The Crisis of the Right to Informational Self-Determination

Angela Vivarelli*

Abstract

This paper focuses on changes in data protection regulation and especially on the risks concerning informational self-determination and privacy created by technologies. The analysis starts from the growing ability to control informational flows – the beating heart of the informational self-determination principal – and goes on to examine consent as a 'tool' for managing personal data. In reality, the evolution of information and communication technologies affects consent, which becomes an 'instrument for building self-identity on the Internet'. There are several factors – with the advent of new tecnologies – that lead to the crisis of consent. The critical issues arise not only from the modern idea of privacy but also from current challenges to data protection regulation, such as the 'privacy paradox', 'datafication', profiling, and Big Data analytics. Starting from the impact these phenomena have on fundamental rights and freedoms, the research question is whether the GDPR's 'privacy by design' offers a satisfying solution or whether a more complex and global reflection is required.

I. Introduction

Within a global landscape dominated by information technologies able to gather millions of personal data each day, reflection on new rules to protect people's fundamental rights and freedoms (the protection of personal identity, freedom of expression, and pluralism of information) becomes a necessity. In such a scenario, observance of the informational self-determination principle requires not only a sufficiently broad ability to control the collection and use of personal data but also the conscious ability to give free, informed, specific, and unambiguous consent for data processing.

The obscure and intricate use of data, and the increasing use of automated decisions, typical of digital services and Big Data analytics, portend significant risks for the fundamental rights and freedoms of data subjects. The paper therefore also focuses on phenomena such as the 'privacy paradox', 'datafication', and profiling, which concretely undermine any guarantee of free and informed consent.

Taking these considerations as its starting point, the General Data Protection Regulation (GDPR)[1] tries to enhance data subject awareness through its

* PhD in Private Law, University of Sannio.

[1] Regulation (EU) 2016/679 (GDPR) of the European Parliament and of the Council of 27

implementation in IT solutions and web architecture. Against such a background, this paper seeks to show that the GDPR's 'privacy by design' offers only a partially satisfactory solution. As will emerge below, a more complex and global reflection is called for considering that, although this innovative approach appears interesting, it neverthless requires some adjustment along the lines of Stefano Rodotà's suggestion:

> 'not everything technologically possible is also socially desirable, ethically acceptable, legally justified'.[2]

On the basis of these observations, Section 2 will address the transition from the right to informational self-determination to the new paradigm of 'privacy self-management'. Section 3 will address the downward spiral of consent and its crisis caused by the advent of new tecnologies. Sections 4, 5, and 6 will illustrate some of the current challenges in the field of data protection regulation (such as the 'privacy paradox', 'datafication', profiling, and Big Data analytics). Specifically, they will focus on the impact of these phenomena on fundamental rights and freedoms. Lastly, there are some concluding remarks on the GDPR's 'privacy by design' solution, evaluting the degree of protection it affords the human person.

II. From 'Informational Self-Determination' to 'Privacy Self-Management'

Informational self-determination became recognized as a right through the decision handed down by the German Constitutional Court in 1983, stating that each person has the right to decide on the transfer, circulation, and use of his or her personal data (*das information Selbstbestimmungsrech*).[3]

April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. On the GDPR see, *inter alia*, M. Maglio et al, *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento UE 2016/679* (Santarcangelo di Romagna: Maggioli Editore, 2017); G. Buttarelli, 'The EU GDPR as a clarion call for a new global digital gold standard' 2 *International Data Privacy Law*, 77 (2016); G. Finocchiaro, *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali* (Bologna-Roma: Zanichelli, 2017); F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Torino: Giappichelli, 2016); F. Di Resta, *La nuova 'Privacy europea': I principali adempimenti del regolamento UE 2016 e profli risarcitori* (Torino: Giappichelli, 2018); C. Kuner et al, *Commentary on the EU General Data Protection Regulation* (Oxford: Oxford University Press, 2018); G.M. Riccio et al, *Gdpr e normativa privacy. Commentario* (Assago: Wolters Kluwer, 2018); M. Soffientini, *Protezione e trattamento dei dati* (Assago: Wolters Kluwer, 2018).

[2] S. Rodotà, Discorso del Presidente del Garante, Relation 2003.

