53]. In ogni caso, anche superando tali (non secondari) dubbi ricostruttivi, nei contratti *P2P* (*Peer-to-Peer*) l'eventuale previsione di una traduzione in linguaggio «naturale» può comportare, laddove presente, incertezze riconducibili alla mancata coincidenza fra le due versioni e, laddove mancante, non indifferenti difficoltà di comprensione (seppure difficili, poi, da far oggetto di prova), è soprattutto nei contratti *B2C* (*Business-to-Consumer*) che l'auspicabile previsione di una traduzione in linguaggio «naturale» rischia di provocare le maggiori difficoltà, continuando a comportare, se presente, rischi di difformità e, se mancante, dubbi applicativi di non poco momento. Si pensi, per esempio, alle perplessità suscitate, in assenza di traduzioni in linguaggio «naturale», dalla possibile declinazione – nell'ambito degli *smart contract B2C* – dell'art. 34, comma 2, cod. cons. (che prescrive chiarezza e comprensibilità nella formulazione delle clausole) oppure dell'art. 72 cod. cons. (che fissa specifici requisiti linguistici per il contratto di multiproprietà) oppure ancora dell'art. 51, comma 1, cod. cons. (che impone al professionista, nei contratti a distanza, di fornire o metter a disposizione del consumatore le informazioni in un linguaggio semplice e comprensibile)[54].

Né sembra particolarmente rassicurante l'attuale panorama (in senso lato) rimediale con alcune soluzioni che sembrano completamente da ripensare (prima ancora, se del caso, che da riscrivere). Non

---

[51] Cfr. CONSOB, *Le offerte iniziali e gli scambi di cripto-attività*, Rapporto finale, 2 gennaio 2020, cit., p. 5. Un'attenzione al problema dell'identificazione delle parti interessate negli *smart contract* è dimostrata anche dalla (già richiamata) formulazione legislativa dell'art. 8-*ter*, comma 2, del c.d. «Decreto Semplificazioni».

[52] Cfr. J.G. ALLEN, *Wrapped and Stacked: «Smart Contracts» and the Interaction of Natural and Formal Language*, in 14 *European Review of Contract Law*, 2018, p. 307 ss.

[53] Cfr., *supra*, § 2 (spec. nt. 11).

[54] Cfr., per tutti, M. MAUGERI, Smart contracts *e disciplina dei contratti*, cit., p. 402; EAD., *ICO and consumer protection*, cit., p. 515 ss.

è possibile tralasciare del tutto, infatti, le problematiche ricondubili, a titolo meramente esemplificativo, alla stipulazione di *smart contract* illeciti e alle modalità di esercizio del diritto di recesso nei rapporti *B2C*.

Nell'ipotesi di *smart contract* illecito, nell'ambito, a sua volta, di un'*ICO*, seguirà comunque – nonostante l'astratta nullità del rapporto – l'esecuzione delle prestazioni. Ne deriva che il rimedio non potrà che essere fondamentalmente restitutorio (fermo restando gli eventuali profili risarcitori). Ciò, a sua volta, non è chiaramente privo di conseguenze. Si pensi, per esempio, al diverso regime della prescrizione fra l'azione di nullità e quella di restituzione: dall'imprescrittibilità dell'azione di accertamento della nullità (art. 1422 cod. civ.) si distingue nettamente, infatti, l'ordinario termine di prescrizione decennale dell'azione di ripetizione delle prestazioni effettuate in esecuzione di un contratto nullo (art. 2946 cod. civ.).

