BIG DATA AND DIGITAL NUDGING. INSIGHTS INTO FREEDOM OF CHOICE, SUSTAINABILITY, AND CYBERSECURITY

Luigi Prosia[1]

Abstract
The collection, processing and analysis in real time of personal data, daily activity of the large digital plays that dominate the private sector, can also play a fundamental role in the public sector to plan, monitor and make responsible decisions in view of a truly inclusive, democratic and participatory development. The use of sophisticated data mining techniques can allow Governments to obtain increasingly detailed and timely information on which to build better intervention strategies in every field (social, economic, environmental), to then verify their effectiveness. However, to safeguard the freedoms and rights of individuals, which may be harmed by unlawful or arbitrary processing of data concerning them, the great opportunities offered by big data analytics must be set within a framework of sustainability and technological security guided by the principle of accountability. This is even more accurate since behavioral economics have removed the paradigm of absolute rationality of *homo œconomicus*, highlighting the cognitive errors inherent in its very nature, bias of the mind that facilitate mechanisms of *libertarian paternalism* (or neuromarketing) able to silently alter the formation of wills, although they are often legitimized starting from the purported purpose of improving individual and collective well-being. If so, *quis custodiet ipsos custodes*?

Keywords
Big Data, Digital Nudging, User Experience Design, Sustainability, Cybersecurity.

Summary

[1] PhD Candidate in Philosophy of Law, Biolaw and Legal Informatics, Department of Law, Rome Tor Vergata University – Italy.

1. IMMERSED IN THE DIGITAL SPACE, WHERE *INFORMATION RULES*[2]

Digitization (with its signals, sensors and electronic pulses) results in the circulation of an incredible amount of data concerning us, which can describe us and quite simply know more about us than we imagine. It can do so to the point of being able to anticipate most of our daily decisions[3]. The data is not only accurate, intimate, correlated and verifiable, but also immense "that it fills all American libraries more than eight times […] [by] a self-perpetuating cycle"[4] according to fragmentary logic[5]. Suffice to say that to represent the amount of content currently available on the Web it is necessary to resort to the zettabyte: a number followed by twenty-one zeros. These figures are destined to grow quickly and without interruption due to the daily exchange of information that spreads in heterogeneous forms and contents and that makes people incredibly more exposed[6]. In fact, they

---

[2] I have named this paragraph after the title of the book by U.S. economists Carl Shapiro and Hal Varian, published by Harvard Business School Press, who had already revealed in 1998 the great power that information would soon assume.

[3] On the indisputable advantages of today's technical-scientific development linked to the possibility of processing a large amount of data without a particular expenditure of time and energy, on the one hand, and on the requests for protection of new rights that this relentless elaboration inevitably entails, on the other, see AMATO MANGIAMELI 2022a, 93-101.

[4] FLORIDI 2017, 13.

[5] "The fragmentation consists in the fact that around each social user swarms of personalized information are thickened, calibrated by automatic algorithms [...]. This is the name of the mass of personal information, related to both commercial and political tastes, obtained from every click, like or little heart, that each of us puts on social media" (BARBERIS 2020, 159).

[6] HARARI 2018, 472, talks about *dataism*, a kind of religion that benefits from the now extreme sharing of data. If for *humanism* experiences happen within us and right there we should find the meaning of everything that happens, for *dataists*, instead, experiences remain worthless if they are not shared. "Twenty years ago, Japanese tourists were the laughingstock of the global village, always walking around armed with cameras and

show themselves to be incapable of guarding their secrets[7] and entrust their social representation to multiple and widespread data sets that modify their knowledge and identity, to the point that we can speak of an *electronic body*[8] ideally opposed to the *physical body*. Moreover, integrated telecommunications systems intensify the transmission, storage and search for information, all of which have become potentially publishable, even more, at relatively minimal cost[9], so that a continuous flow shapes every level of planetary life, now increasingly conditioned "by the speed and carelessness of the hasty telematic word of mouth"[10]. Through ICT, individuals experience new existential and mental models that transform the intrinsic nature of reality to the exent that the barriers between *online* and *offline* corrode and make *being there* perfectly superimposable to *being connected*. As a result, technology ceases to be a mere tool (to calculate, write, store, inform, educate), and becomes "prosthesis that surpasses and perfects man and nature"[11], as we live, grow and interact, with greater or lesser success and in a more or less healthy way, depending on the (knowledge-)information made available by new devices: laptops, apps and

photographing whatever subject came their way. Now everyone is like that [...]. The new motto says: 'If you experience something – record it. If you record something – upload it. If you upload something – share it'".

[7] On the Net as a genetically unsuitable environment for keeping secrets, see ZICCARDI 2022, 81 ss.

[8] For a definition of the *electronic* (or *logical*) *body* generated by the many traces left on the Net by users, as well as the risks it raises, please refer to RODOTÀ 2015, 270.

[9] On this point, particularly interesting are the observations of GRANIERI 2006, 28-29: "At the time of mass media and large editorial distributions [...] it was necessary to select the contents before 'investing' in their transmission [...]. Today the digital society is showing us a process that is organized on a principle exactly opposite [...] [and this] from the point of view of the history of human communications is a difference in approach comparable to Ptolemaic discovery in astronomy […] or the acceptance that the earth is round and not flat".

[10] CAMPAGNOLI 2020, 78.