[3] *Volkszählungsurteil, Bundesverfassungsgericht* 15 December 1983, 1 BvR 209/83, *Neue juristische Wochenschrift*, 419 (1984) with comment of S. Simitis, 'Die informationelle Selbstbestimmung – Grundbedingungen einer verfassungskonformen Informationsordnung' *Neue juristische Wochenschrift*, 398 (1984). W. Steinmüller, 'Das informationelle Selbstbestimmungsrecht: wie es entstand und was man daraus lernen kann' *Recht der Datenverarbeitung*, 158 (2007); G.

Modern technologies and the automated processing of personal data allow operations that were almost unimaginable in the past, but they can have an adverse effect on the dignity and free development of individuals' personalities. On these grounds, the German Court identified two fundamental freedoms: the right to the free development of one's personality (Art 2, para 1, of the German Constitution), and the unviolability of human dignity (Art 1, para 1, of the German Constitution). From these norms a fundamental right emerges that envisages the right of individuals to self-determination and to establish, autonomously and without interference, when self-disclosure is lawful and fair.

In its original formulation, the right to informational self-determination is the result of a biphasic protection mechanism. In the passive phase, the controller (or processor) informs the data subject regarding the characteristics of the processing (purposes, methods, limits, etc). The right to informational self-determination is then expressed in the active phase, when the data subject can influence the communication flows relating to his or her personal data.[4]

In Italy, the first ruling of the Italian Data Protection Authority (the BNL case) recognizes the right to informational self-determination in its statement:

> 'consent can be effectively considered free only if it appears as a manifestation of the right to informational self-determination, therefore shielded from any pressure, and if it is not conditional upon accepting clauses that bring about any significant imbalance relating to the rights and obligations arising from the contract'.[5]

From this perspective, an individual not only decides if and how to disclose personal information; s/he also has the power to control its subsequent dissemination. This result definitively marks the transition from a static view of privacy to a dynamic one known as 'informational privacy'.[6] This is defined in scholarship as the transition from the 'person-information-secrecy' trinomial to

Sartor, 'Tutela della personalità e normativa per la protezione dei dati. La sentenza della corte costituzionale tedesca sul censimento del 1983 nel dibattito dottrinale sui profili costituzionalistici del Datenschutz' *Informatica e diritto*, 95 (1986). For a broad overview, P. Schwartz, 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination' 38 *American Journal of Comparative Law*, 686 (1989).

[4] See, for all, A. Mantelero, 'Privacy' *Contratto e impresa*, 757 (2008).

[5] The Italian Data Protection ruling of 28 May 1997, Bollettino 'Cittadini e Società dell'Informazione', Anno I – May/July 1997 – *Il Foro italiano*, 3 (1997). For a comment, cf V. Zeno-Zencovich, 'Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del Garante' *Corriere giuridico*, 915 (1997).

[6] S. Rodotà, *Il diritto di avere diritti* (Roma-Bari: Edizioni Laterza), 319, discussed about a 'reinvention of the privay'. S. Warren and L. Brandeis, 'The Right to Privacy' 5 *Harvard Law Review*, 193-220 (1890), signed the passage from the 'privacy-property' to the 'privacy-dignity'. See also G.B. Ferri, 'Persona e privacy', in Id et al, *Il riserbo e la notizia. Atti del Convegno di Studio. Macerata, 5-6 marzo 1982* (Napoli: Edizioni Scientifiche Italiane, 1983), 61 and G. Buttarelli, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione* (Milano: Giuffrè, 1997), 3.

the 'person-information-circulation-control' quadrinomial.[7]

A data subject's self-disclosure choice is significantly aided by consent, through which data subjects authorize (or deny) third parties to use their personal information.[8] In general terms, according to the regulation, consent forms one of the legal bases for lawful and fair data processing (in EU law, Art 7, Directive 95/46/CE; in Italian law, Art 23 of the Privacy Code) and is considered an instrument for monitoring personal informational flows. Consent means any freely given, specific, informed, and unambiguous indication on the part of the data subject that s/he agrees, through a statement or clear affirmative action, to his or her personal data being processed. These basic requirements for effective and legally valid consent allow people to know the identity of the controller or the processor, and the purposes and limits of use, as well as their rights. Consent re-emerges in a stronger form in the new regulatory framework:[9] Arts 6 and 7 and Recital 32 GDPR state that not only must it be freely given, informed, and specific, but also unambiguous (Art 4, lett 11) GDPR), expressed through clear affirmative action as a guarantee that the data subject fully agrees to make personal data available. On the basis of these provisions therefore, silence, pre-ticked boxes, or inactivity cannot constitute consent. Thanks to innovations and