Nei rapporti *B2C* solleva non poche perplessità, invece, la disciplina sull'esercizio del diritto di recesso. Quest'ultimo, come noto, rappresenta lo strumento rimediale forse più diffuso nell'ambito dei rapporti contrattuali conclusi a distanza (o negoziati fuori dei locali commerciali): l'art. 52 cod. cons., infatti, dispone la possibilità per il consumatore di recedere dal contratto entro un periodo di quattordici giorni senza dovere fornire nemmeno motivazioni. Le *ICO* e, più genericamente, l'esecuzione di *smart contract* nell'ambito finanziario – malgrado l'art. 59, comma 1, lett. o), cod. cons. configuri forse un'eccezione astrattamente (seppure con evidenti difficoltà) applicabile nel caso di specie (richiamando «la fornitura di contenuto digitale mediante un supporto non materiale se l'esecuzione è iniziata con l'accordo espresso del consumatore e con la sua accettazione del fatto che in tal caso avrebbe perso il diritto di recesso») – sembrano porre problemi rilevanti circa la compatibilità non soltanto fra il funzionamento degli *smart contract* e dello strumento rimediale, ma addirittura fra le ragioni stesse che spingono i consumatori ad avvalersi delle nuove tecnologie (a partire dall'esigenza di aver un'esecuzione certa, immediata e automatizzata del rapporto) e del recesso[55].

[55] Anche la suddetta Risoluzione del Parlamento europeo del 20 ottobre 2020 invita pertanto la Commissione UE a rivedere la complessa questione del diritto di recesso, prevedendo misure atte ad assicurare che i contratti intelligenti siano dotati di meccanismi in grado di arrestarne e invertirne l'esecuzione (cfr. *Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione sulla legge sui servizi digitali: adeguare le norme di diritto commerciale e civile per i soggetti commerciali che operano* online, cit., spec. §§ 35-36). Altrimenti, seppur a costo di prevedere un rimedio al

14.5. Considerazioni conclusive

L'analisi delle caratteristiche delle *ICO* e degli *smart contract* nel settore finanziario mostra pertanto un'alternativa fra un approccio sostanzialmente «attendista» – volto a monitorare l'evoluzione della prassi, facendo rientrare (o meno), di volta in volta, tali fenomeni nell'articolata legislazione previgente[56] – e uno, per così dire, «interventista» – diretto a sollecitare la predisposizione (più o meno rapida) di una regolamentazione *ad hoc* (nazionale o, preferibilmente, sovranazionale)[57].

---

contempo «depotenziato e gravoso» (M. MAUGERI, Smart contracts *e disciplina dei contratti*, cit., p. 404), sembra forse possibile per il consumatore far valere il recesso al di fuori della *DLT*. Si rischia, però, così di non riuscire, per un verso, a evitare, in ogni caso, l'obbligo di adempiere da parte del consumatore e, per un altro, a superare delle (significative) difficoltà riconducibili all'acquisizione nello *smart contract* dell'accordo espresso del consumatore relativo alla perdita del diritto di recesso (v. art. 59, comma 1, lett. o), cod. cons.). D'altronde, l'odierno frastagliato panorama normativo – già, seppure rapidamente, tratteggiato – non sembra in grado attualmente di fornire un'inequivoca risposta all'esigenza di coordinamento fra le numerose discipline in vigore o in corso di approvazione. Si pensi, per esempio, alle ulteriori previsioni – anche, per l'appunto, a proposito del diritto di recesso – oggi contenute nella disciplina di contrattazione a distanza in generale (direttiva 2011/83/UE), nella disciplina eurounitaria di contrattazione a distanza dei servizi finanziari (direttiva 2002/65/CE, che lascerà presto il posto alla già richiamata proposta di nuova direttiva sui contratti finanziari a distanza con i consumatori, pubblicata nel maggio del 2022, destinata a modificare significativamente anche la suddetta direttiva 2011/83/UE) e nella disciplina di cui all'art. 67-*bis* ss. (spec. art. 67-*duodecies*) del codice del consumo (e alla relativa normativa secondaria della CONSOB sulla raccolta di capitali di rischio tramite portali *online*). A ciò si aggiungono poi le incertezze applicative derivanti dalla normativa (in vigore e *in itinere*), di matrice eurounitaria, sulle clausole abusive e sulle pratiche commerciali scorrette. Sembra così emergere, specie con riferimento ad aspetti peculiari come la disciplina del diritto di recesso, la necessità d'ipotizzare forse una chiara normativa (anche privatistica) *ad hoc* per queste nuove tecnologie, anziché cercare sempre di riadattare, se del caso anche con evidenti forzature, la normativa (consumeristica) preesistente.