[11] DIONIGI 2019, 48.

platforms that "go beyond the dialectic of means to achieve the rhetoric of goals"[12].

At the same time, however, man is constantly challenged by recovery and from the processing of data starting from one's own habits on the Net (from websites visited to emails exchanged, from chats to online purchases) that can be recorded and computed with unprecedented precision thanks to the action of software so sophisticated as to greatly exceed the intellectual and working limits of a human being[13]. The aim is undoubtedly to collect and store more and more information and then produce further and more valuable[14], whereas, as Granger states in *Fahrenheit 451* regarding surveillance activities in the context of an unidentified despotic society where reading or possessing books is considered a criminal offence, "you never know when knowing certain data will be useful to you!"[15]. And this, today, is particularly useful to the superstar companies of Silicon Valley (Amazon, Apple, Google and other digital giants), whose economic-industrial model "aspires to transform every gesture, every breath, every relationship into an opportunity for profit"[16].

2. FROM MONOPOLIES TO OPEN DATA

[12] AMATO MANGIAMELI 2020a, 32.

[13] On how digital technologies, beyond the benefits brought to our lives, expose to an uncontrollable power, such as that of generalized surveillance, the considerations of TINCANI 2015, 19-40; 2016, 19-63; 2018, 51-78.

[14] With all the difficulties that derive from it in relation to the requirement of consent, which pursuant to the GDPR must be explicitly and freely referred to specific processing purposes illustrated in a clear and precise way. In this regard, reference should be made to the *European Parliament resolution on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement*, March 14, 2017 (2016/2225(INI)).

[15] BRADBURY 1978, 175.

[16] SADIN 2018, 13.

Faced with the profound *reontologization* and *rehistoriologization*[17] of the world caused by the advent of the Internet – the quickest, cheapest and most efficient (but also not the safest) existing means of communication – it is therefore no coincidence that Big Tech base their business systems on data, also making numerous efforts to ensure the exclusive domination of what is the key resource of the twenty-first century. The value of data, in fact, does not end with their use, indeed it increases the more they are used, according to different combinations always made possible by the unprecedented storage and analysis capabilities (or data mining techniques) of the algorithms[18]. From this point of view, the frequent metaphor of data as the new oil, another important raw material that however is consumed as it burns, appears reductive for the fact that digital information, unlike the source from which it originates, it is modular and multipliable in copies, and is not lost or destroyed by the use itself.

It is more correct, then, to speak of data as a non-rival asset, which not being consumed like oil can be used simultaneously by several people. It is possible to extract continuously from it, without reducing at all the surprising quality, new indications and perspectives. Whereas, at present, this translates into a competitive advantage for only established digital monopolists, resulting in power imbalances between those who hold the data and those who intentionally or inadvertently provides them. This disparity could be overcome by making its flow free and open to all (citizens, Governments, international organizations, traditional businesses)[19]. In doing so, data, especially that characterized by large volumes, speed, variety

[17] FLORIDI 2020, in part. 23 ss.

[18] The algorithms are "the real intellectual gems of digital superstars and their incredible engineers, an intellectual property worth preserving better than the Kremlin guards Lenin's body" (RAMGE, MAYER-SCHÖNBERGER 2021, 28). Nevertheless, on how the same algorithms conceal mechanisms of alteration of information and conditioning of action to the point of compromising the stability of the same democratic systems, reference is made to AMATO MANGIAMELI 2019, 107-124.

[19] MAYER-SCHÖNBERGER, RAMGE 2018.

and easy visualization (the so-called big data), could increase alongside the profit of a few, the well-being of many, configuring even for the latter a safe investment in economic and social terms place that

> the results [of data processing] that appear today to be of no one or of little interest could suddenly assume vital importance [...] due to unforeseeable future events – such as, for example, a pandemic, a natural cataclysm or an upheaval of the stock markets – or further developments in information technology[20].

The possibility of obtaining sensible and statistically consistent forecasts from the processing of data, on which to calibrate the various decision-making processes, can be a stimulus to innovation and growth, both in the private and in the public sector. In the first area, analytics systems would allow to optimize performance, increase productivity, lower costs and, in general, develop more significant forms of corporatism. In the second case, however, what is at stake goes beyond mere economic power, and concerns more closely precious values such as the security of citizens, the development of collective knowledge[21], the safeguarding of justice and equity, the prevention and combating of discrimination. This is because, by directing data towards the collective good, numerous public sectors (health, transport, environment, energy) could know real opportunities for change certainly for the better, as they are linked to a more efficient and personalized provision of services, the enactment of more accurate and timely measures (whose effectiveness must also be verified), as well as considerable tax savings.
There is a need, therefore, for much wider access to data to try to reduce the current information asymmetry between organizations and companies,

[20] SARACENI 2023, 42.
[21] On this point, I refer to the refined and far-sighted reflections of LÉVY 2002.

individuals and customers, State and society, thus promoting a correct transition to digital based on open data for all, as Europe has been supporting politically for some years. The words spoken by the European Commission President Ursula Von der Leyen in February 2020, at the opening of the works dedicated to digital strategy initiatives, move in this direction:

> We want data to be available to everyone, both public and private, large and small, whether they are startups or Web giants. [...] As a party to the dispute, large commercial digital players must accept their responsibility, including that of allowing Europeans access to the data they collect[22].