[7] S. Rodotà, *Tecnologie e diritti* (Bologna: il Mulino, 1995), 102; S. Sica, Sub *artt. 1-6. Principi generali*, in Id and P. Stanzione eds, *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196* (Bologna: Zanichelli, 2004), 4. In such way, Corte di Cassazione 5 April 2012 no 5525, *Danno e Responsabilità*, 747 (2012); *Il diritto dell'informazione e dell'informatica*, 10 (2012); with commentary of G. Citarella, 'Aggiornamento degli archivi online, tra diritto all'oblio e rettifica «atipica»' *Responsabilità civile e previdenza*, 1147 (2014), in which the Supreme Court states 'il D.Lgs. 196 del 2003 ha (…) sancito il passaggio da una concezione statica a una concezione dinamica della tutela della riservatezza, tesa al controllo dell'utilizzo e del destino dei dati. L'interessato è divenuto compartecipe nell'utilizzazione dei propri dati personali'.

[8] See V. Carbone, 'Il consenso, anzi i consensi, nel trattamento informatico dei dati personali' *Danno e responsabilità,* 23 (1998); D. Messinetti, 'Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali' *Rivista critica di diritto privato*, 350 (1998); F. Cafaggi, 'Qualche appunto su circolazione, appartenenza e riappropriazione nella disciplina dei dati personali' *Danno e responsabilità*, 615 (1998); S. Sica, 'Il consenso al trattamento dei dati: metodi e modelli di qualificazione giuridica' *Rivista di diritto civile*, 612 (2001).; S. Niger, 'Il «mito» del consenso alla luce del codice in materia di protezione dei dati personali' *Cyberspazio e diritto*, 499 (2005); A. Fici and E. Pellecchia, 'Il consenso al trattamento', in R. Pardolesi ed, *Diritto alla riservatezza e circolazione dei dati personali* (Milano: Giuffrè, 2003), I, 504; S. Mazzamuto, 'Il principio del consenso e il problema della revoca', in R. Panetta ed, *Libera circolazione e protezione dei dati personali* (Milano: Giuffrè, 2006), 996; G. Oppo, Sul consenso dell'interessato, in V. Cuffaro et al eds, *Trattamento dei dati e tutela della persona* (Milano: Giuffrè, 1998), 124. In the recent literature, E. Kosta, *Consent in European Data Protection Law* (Leiden-Boston: Martinus Nijhoff Publisher, 2013), 51; F. Bravo, 'Il consenso e le altre condizioni di liceità del trattamento di dati personali', in G. Finocchiaro ed, *Il nuovo Regolamento europeo sulla privacy* n 1 above, 101; S. Thobani, *I requisiti del consenso al trattamento dei dati personali* (Sant'Arcangelo di Romagna: Maggioli Editore, 2016), 84. The Working Group Art 29 published the *Guidelines on Consent under Regulation 2016/679*, 28 November 2017, 18-19, available at tinyurl.com/y9bpzs66 (last visited 7 July 2020); before, see the *Opinion on Consent* 15/2011.

[9] According to the GDPR, suitable articles are; while suitable recitals are (32-33-38-40-42-43-50-51-54-71-111-155-161-171).

developments in communication technology, the user's consent becomes a tool for regulating information flows, and the advent of social networks and sharing online platforms make consent an 'instrument for building self-identity on the Internet'.[10] In this vein, users play an active role by managing their own data flows, protected by transparent rules on collection and processing. The aim is to enable data subjects to make informed decisions regarding the circulation of their data in a specific context at a specific time. This approach should be a source of empowerment for users and, at the same time, ensure the right to informational self-determination.

In North American literature, this approach is summed up in the formula 'privacy self-management',[11] based on the 'notice and choice' mechanism.[12] This expression refers to a means through which users give free, informed, and specific consent to processing their personal data and can control how their own identity is constructed in the online environment.