[56] Cfr., per tutti, R. PARDOLESI, A. DAVOLA, «Smart contract»*: lusinghe ed equivoci dell'innovazione purchessia*, in *Foro it.*, 2019, V, p. 195 ss.

[57] Cfr. S. GRUNDMANN, P. HACKER, *Digital Technology as a Challenge to European Contract Law*, in *European Review of Contract Law*, 2017, p. 255 ss.; e, nella letteratura italiana, A.M. BENEDETTI, *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari*, cit., pp. 425-426. Quest'ultimo, riflettendo sui possibili scenari corrispondenti ai problemi derivanti dall'intensificarsi dei rapporti fra contratti e algoritmi, auspica, infatti, non soltanto l'ennesima (pur necessaria) direttiva europea, ma soprattutto «una nuova "Convenzione di Vienna", cui affidare la costruzione di un vero e proprio codice mondiale del contratto algoritmico».

Fermo restando l'esigenza di adottare sempre una prospettiva concreta, che valuti la singola operazione nel suo complesso al fine di assicurarne il più corretto inquadramento giuridico, sembra preferibile – anche alla luce dell'esponenziale crescita della finanza digitale[58] – potenziare gli sforzi per una piena comprensione dei fenomeni (tecnologici ed economici) da regolare, valutando, nel frattempo, le possibili conseguenze di un eventuale intervento normativo anche nazionale. Quest'ultimo non sembra più rinviabile *sine die* per via dell'esigenza, sempre più pressante, di assicurare, per un verso, un'effettiva tutela dei soggetti coinvolti in operazioni e scenari profondamente diversi rispetto al passato e, per un altro, una maggiore certezza ad un nuovo *business* in espansione. Anche il rischio di una sempre maggiore concorrenza regolatoria tra gli ordinamenti sembra suggerire l'esigenza d'iniziare ad ipotizzare un organico intervento normativo nell'intento perlomeno di gestire (se non di guidare) lo sviluppo del fenomeno nell'interesse dei singoli soggetti coinvolti e dell'intero sistema finanziario ed economico.

Simili rilievi suggeriscono però di riannodare il filo del discorso – a partire dalle sue premesse "tecnologiche" e "metodologiche" – per svolgere delle rapide notazioni.

La prima riguarda l'esigenza di valorizzare le peculiarità – specie tecnologiche ed economiche – dello scambio di criptoattività. Ne derivano riflessi significativi tanto sull'*iter* quanto sul modello normativo. È così da salutarsi con favore non soltanto il ruolo centrale assunto dalle diverse autorità indipendenti di vigilanza (nazionali ed europee), ma anche il coinvolgimento, già in una fase preliminare, di operatori ed esperti del settore (chiamati, da parte delle diverse autorità, a presentare spesso osservazioni e considerazioni). Meno soddisfacente è, invece, l'attuale stato di elaborazione dei modelli normativi e regolamentari, che riservano solitamente, ancor oggi, un'attenzione prevalente (ove non esclusiva) ai profili di diritto finanziario, mentre sono le stesse caratteristiche peculiari delle *ICO* e dell'applicazione degli *smart contract* nell'ambito finanziario ad imporre, come si è visto, un

Nella direzione di un intervento *ad hoc* sembra ormai suggerire di muoversi la stessa CONSOB (al riguardo può richiamarsi, fra l'altro, la recente intervista rilasciata, lo scorso 2 giugno 2022, dal Commissario Paolo Ciocca al Messaggero: *https://www.ilmessaggero.it/economia/moltoeconomia/bitcoin_commissario_consob_paolo_ciocca_crypoto_asset_italia-6724666.html*).