Only by conquering the goal of this universal data sharing and resetting, consequently, power relations, state institutions, non-profit associations and civil society at large will be able to deal with the environmental, economic and humanitarian emergencies taking place. Conversely, an unequal distribution of (knowledge-)information will always be an obstacle to the advancement of social, scientific and economic progress, understood with a view to truly inclusive, democratic and sustainable development.

3. FROM NEUROMARKETING TO PUBLIC UTILITY NUDGING

The digital revolution, in addition to intensifying information asymmetries in a way that the pioneers of the Web could not have foreseen, has also favored the emergence of new tools, based once again on information (and its representation), to promote in an indirect but still significant way certain behavior which is considered desirable in the opinion of the regulators on duty.

[22] 2020.

Reference is to all those techniques widely used in today's online decision-making environments, used by Big Tech to steer the conduct of individuals in certain directions, depending on how the information is shown on the screens of our devices[23]. Indeed, on the Net, our every choice is also the result of the layout of the user interface defined by the designer. So, for example, when the payment app Square Point of Sale, particularly used in the United States, opted for cleaner and more immediate graphics, it facilitated the release of tips to traders, who increased in number and size[24]. The effectiveness of this "new mass communication strategy"[25] is linked to the fact that people are now used to making judgments or making decisions (concerning the destination of a trip, the right partner in life, the best market investment) essentially on the screen, which has become "the scene, the stage of actions and relationships here and now […] in which subjects live and (rap-)present their stories"[26]. On the screen, however, everything can be questioned and reconstructed from scratch an infinite number of times to facilitate access to products and services by the user(-consumer) or, more simply, to encourage their eagerness to share. And who knows how to take advantage of this remarkable and rapid engineering, which is a real art of design, can achieve amazing results on an economic level, of innovation and above all multisensory involvement. From here, the user interface is enriched with elements subservient to the logic of the so-called digital

[23] BENARTZI, LEHRER 2015.
[24] CARR 2013.
[25] AMATO MANGIAMELI 2017, 158.
[26] Therein, 150.

nudging[27]. The reference is to: banner[28], pop-up[29] and landing page[30] that create targeted graphics; specific sections, such as consumer feedback; ambiguous configurations such as the so-called dark patterns, capable of misleading Internet users in the expression of their actual preferences[31]. Just think, for example, of the default settings, which are often accepted passively with significant consequences regarding the conferment of personal data to Internet service providers. This, on the one hand, is representative of the common tendency of users to leave things as they are, while on the other, it demonstrates how the characteristics of virtual environments can alter behavior in a predictable way, without the need to leverage substantial economic incentives nor, moreover, prohibit any choice, but only by implementing a kind of *libertarian paternalism*[32]. It is enough then that the procedures to change the default settings are purposely long and complex for users to desist.

---

[27] WEINMANN, SCHNEIDER, VOM BROCKE 2016, 433-436; MIRSCH, LEHRER, JUNG 2017, 634-648.

[28] Advertisements placed in some strategic points of a Web page, within special boxes or highly visible rectangles, whose purpose is certainly to stimulate the user to click on them to deepen the topic presented – when you do not click on it by mistake – and thus increase advertising revenue.

[29] All those communicative elements that during surfing the Net suddenly overlap with the content of the visited Web page to attract our attention, sometimes to inform (the case of the pop-up on cookies or privacy policy), sometimes only to promote (think of the invitation, implemented through a so-called call to action, to subscribe to a newsletter or to leave a comment).

[30] The landing web page is created specifically for marketing purposes. The Internet user reaches it after clicking on a given link. Thanks to it, the homepage of a site is immediately linked to an advertising campaign in which the net-surfer finds himself/herself immersed and will most likely buy an additional paid service. For example, the extension of the warranty from one to two years (not always convenient for him/her) on the product just purchased.

[31] For a clear example of the main types of dark patterns, see EUROPEAN DATA PROTECTION BOARD 2022.

[32] To deepen the theory of *libertarian paternalism*, see THALER, SUNSTEIN 2022.

The reason lies in an interference operating at the level of the subconscious thanks to the contribution of heuristics and cognitive biases, according to which individuals, prone to inertia, are led not to decide or to postpone the same decision continuously, make choices based on emotions and/or feelings, are content with a partial information framework, reflect little on the long-term effects of their determination and end up imitating others because they feel basically judged[33]. A way of proceeding, this, perfectly in line with the duality typical of thought processes, that during daily activities are fast, automatic and guided by intuition (System 1), while they become slower, more tiring and more complicated when reason is called into question (System 2)[34]. The first types of process can sometimes be exploited by the designer of human-machine interaction to manipulate individuals and groups according to the logic of maximizing profit, encouraging them to buy more products or services than necessary, to use certain functions rather than others, and in general to increase the time spent on the Web, because more they are, for example, on social networks, the greater the economic benefit for the companies that manage them. This also operates the recommendation systems, which produce high business value, automatically select items of interest to the user, those that he/she will most likely appreciate because they are in line with his/her own propensities, to make them more visible and accessible, often in the form of an ordered list, and thus put in place an excellent neuromarketing strategy.

Now, considering that on the Net our ability to concentrate is continuously interrupted and distorted by an overwhelming amount of information almost impossible to process carefully, an appropriate use of digital nudging

---

[33] KAHNEMAN, SLOVIC, TVERSKY 1982.