III. From Physiology to Pathology: The Downward Spiral of Consent

Behind the allure of 'privacy self-management' lurks the failure of the edifice itself.[13] The freedom and informed nature of consent are undermined by the processing of data that bypass the data subject's approval. In reality, they favour the commercial exploitation of personal data, jeopardizing users' privacy, personal

[10] On this point, D. Messinetti, *Circolazione dei dati* n 8 above, 348-349, underlines 'l'identità personale viene considerata come un corpo che dà luogo ad un dispositivo di socializzazione. Un dispositivo, cioè, che ha la sua ragione d'essere nel fatto che l'informazione crea conoscenza intorno all'identità personale; esso ha tra i suoi obiettivi principali quello di riprodurre il gioco delle relazioni nella quali la persona può rientrare. Il dispositivo di tutela, perciò, tende in questa prospettiva, a estendere le forme di controllo e a mantenere la legge ce le governa nella forma della riservatezza'.

[11] For an explanation of this mechanism, see D. Solove, 'Privacy Self-Management and the Consent Dilemma' *Harvard Law Review*, 1880 (2013).

[12] P. Schwartz and D. Solove, 'Notice and Choice: Implications for Digital Marketing to Youth', available at tinyurl.com/ybun5ps3 (last visited 7 July 2020) highlight 'the idea behind notice and choice can be summarized in this fashion: as longas a company provides notice of its privacy practices, and people have some kind of choice about whether to provide the data or not, then privacy is sufficiently protected'; R. Warner and R. Sloan, 'Beyond Notice and Choice: Privacy, Norms and Consent' *Journal of High Technology Law*, 6 (2014); S. Fischer-Hübner et al, 'Online Privacy: Towards Informational Self-Determination on the Internet, Manifesto from Dagstuhl Perspectives Workshop' 1106 (2011), available at tinyurl.com/y72tt59c (last visited 7 July 2020) underlined 'user-centric identity management allows users to detect any linkages to third parties created from the primary relationship. Enterprise policies and procedures should support user-centric identity management as well, to prevent unwanted linkages and inadvertent disclosures of personal data'.

[13] R. Warner and R. Sloan, 'Beyond Notice and Choice' n 12 above, six point out as the consent, only apparently, ensures a free and informed choice. F. Cate, 'The Failure of Fair Information Practice Principles', in J. Winn ed, *Consumer Protection in the Age of the Information Economy* (Burlington: Ashgate Publishing Company, 2006), 342, observes 'it is common for proponents of Notice and Choice to over-emphasize consent and ignore important tradeoff issues'.

identity, and dignity.

In theory, the process of collection and processing data is lawful and fair if consent is given after receiving exhaustive information and when it is expressed freely and in specific terms. The reality, however, reveals a significant divergence from the legal provisions, and very often the data subject's intentions are not truly ascertained, as users often appear disoriented and unaware when expressing their consent. These conditions undermine the safeguards underlying the rule of consent, marking its downward spiral.[14] The user's vulnerability depends on the asymmetry that arises in relation to internet service providers, principally due to a technical information deficit on the data subject's side. In effect, users frequently do not understand the terms and conditions surrounding the use of their data because they are written in unclear and incomprehensible language, or else they are difficult to find on websites, or again, users may not have a sufficient level of technological literacy.

These problems compromise the 'notice and choice' profiles in terms of both information (notice) and consent (choice).[15] With regard to this form of approval, online service providers ought to offer navigators specific information regarding the collection and processing of their personal data by publishing the terms and conditions of data use in dedicated areas of their websites. Users can refuse to allow this, for example, by changing their privacy settings. Under this scheme, known as 'opt-out', the mere publication of terms and conditions authorizes data controllers to process users' personal data, unless they explicitly deny their consent. This model is disconcerting, considering that it is often even quite difficult to understand one's rights and give informed consent in online environments due

[14] Cf S. Rodotà, 'Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali' *Rivista critica di diritto privato*, 583 (1997); G. Mirabelli, 'Le posizioni soggettive nell'elaborazione elettronica dei dati personali' *Il diritto dell'informazione e dell'informatica*, 324 (1993); S. Rodotà, 'Protezione dei dati e circolazione della informazioni' *Rivista critica di diritto privato*, 600 (1997); F.G. Viterbo, *Protezione dei dati personali e autonomia negoziale* (Napoli: Edizioni Scientifiche Italiane, 2008), 207.