[58] Cfr. V. CARLINI, Boom *per le criptovalute: 3.200 nuovi* asset *nel 2021. Ma c'è il rischio normativo*, in *IlSole24Ore*, 20.08.2021, pp. 1, 18.

ripensamento significativo anche della disciplina privatistica che, spesso mutuata dalla (poco coordinata) normativa consumeristica, non sempre risulta espressione di una visione coerente del fenomeno nel suo complesso.

La seconda notazione non può che riferirsi pertanto al ruolo del diritto civile (e, in particolare, dei consumatori) nella prospettiva dello scambio di criptoattività. Non c'è dubbio che fenomeni del genere, avvalendosi delle nuove tecnologie, comportino una sostanziale disintermediazione del sistema finanziario, suggerendo un ulteriore approfondimento delle riflessioni sul compito (ed inevitabilmente sui confini) del c.d. «diritto privato regolatorio»[59]. Quest'ultimo sembra chiamato, infatti, a dar un contributo rilevante – auspicabilmente coordinato con l'apporto di una (altrettanto) rinnovata disciplina finanziaria e pubblicistica (di matrice nazionale ed eurounitaria) – nella regolamentazione dell'intero fenomeno senza trascurare poi le rilevanti problematiche sollevate (e le prime risposte prospettate), sotto il profilo più strettamente processuale, circa l'azionabilità delle pretese e l'effettiva giustiziabilità delle eventuali lesioni dei diritti dei soggetti coinvolti[60].

La terza ed ultima notazione non può che abbracciare metaforicamente l'intero pianeta, sollevando, ancor una volta, la problematica della frammentarietà della disciplina di fenomeni destinati, per definizione, ad essere globali[61]. La prospettiva eurounitaria – contenuta prevalentemente (ma, come si è visto, non solo) nella c.d. «Proposta MiCAR»[62] - rappresenta sicuramente un passo in avanti: si può e si deve,

---

[59] Per interessanti spunti di riflessione sul c.d. "diritto privato regolatorio", si rinvia ai contributi raccolti in M. MAUGERI e A. ZOPPINI (a cura di), *Funzioni del diritto privato e tecniche di regolazione del mercato*, Bologna, 2010; e, più recentemente, cfr. A. ZOPPINI, *Il diritto privato e i suoi confini*, cit., p. 201 ss.

[60] Quest'ultimo profilo comincia, per esempio, ad essere considerato – con un approccio giustamente sovranazionale (riconoscendo un ruolo, ancor una volta centrale, alle autorità di vigilanza nazionali ed europee, come l'ABE e l'ESMA) – nell'ambito del Titolo VII («Autorità competenti, ABE ed ESMA») della Proposta di Regolamento MiCAR.

[61] Nella prospettiva di una regolamentazione pienamente sovranazionale (se non addirittura, come suggerito nel testo, mondiale) si pensi, per esempio, al ruolo che potrebbe essere svolto, già oggi, dalle raccomandazioni rivolte dall'OCSE (organizzazione internazionale che, come noto, raggruppa 38 Paesi, seppur in assenza di Cina e Russia, con il fine di favorire la cooperazione e lo sviluppo economico) a governi e operatori del mercato sull'uso responsabile e consapevole della *blockchain*. L'ampia e documentata attività dell'OCSE sull'argomento è oggi facilmente consultabile e reperibile *online*: *https://www.oecd.org/daf/blockchain/*.

[62] Cfr., *supra*, §§ 4, 4.1.

però, fare di più. All'indomani dell'entrata in vigore del regolamento si presenteranno, infatti, nuove sfide: dall'armonica applicazione della nuova disciplina alla necessità di prevedere regole specifiche anche sul fronte civilistico, passando, infine, per l'auspicata predisposizione di nuove ed efficaci normative con aspirazioni di carattere davvero mondiale. Nell'era della finanza digitale il trasferimento di ricchezze sembra non avere più confini…e la sua disciplina?