[34] KAHNEMAN 2020. In truth, there are many theories that question the possibility of making such a clear distinction between the two categories of cognitive processes, consequence of the dualism of the mind, that is, the existence of two opposite systems. However, it is not appropriate here to dwell on them, because there would be a risk of going beyond the proper field of philosophical-juridical analysis, therefore please refer to the in-depth examination of VIALE 2018, in part. 25-53 and 81-98.

tools could certainly help us make more satisfying choices, overcoming the vulnerability inherent in the formation of our will. In other words, these tools could correct cognitive limitations inherent in our decision-making processes since behavioral economics have definitively removed the paradigm of absolute rationality of *homo œconomicus* as a decision-maker always capable of wise choices, because he is totally indifferent to the context in which he operates[35]. Moreover, the implementation of digital nudges, relatively small changes to the user interface, is fast, simple and cheap, yet very profitable, given that the Internet provides specific features, such as profiling, that allow a perfect customization of choices. Therefore, the fact remains that technologies rarely combine such choices in favor of individuals[36], to which it is required, therefore, increased awareness and greater sensitivity to their use[37].

Not only that, the design of devices, applications and websites could even be of public use if it succeeds in encouraging citizens to engage in socially responsible behavior, how to lead a healthy life, reduce litter and energy consumption, make donations or participate in charitable activities, simply planning options so that the most advantageous, not only for digital monopolists but above all for the community, you also become the most salient, convincing and easy to choose. In this regard, however, the user interface should be designed in such a way as to be increasingly fair, protective and sustainable, attentive to man as an end that qualifies progress,

---

[35] The first to propose the paradigm of *bounded rationality* contrary to that of *homo œconomicus* was SIMON (1955, 99-118).

[36] Not surprisingly, AMATO MANGIAMELI 2004, 15, illustrates how technologies, governed by new private forces (economic and political), while facilitating connections and synergies between individuals, also generate new vulnerabilities and inequalities, bringing with them "the risk of a global society in which an elite rules over electronic proletarians, no longer masters of bodies and minds".

[37] On how digital education, or rather, equal and conscious access to information technologies can contribute to overcoming poverty, see SARACENI 2019.

but oriented towards the common good[38]. Making good decisions, after all, is the most important skill of our lives, private and professional, as the planning of the future, both ours and others, depends on it.

4. FROM THE *JUNGLE* TO THE *GARDEN*: MORE SUSTAINABILITY AND SAFETY!

Despite the most optimistic expectations related to the examined approach to open data and the possible positive implications of digital nudging that, alongside the profit of a few, could convey the well-being of many if thought and designed to be at the service of man, there are still many critical issues and limitations regarding free access to information. In a context of data surveillance[39], the sources of risk multiply out of all proportion, mixing indiscriminately with the great opportunities offered by new technologies, and security and computer insecurity are constantly changing[40]. Individuals, rather than subjects of law and holders of rights, are often treated as means of economic and/or political ends[41], thus seeing the effective enjoyment of their freedoms jeopardized and even their own nature as thinking individuals and responsible for their said actions. Just think of how, in the case of marketing, they are reduced to mere *interfaces* between the product or service which is sometimes a human agent, sometimes artificial, or even

---

[38] BENANTI, MAFFETTONE 2022, 9-30.

[39] HELZEL 2023, 146-150.

[40] In this regard, the observations by CLARKE (1988, 498-512) are still relevant, taking a neutral approach with respect to dataveillance technologies, supporting their multiple purposes, and not all of them necessarily deplorable. Consider, for example, how the open data of the Public Administration allows citizens to control the work of rulers, to achieve a democracy that is both more transparent and more efficient.

[41] For a specific analysis of the role of digital communication for electoral purposes, see ZICCARDI 2019a, while for the effects of information technologies on the economic sector, reference should be made to SRNICEK 2017.

hybrid wants to sell and their monetary resources[42]. In this *interfacing process*, profiling and recommendation systems managed by AI can certainly play a crucial role, but if it only matters the result to be achieved, there are some concerns about *algorithmic governability*[43] and the consequent dehumanization of people[44].

Now, if this is the picture, only a well-regulated alliance between technology and law, inspired by the principles of proportionality and transparency as well as the highest moral values, could represent the cornerstone of a far-sighted democratic response to possible violations (of different order and degree) that lurk in the folds of digital. On the one hand, law can put technology at the service of mankind, of his/her freedom, of its civil growth and also of its security; on the other, technology, in serving individual rights and stakeholder demands, must not be unidirectional, but must guarantee a development as harmonious as possible if one does not want to contradict the formula of the Kantian categorical imperative that one must always act by treating humanity, both in oneself and in that of others, as an end and never simply as a means[45].

Faced with a paternalism in libertarian theory only that, assuming an increasingly private character, seems to leave great freedom to citizens-users-consumers while through prods it threatens the neutrality of the Rule of law, the need for computer security[46] is very concrete and urgent, to be declined necessarily in a supranational key. On the other hand, moving within a deterritorialized space[47], where vulnerabilities are also global, it is essential to shift the regulatory framework, including general principles,

---

[42] FLORIDI cit., in part. 135-145.

[43] I make my own the evocative and effective expression of ROUVROY 2017.

[44] FIORIGLIO 2021, 53-67.

[45] KANT 1995, 88.