[15] A. Mantelero, 'The Future Of Consumer Data Protection In The E.U.' 30(6) *Computer Law and Security Review,* 643 (2014); P. Schwartz, 'Internet Privacy and the State' *Connecticut Law Review*, 815 (2000) pointed out 'Notice and Choice does not ensure free choice because of information asymmetries, collective action problems, limited rationality, and a lack of market options'; M.J. Radin, *Boilerplate: The Fine Print, Vanishing Rights, And The Rule Of Law* (New Jersey: Princeton University Press, 2013), 19 observes 'notice and choice as implemented is inconsistent with the requirements of free choice'; H. Nissenbaum, 'A Contextual Approach to Privacy Online' *Daedalus*, 32, 36 (2011) underlined 'achieving transparency means conveying information handling practices (however) If notice…finely details every (relevant fact)… we know that it is unlikely to be understood, let alone read. But summarizing practices in the style of, say, nutrition labels is no more helpful because it drains away important details, ones that are likely to make a difference, and arguing for a much greater reliance on context'; Id, 'Privacy as contextual integrity' *Washington Law Review*, 119 (2004); J.H. Beales and T.J. Muris, 'Choice or Consequences: Protecting Privacy in Commercial Information' *University of Chicago Law Review*, 114 (2008) underlined 'the reality that decisions about information sharing are not worth thinking about for the vast majority of consumers contradicts the fundamental premise of the notice approach to privacy'.

to the opacity of privacy policies.[16]

In the notice and choice model, the 'opt-in' scheme – adopted by the current data protection regulation (eg, Recital 32 GDPR) – also creates some concern.[17] This model allows information storage or access (ie, stored on the terminal of a subscriber or user) only if the subscriber or the user have given prior consent after being presented with clear and full information. Despite the good intentions, this mechanism too shows some structural deficiencies. The technological processes regarding personal data cause them to be dispersed and place them beyond the control of the data subject. For example, browser settings are often set by default to collect data and thus include one that looks like an option to accept default cookies. This common practice clashes with the provisions of the GDPR, which require explicit consent for the automated processing of personal data (Art 9, Regulation 679/2016). The use of browser settings without changing the default option – set to accept cookies automatically – creates in fact an inability to express free, informed, aware, and unambiguous consent. It is not clear whether keeping this option is the result of informed choice or is only a sign of indifference or lack of awareness. This leads to 'inertia by default',[18] namely the passivity of users on line, which in turn leads to the 'privacy paradox'.

IV. The Privacy Paradox and Modifications to the Decision-Making Process

The 'privacy paradox' is a phenomenon that arises from the use that individuals make of communication technologies as a result of limited knowledge of their rights and freedoms in the digital era. The latest developments in the field of communication together with the massive use of social media highlight the occasional need for individuals to share personal information, with a significant tendency to self-disclosure.[19]

Although the need to share personal information causes concern among users regarding their privacy, people's behaviour online does not actually reflect this fear.[20] This dichotomy is called the 'privacy paradox'. More specifically, the paradoxical situation emerges from a divergence between thought and action.

[16] R. Warner and R. Sloan, 'Beyond Notice and Choice' n 12 above, 8.

[17] F.H. Cate and V. Mayer-Schönberger, 'Notice and consent in a world of Big Data' *International Data Privacy Law*, 67-73 (2013).

[18] D. De Lima and A. Legge, 'The European Union's approach to online behavioural advertising: Protecting individuals or restricting business?' *Computer Law and Security Review*, 67, 73 (2014).

[19] A.R. Popoli, 'Social Network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza' *Il diritto dell'informazione e dell'informatica,* 981 (2014).

[20] S. Kokolais, 'Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon' *Computer and Security*, 122 (2017) and M. Vassallo, *Achilles' paradigm and the so-called 'privacy paradox' in the era of Big Data*, *Paper for the X ESPAnet Italy Conference "The Welfare and the losers of globalization: social policies facing old and new inequalities"*, September 2017, available at tinyurl.com/y7abfd4y (last visited 7 July 2020).