Autori

Attilio Altieri, Assegnista di ricerca presso l'Università di Foggia;

Alessandro Bernes, Ricercatore presso l'Università Cà Foscari di Venezia;

Lucio Casalini, Assegnista di ricerca presso l'Università di Camerino;

Filippo D'Angelo, Ricercatore presso l'Università di Sassari;

Ilaria Garaci, Professore associato presso l'Università Europea di Roma;

Daniele Imbruglia, Ricercatore presso l'Università di Roma La Sapienza;

Enzo Maria Incutti, Dottorando presso l'Università di Roma La Sapienza;

Silvia Martinelli, Assegnista di ricerca presso l'Università di Torino;

Anita Mollo, Assegnista di ricerca presso la Scuola Superiore Meridionale;

Roberta Montinaro, Professoressa ordinaria presso l'Università L'Orientale di Napoli;

Salvatore Orlando, Professore ordinario presso l'Università di Roma La Sapienza;

Francesco Pacileo, Ricercatore presso l'Università di Roma La Sapienza;

Federico Ruggeri, Assegnista di ricerca presso l'Università di Palermo;

Emanuele Tuccari, Ricercatore presso l'Università di Pavia.

Collana Materiali e documenti

Per informazioni sui volumi precedenti della collana, consultare il sito:
www.editricesapienza.it | *For information on the previous volumes included in the series, please visit the following website: www.editricesapienza.it*

82. Dialoghi sull'Architettura I
Dottorato di Ricerca in Storia, Disegno e Restauro dell'Architettura
a cura di Simone Lucchetti, Sofia Menconero, Alessandra Ponzetta

83. Archivi digitali di Sapienza
Itinerari culturali per la conoscenza
Atti del Seminario, Roma, 18-19 marzo 2021
a cura di Sara Colaceci, Alekos Diacodimitri, Giulia Pettoello, Francesca Porfiri, Federico Rebecchini

84. Il disagio giovanile oggi
Report del Consiglio Nazionale dei Giovani
a cura del Consiglio Nazionale dei Giovani

85. Corso interdisciplinare "Scienze della Sostenibilità"
Sintesi dei contributi (20/21)
a cura di Livio de Santoli, Fausto Manes, Gianluca Senatore

86. Palazzo Corsini e il suo giardino ad Albano Laziale
Rilievo, storia, indagini termografiche e restauro
Gilberto De Giusti e Marta Formosa

87. Casi di marketing Vol. XVI
Quaderni del Master Universitario in Marketing Management
a cura di Michela Patrizi

88. Giuseppe Sardi
Architetto e Capomastro nel territorio romano del XVIII secolo
Marta Formosa e Gilberto De Giusti

89. Oltre gli stereotipi sulla violenza di genere
Approcci, teorie e ricerche
a cura di Giovanna Gianturco e Giovanni Brancato

90. Annuario 2022
Osservatorio Giuridico sulla Innovazione Digitale
Yearbook 2022
Juridical Observatory on Digital Innovation
a cura di Salvatore Orlando e Giuseppina Capaldo

Il volume - che fa seguito all'omologo Annuario 2021 - contiene contributi di docenti e ricercatori di varie Università italiane su una pluralità di tematiche che sollecitano la riflessione circa la tenuta delle categorie giuridiche tradizionali a cospetto delle trasformazioni dei modelli di relazione recate dalle tecnologie digitali. Gli scritti sono maturati nel contesto delle attività di ricerca e seminariali promosse dall'Osservatorio Giuridico sulla Innovazione Digitale (OGID), costituito presso il Dipartimento di Diritto ed economia delle attività produttive dell'Università Sapienza di Roma.

I curatori dell'opera, **Salvatore Orlando** e **Giuseppina Capaldo**, sono professori ordinari di diritto privato presso il Dipartimento di Diritto ed economia delle attività produttive di Sapienza Università di Roma.

ISBN 978-88-9377-256-3

www.editricesapienza.it