[46] For a thorough examination of computer security, see ATERNO 2022.

[47] Deterritorialization is part, together with decentralization and dataveillance, of the three founding guidelines of the new digital space, as AMATO MANGIAMELI explains (2000, in part. 1-25, and more recently, 2023, 101-107).

detailed sector disciplines, as well as proactive ethical guidelines[48], from the state to the interstate horizon. Furthermore, it is no longer possible to identify security on the Net with the sole activation and implementation of all those hardware and software tools, therefore purely informatic, suitable to protect us from hacker attacks and incursions in our most intimate sphere. Being immersed daily in a dense swarm of information, where we move perhaps too casually without adopting prudential attitudes at the same time, and hardly ever almost respecting that duty of diligence of the *pater familias* that must apply both in the real and in the virtual, it is appropriate to take a further step from an eminently cultural point of view. Cybersecurity, in other words, must also include capacity, that the whole of civil society is called to bring to maturity, to be able to accept and critically manage the *reontologizing* and *rehistoricizing power* of digital and AI technologies, so as not to arrive, in enthusiastic admiration and indiscriminate, to entrust to cold algorithms the most important decisions of our lives, how to marry or what career to pursue. In doing so, digital itself, too often abandoned to the crude logic of the market, without a community project and instead the prerogative of a few (and often brutal) U.S. monopolists, would acquire an extraordinary strength that would benefit individual and collective well-being. And so, the chaotic *jungle* dominated by mechanisms that are often obscure and ethically reprehensible would become a clear and pluralistic *garden*, built on the

[48] SARTOR 2022, p. 100, doubts that rules and principles, as well as their implementation by the public authorities, may be sufficient to ensure adequate protection of citizens in the absence of the development of counter-powers or compensatory powers of civil society, to which to entrust the important task of detecting abuses, inform the public, promote enforcement, exert forms of collective pressure. And this also using (to its advantage) the same means used by the (IT) power to which society wants to oppose, therefore AI and its systems.

foundations of solidarity[49], trust[50] and sharing[51].

5. ACCOUNTABILITY AS A LITMUS TEST

Moving now in a mirrored direction, the value and need of cybersecurity, as well as the important prerogative of individuals, can also represent an opportunity in terms of operations and efficiency for all those small entrepreneurial realities or large, whether public or private, that in data management know how to take a so-called risk-centric perspective[52]. This is a novel approach that uses *ex ante* assessment of possible negative individual freedom impacts and rights related to the processing operations in a given organization, thanks to which to independently determine, that is, without asking for prior *placet* to the Supervisory Authorities as happened in the past, the most appropriate measures (technical, physical, logical, operational) to mitigate these impacts, taking into account processes, needs and

[49] For a reconstruction of the different forms of solidarity (juridical, civil, family), that within the legal system transcend purely economic private interests with a view to higher public ends and whose mutual implication is considered even necessary for the full development of the person and for the realization of the widest social cohesion between citizens and foreigners, please refer to AMATO MANGIAMELI 2022b, in part. 132-141.

[50] On the crisis of mutual trust afflicting contemporary society, so individuals are often wary of information received through digital media (and/or public institutions) even though I can't do without it, and on the necessity of its rebirth as a precondition for social cooperation, and therefore an indispensable resource for the achievement of objectives of common interest, see O'NEILL 2003.

[51] With respect to sharing as a structural paradigm of the Net that stimulates innovation, transparency and the search for aggregation against the personal (and competitive) interest of material gain typical of capitalism (just think of the peer-to-peer protocol, open-source software, the same end-to-end architecture), see: CARLSSON 2009; RIFKIN 2017.

[52] See *ex multis*: MANTELERO 2017, 144-164; D'AMBROSIO 2017; BALDI, MULA 2020, 167-200.

mechanisms within the organization itself[53]. To ensure the highest levels of security, these measures must: *i*) be adopted from the earliest stages of design of products, applications and services of the company and then persist throughout the processing chain; *ii*) vary according to the different circumstances and the technological tools used from time to time to process the data; *iii*) be integrated within a dynamic corporate style so that they are not reduced to a mere (and inflexible) check-list of regulatory obligations. Moreover, decisions based on contextualization may prove to be more effective than decisions made for the sole purpose of adapting to abstract criteria laid down by law[54], promoting compliance with the general principles applicable to the protection of personal data[55].

---

[53] For further considerations on how to decline the principle of accountability, please refer to ZICCARDI 2019b, 87-90.

[54] This is why the Regulation (EU) does not contain an exhaustive and precise list of security measures to be activated so that data is not stolen, lost or used in a manner distorted with respect to the purposes for which they were collected, but it is expressed only in terms of their adequacy for risk, that is to say, effective protection of natural persons. Indeed, the GDPR provides operational indications aimed at identifying the measures suitable to ensure compliance with the legislation, and to demonstrate it, even if nothing can exempt the controller from any verification activities by the Supervisory Authorities. Among these activities, it is important to point out here: the identification and subsequent appointment of any processors (art. 28); the correct authorization and instruction of natural persons who process personal data under the direct authority of the controller (art. 29); the development of its own security plan as appropriate and effective as possible with respect to the risk inherent in the characteristics of operations involving personal data, balancing opposing interests with full autonomy of judgment and looking yes to costs, but also to the state of the art and the best available technologies (art. 32); the preparation of data protection impact assessments (or DPIA) when a processing presents a high risk for the rights and freedoms of natural persons and upstream of the processing itself (art. 35); the designation of a data protection officer (art. 37); the adoption of codes of conduct and the obtaining of certifications (artt. 40-42).