When people take part in interviews and/or surveys, they appear to be very aware of privacy issues. In these situations, their answers to questionnaires show particular sensitivity towards preserving their privacy from undue invasion or maintaining constant control over information flows regarding them. At the same time, in contrast with these abstract worries, behavioural analysis reveals particular nonchalance when it comes to sharing personal information. Systemic factors, such as the graphic appearance of a website, the type of information involved, the use of default options and so on are factors that influence data subjects.[21]

At the root of this paradox, the gap between users' thoughts and actions depends on the relationship between users' cognitive inadequacy and the uncontrolled sharing of personal data in online environments.[22] Sharing personal information highlights critical aspects regarding self-regulation skills and the ability to contain one's impulses, so the emotional matrix overrides rationality. These results compromise some of the classic solutions to the problem of online privacy, such as prior, free, informed, and unambiguous consent.[23]

Behavioural science literature shows that approval for processing personal data is based on heuristics and bias, both of which condition action irrationally.[24] Thus,

> 'reaching a decision regarding processing is conditioned by an individual's general perception of his or her ability to control it at a given time (the control paradox) or the type of service to which the information applies and, broadly, the incapacity of the human mind to fully evaluate all the costs and benefits of a given action (limited rationality)'.[25]

Furthermore, giving people more information on how their data are used can, paradoxically, increase the cognitive load of the choice and cause dysfunctions

[21] G.A. Veltri and A. Ivchenko, 'The impact of different forms of cognitive scarcity on online privacy disclosure' *Computers in human behaviour*, 238-246 (2017).

[22] ibid 239. See, also, A. Acquisti et al, 'Privacy and human behavior in the age of information' *Science*, 509-514 (2015).

[23] L. Gatt et al, 'Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali' *Politica del diritto*, 339 (2017).

[24] Our innate bounded rationality limits our ability to acquire, memorize, and process all relevant information, and it makes us rely on simplified mental models, approximate strategies, and heuristics. Risk assessment is also skewed by the availability heuristic where people assess familiar dangers as riskier than unfamiliar ones. Privacy decisions are affected by cognitive biases and heuristics (eg, optimism bias, overconfidence, affect bias, fuzzy-boundary and benefit heuristics, hyperbolic discounting. Privacy decisions are affected by bounded rationality, incomplete information and information asymmetries. Cf A. Acquisti and J. Grossklags, 'Privacy and Rationality: A Survey', in K.J. Strandburg and D. Raicu eds, *Privacy and technologies of identity* (New York: Springer US, 2006), 25-26; Y.M. Baek, 'Solving the privacy paradox: a counter-argument experimental approach' *Computer and Human Behaviour*, 33-42 (2014).

[25] I.A. Caggiano, 'Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali' *Osservatorio del diritto civile e commerciale*, 94 (2018).

in relation to how they manage their privacy.[26]

On the cognitive level, there are two other conditioning factors: the abstract concept of data processing and the 'routine character' of consent. Regarding the first, abstraction is a problem of communication, as it does not enable correct understanding by users. On the other hand, in terms of the second factor, the enormous number of digital services means that there is a continuous demand for consent, which contributes to diminished attention levels among data subjects. The decision-making process thus often becomes nothing more than an instinctive behaviour in relation to specific suggestions and is not the result of informed choice.[27]

V. Datafication, Profiling, and Risks for Fundamental Rights

In the current socio-economic context, data has become a key asset in the economy of our society.[28] 'The problem with information is that it is a means by which a good meets – and most often clashes – with personal data'.[29] Potential conflict is caused not only by the economic importance of personal data but also by the influence that technology has on the phenomenon of 'datafication'.[30]

[26] B. Bergemann, 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection', in M. Hansen et al eds, *Privacy and Identity Management. The Smart Revolution* (New York City: Springer International Publishing, 2018), 111-131.

[27] E. Carolan, 'The continuing problems with online consent under the EU's emerging data protection principles' 3 *Computer Law and Security Report,* 471-472 (2016): 'there are arguably two main lessons from this brief overview of the influence of psychological characteristics on user consent online. The first is the general point that the giving of consent by an individual cannot – from a psychological perspective – be definitely regarded as a rational articulation of the individual's views. These various heuristics and biases demonstrate that decision-making is often, if not more, as much a matter of largely intuitive responses to particular prompts as it is a process of reasoned or deliberative reflection'.