[55] These are the principles of lawfulness, fairness, transparency, purpose limitation and storage, minimization, accuracy, integrity and confidentiality, sanctioned by art. 5, par. 1, of the GDPR, which the controller is not only called upon to observe, but must also be

All this would allow Regulation (EU) 2016/679 (*General Data Protection Regulation* or GDPR)[56], built entirely on the concept of accountability[57], to unveil its great potential, demonstrating how the provision of solutions to reinvigorate the increasingly compromised privacy of individuals can be a source of competitive advantage for the various Internet service providers, and for the user, a reason to trust in digital[58].

In more detail, when we talk about accountability as an operational strategy that emphasizes the substance of the fulfillment in terms of creativity and proactivity of the controller[59] and its verifiability (in fact and not only on

able, *ex* art. 5, par. 2, to prove that you have complied, especially with regard to the adequacy and effectiveness of the security measures actually used. For a clearer examination of these principles, please refer to AMATO MANGIAMELI 2020b, in part. 62 ss.

[56] Among the contributions to say the least numerous on the new Regulation (EU) are: BOLOGNINI, PELINO, BISTOLFI 2016; CICCIA MESSINA, BERNARDI 2017; FINOCCHIARO 2019; RICCIO, SCORZA, BELISARIO 2022.

[57] In truth, the concept of accountability, as a strategic axiom that empowers different organizations to protect the security of computer systems, networks, personal data and company secrets, permeates the entire European cybersecurity regulatory sector: Directive (EU) 943/2016, aimed at protecting know-how and confidential business information (trade secrets) against acquisition, unlawful use and disclosure, carried out in Italy with d.lgs. n. 63/2018; Directive (EU) 1148/2016 (so-called NIS 1), containing measures for a high common level of security of networks and information systems in the Union and implemented in our Country with d.lgs. n. 65/2018 (now repealed); Regulation (EU) 881/2019 (so-called Cybersecurity Act); more recently, Regulation (EU) 2554/2022 (or DORA Regulation), on digital operational resilience for the financial sector, and Directive (EU) 2555/2022 (so-called NIS 2), still in the process of transposition, that art. 21 requires public and private entities operating in essential and important services to take technical measures, adequate and proportionate operational and organizational to manage the security risks of the IT and network systems used in their activities or in the provision of services, as well as to prevent or minimize the impact of accidents on the recipients of the services themselves.

[58] CELELLA 2018, 211-224.

[59] Pursuant to art. 4, par. 1, n. 7, of the GDPR, the controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". A figure, this, today central and

paper) by the Supervisory Authorities, the reference is to two different but related sides: on the one hand, the responsibility to build a data management system that is as secure as possible, preparing measures and procedures adapted to the nature of the data, but also constantly reviewable and updatable, especially following the emergence of new vulnerabilities; on the other hand, the need to report on what has been done for security reasons, pre-establishing a documentary apparatus to be shown for this purpose to the Supervisory Authorities to prove that they have correctly complied with the provisions of the law (art. 24, par. 1, of the GDPR). It is the so-called procedural burden of proof, which can be well acquitted just by filling in the record of processing activities[60] if you do not want to incur the huge financial penalties imposed pursuant to art. 83, par. 5, lett. *a*) of the GDPR[61].
With a pragmatic view to applying the principle of accountability, always aimed at (and only) placing individuals with their rights at the center of IT activity, particular attention should then be paid to the technique commonly summarized by the expression "data protection by default and by design" (art. 25 of the GDPR) for which the controller must *ab origine*, that is, from the moment of the simple design of a service based on personal information, minimize both the amount of data collected, and the extent of the processing carried out after their acquisition.
In the latter case, the use of prudent pseudonymization, to attribute

strategic to ensure a real protection of the fundamental right to the protection of personal data in any context, be it real or virtual, since it is entirely discretionary, as well as the consequent liability, the methods of implementing the principles and basic rules of European legislation.

[60] The record of processing activities, newly introduced by European legislation and governed by art. 30 of the GDPR, is the tool that allows the controller to keep track of all the treatments in place in its organizational structure and that, if requested, must be made available to the Supervisory Authorities, since at the time of the audit it can offer a complete picture of the degree of corporate compliance.

[61] For an in-depth analysis of the sanctioning framework, please refer to BORRILLO 2020, 326-356.

personal data to a specific data subject only by using additional knowledge (or reidentification keys) that are not available to everyone (art. 4, par. 1, n. 5, and recital 28 of the GDPR), can certainly make the difference as a virtuous index of technological security, allowing damage to be prevented rather than repaired, just as the conscious and documented responsibility placed on the part of the controller wants. On the other hand, in the face of the enormous weight (social, economic and political) assumed today by the data, a revolutionary change of perspective is increasingly needed: the centre of gravity of the protection of individuals must progressively shift from the *ontological* moment of the collection of data concerning them to the *epistemological* one, certainly more elusive, than their analysis to always obtain new indications[62]. Precisely the latter, used too often subtly by those who handle data, they allow us to influence almost all our daily decisions. And in doing so between prods and deficiencies of human cognition, they almost always hit the target, now having new and indispensable allies: logos, shapes, colors and persuasive effects of Web design. All that remains is to formulate single but fundamental hope, the only one able to inextricably weld together technical-IT aspects, sociocultural and distinctly legal: more security, for everyone and for the benefit of all!

[62] But if this is the case, that is, if the holders of computer power can come to know, in an incomparable way, more than even an absolute monarch of the past could know of his subjects, as BOBBIO (1985, 21) already announced a few years ago, "the figure of the citizen is impoverished, while that of the subject re-emerges and that of the consumer is forcefully imposed" (RODOTÀ 2004, 172).

REFERENCES

AMATO MANGIAMELI, Agata C., *Stati post-moderni e diritto dei popoli*, Turin, 2004.

– *Tecno-regolazione e diritto. Brevi note su limiti e differenze*, 147-167, in *Il diritto dell'informazione e dell'informatica*, 32, 2/2017.

– *Algoritmi e big data. Dalla carta sulla robotica*, 107-124, in *Rivista di filosofia del diritto*, 8, 1/2019.

– *Diritto e Cyberspace. Appunti di informatica giuridica e filosofia del diritto*, Turin, 2000.

– *Un nuovo bene: l'informazione*, 29-44, in AMATO MANGIAMELI, Agata C., CAMPAGNOLI, Maria Novella, *Strategie digitali. #diritto_educazione_tecnologie*, Turin, 2020a.

– *Qualche nuovo s/oggetto. Tra algoritmi, intelligenza artificiale, big data*, 45-74, in AMATO MANGIAMELI, Agata C., CAMPAGNOLI, Maria Novella, *Strategie digitali. #diritto_educazione_tecnologie*, Turin, 2020b.

– *Intelligenza artificiale, big data e nuovi diritti*, 93-101, in *Rivista italiana di informatica e diritto*, 1/2022a.

– *I diritti umani tra teorie e prassi*, Turin, 2022b.

– *Cyberspace* (entry), 101-107, in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

ATERNO, Stefano, *Sicurezza informatica. Aspetti giuridici e tecnici*, Pisa, 2022.

BALDI, Alessio, MULA, Davide, *Responsabilità civile e intelligenza artificiale*, 167-200, in TADDEI ELMI, Giancarlo, CONTALDO, Alfonso (eds.), *Intelligenza artificiale. Algoritmi giuridici. Ius condendum o "fantadiritto"?*, Pisa, 2020.

BARBERIS, Mauro, *Come Internet sta uccidendo la democrazia. Populismo digitale*, Milan, 2020.

BENANTI, Paolo, MAFFETTONE, Sebastiano, *Decisioni politiche e sostenibilità digitale*, 9-30, in SEVERINO, Paola (ed.), *Intelligenza artificiale. Politica, economia, diritto, tecnologia*, Rome, 2022.

BENARTZI, Shlomo, LEHRER, Jonah, *The Smarter Screen: Surprising Ways to Influence and Improve Online Behavior*, New York, 2015.

BOBBIO, Norberto, *Stato, governo, società. Frammenti di un dizionario politico*, Turin, 1985.

BOLOGNINI, Luca, PELINO, Enrico, BISTOLFI, Camilla, *Il Regolamento Privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milan, 2016.

BORRILLO, Barbara, *La tutela della privacy e le nuove tecnologie: il principio di accountability e le sanzioni inflitte dalle Autorità di controllo dell'Unione europea dopo l'entrata in vigore del GDPR*, 326-356, in *Dirittifondamentali.it*, May 18, 2/2020.

BRADBURY, Ray, *Fahrenheit 451*, trad. it., Milan, 1978.

CAMPAGNOLI, Maria Novella, *Informazione, social network & diritto. Dalle fake news all'hate speech online. Risvolti psicologici, profili giuridici, interventi normativi*, Milan, 2020.

CARLSSON, Chris, *Now Utopia. Come il ciclismo creativo, l'orticoltura comunitaria, la permacoltura, la galassia P2P e l'ecohacking stanno reinventando il nostro futuro*, trad. it., Milan, 2009.

CARR, Austin, *How Square Register's UI Guilts You into Leaving Tips*, in *Fast Company Magazine*, December 12, 2013.

CELELLA, Rosanna, *Il principio di responsabilizzazione: la novità del GDPR*, 211-224, in *Ciberspazio e Diritto*, 19, 1-2/2018.

CICCIA MESSINA, Antonio, BERNARDI, Nicola, *Privacy e Regolamento europeo*, Milan, 2017.

CLARKE, Roger A., *Information Technology and Dataveillance*, 498-512, in *Communications of the ACM*, 31, 5/1988.

D'AMBROSIO, Marcello, *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Naples, 2017.

DIONIGI, Ivano, *Osa Sapere. Contro la paura e l'ignoranza*, Milan, 2019.

EUROPEAN DATA PROTECTION BOARD, *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*, in *https://edpb.europa.eu/our-work-tools/documents/public-*

consultations/2022/guidelines-32022-dark-patterns-social-media_en., Bruxelles, May 2, 2022.

FINOCCHIARO, Giusella, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019.

FIORIGLIO, Gianluigi, *La società algoritmica fra opacità e spiegabilità: profili informatico-giuridici*, 53-67, in *Ars interpretandi*, 26, 1/2021.

FLORIDI, Luciano, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, trad. it., Milan, 2017.

– *Il verde e il blu. Idee ingenue per migliorare la politica*, Milan, 2020.

GRANIERI, Giuseppe, *La società digitale*, Rome-Bari, 2006.

HARARI, Yuval N., *Homo Deus. Breve storia del futuro*, trad.it., Milan, 2018.

HELZEL, Paola B., *Dataveglianza* (entry), 146-150, in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

KAHNEMAN, Daniel, SLOVIC, Paul, TVERSKY, Amos (eds.), *Judgment under Uncertainty: Heuristics and Biases*, Cambridge, 1982.

KAHNEMAN, Daniel, *Pensieri lenti e veloci*, trad. it., Milano, 2020.

KANT, Immanuel, *Fondazione della metafisica dei costumi*, in *Scritti morali*, trad. it., Turin, 1995.

LÉVY, Pierre, *L'intelligenza collettiva. Per un'antropologia del cyberspazio*, trad. it., Milan, 2002.

MANTELERO, Alessandro, *Responsabilità e rischio nel Regolamento UE n. 2016/679*, 144-164, in *Le nuove leggi civili commentate*, 15, 1/2017.

MAYER-SCHÖNBERGER, Viktor, RAMGE, Thomas, *Reinventare il capitalismo nell'era dei big data*, trad. it., Milan, 2018.

MIRSCH, Tobias, LEHRER, Christiane, JUNG, Reinhard, *Digital Nudging: Altering User Behavior in Digital Environments*, 634-648, in LEIMEISTER, Jan M., BRENNER, Walter (eds.), *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)*, St. Gallen, 2017.

O'NEILL, Onora, *Una questione di fiducia*, trad. it., Milan, 2003.

RAMGE, Thomas, MAYER-SCHÖNBERGER, Viktor, *Fuori i dati! Rompere i monopoli sulle informazioni per rilanciare il progresso*, trad. it., Milan, 2021.

RICCIO, Giovanni M., SCORZA, Guido, BELISARIO, Ernesto (eds.), *GDPR e Normativa Privacy. Commentario*, Milan, 2022.

RIFKIN, Jeremy, *La società a costo marginale zero. L'Internet delle cose, l'ascesa del 'Commons' collaborativo e l'eclissi del capitalismo*, trad. it., Milan, 2017.

RODOTÀ, Stefano, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Rome-Bari, 2004.

– *Il diritto di avere diritti*, Rome-Bari, 2015.

ROUVROY, Antoinette, *Gouverner hors les normes: la gouvernementalité algorithmique*, in *Lacan Quotidien*, 733, July 6, 2017.

SADIN, Éric, *La siliconizzazione del mondo. L'inarrestabile espansione del liberismo digitale*, trad. it., Turin, 2018.

SARACENI, Guido, *Digital Divide e povertà*, 1-19, in *Dirittifondamentali.it*, October 28, 2/2019.

– *Big data* (entry), 41-46, in AMATO MANGIAMELI, Agata C., SARACENI, Guido (eds.), *Cento e una voce di informatica giuridica*, Turin, 2023.

SARTOR, Giovanni, *L'intelligenza artificiale e il diritto*, Turin, 2022.

SHAPIRO, Carl, VARIAN, Hal R., *Information Rules. A Strategic Guide to the Network Economy*, Cambridge, 1998.

SIMON, Herbert, *A Behavioral Model of Rational Choice*, 99-118, in *The Quarterly Journal of Economics*, 69, 1/1955.

SRNICEK, Nick, *Capitalismo digitale: Google, Facebook, Amazon e la nuova economia del Web*, Rome, 2017.

THALER, Richard H., SUNSTEIN, Cass R., *Nudge. La spinta gentile. La nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità. L'edizione definitiva*, trad. it., Milan, 2022.

TINCANI, Persio, *Controllo e sorveglianza*, 19-40, in BRIGHI, Raffaella, ZULLO, Silvia (eds.), *Filosofia del diritto e nuove tecnologie*, Rome, 2015.

– *Un altro dono dello spirito maligno. Nuova sorveglianza e comportamenti individuali*, 19-63, in PELLICCIOLI, Luca (ed.), *La privacy nell'età dell'informazione. Concetti e problemi*, Milan, 2016.
– *Sorveglianza e potere. Disavventure dell'asimmetria cognitiva*, 51-78, in *Ragion pratica*, 1/2018.
VIALE, Roberto, *Oltre il nudge. Libertà di scelta, felicità e comportamento*, Bologna, 2018.
WEINMANN, Markus, SCHNEIDER, Christoph, VOM BROCKE, Jon, *Digital Nudging*, 433-436, in *Business & Information Systems Engineering*, 58, 6/2016.
ZICCARDI, Giovanni, *Tecnologie per il potere. Come usare i social network in politica*, Milan, 2019a.
– *Il GDPR e i suoi adempimenti*, 87-90, in ZICCARDI, Giovanni, PERRI, Pierluigi (eds.), *Tecnologia e diritto*, II, Milan, 2019b.
– *Diritti digitali. Informatica giuridica per le nuove professioni*, Milan, 2022.
VON DER LEYEN, Ursula, *Shaping Europe's Digital Future: Op-Ed by Ursula von der Leyen, President of the European Commission*, in *https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260*, Bruxelles, February 19, 2020.