[28] P. Perlingieri, 'L'informazione come bene giuridico' *Rassegna di diritto civile*, 326 (1990). On this point, cf S. Schaff, 'La nozione di informazione e la sua rilevanza giuridica' *Il diritto dell'informazione e dell'informatica,* 445 (1987); R. Pardolesi and C. Motti, 'L'informazione come bene', in G. De Nova et al eds, *Dalle* res *alle* new properties (Milano: FrancoAngeli Editore, 1991), 37; P. D'Addino Serravalle, *I nuovi beni e il processo di oggettivazione giuridica. Profili sistematici* (Napoli: Edizioni Scientifiche Italiane, 1999), 92.

[29] V. Zeno-Zencovich, 'Informazione' *Digesto delle discipline Privatistiche* (Torino: UTET giuridica, 1993), 13.

[30] B. Bates, 'Information as an economic good: a re-evaluation of theoretical approaches', in B.D. Ruben and L.A. Lievrouw eds, *Mediation, information and communication. Information and behaviour* (New Brunswick: Transaction books, 1990), 3, 379-394; P.M. Schwartz, 'Property, Privacy and Personal Data' 7 *Harvard Law Review*, 2056 (2004), according to whom 'personal information is an important currency in the new millennium. The monetary value of personal data is large and still growing'. Recently, V. Ricciuto, 'La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno' *Il diritto dell'informazione e dell'informatica*, 689 (2018). On the commercial value of personal data, see F.G. Viterbo, 'Freedom of contract and the commercial value of personal data' Contratto e impresa/Europa, 593-622 (2016), who points out 'personal data are not simply pieces of information. They refer to a particular, identified or identifiable natural person and can be capable of revealing some of the most intimate

In the area of information, the traditional proprietary paradigm (based on the *ius excludendi alios* of the owner) is considered inadequate to represent the concept of property.[31] The general process of 'functionalization' that involves this right[32] attracts personal data within its range of action.[33]

Therefore, information moves away from being a simple functional element to become part of a process of particular economic and strategic value. This change causes the gradual *patrimonialization* of personal information in commercial exchanges. From this perspective, consumer habits represent an economic resource for online operators:[34] indeed, various digital services, apparently offered free of charge, are financed by the use of personal data.[35]

In such cases, while users are surfing the web, their data can be collected in one of two ways: a) 'clear data collection', when users intentionally and actively reveal their information, and b) 'hidden data collection', when network operators store users' data without their knowledge or involvement.[36]

The former category includes data that the user voluntarily delivers to the service provider, search engines, e-mail services, websites, information sites, etc. In these cases, there is generally an exchange between the Internet service offered

and delicate aspects of that individual's personality, such as his/her state of health or sex life, for example. Their significance is not linked to the economic and quantitative criterion of marketability, but rather, to a rationale based on the protection of human rights and values'.

[31] A. Mantelero, 'Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies' *Il diritto dell'informazione e dell'informatica*, 781, 785 (2012); L. Mormile, 'Lo statuto giuridico dei dati personali', in R. Panetta ed, *Libera circolazione e protezione dei dati personali* (Milano: Giuffrè, 2006), 536.

[32] P. Perlingieri, *Introduzione alla problematica della «proprietà»* (Napoli: Edizioni Scientifiche Italiane, 1970), 65 highlights 'in forza di un'interpretazione sistematica ed unitaria dell'ordinamento, dove il dato costituzionale è parte integrante e dominante, si debba accogliere una concezione unitaria della proprietà, che non può considerarsi un diritto soggettivo tout-court, piuttosto una situazione giuridica soggettiva complessa, comprensiva di situazioni attive di vantaggio – serie di facoltà nell'interesse del proprietario – e di situazioni passive per lo stesso proprietario – cioè limiti, limitazioni, vincoli, obblighi'.

[33] F.G. Viterbo, *Freedom of contract* n 30 above, 607, according to whom 'the problem is not how to establish when a person owns personal data and when (s)he does not. The real crux of the question is establishing whether and how personal data can circulate, that is to say, whether and how they may be processed. Although not all the processing rules have the same scope of application, separating the rules governing circulation from those governing the processing of personal data does not seem possible in any case'.

[34] M. Viggiani, '«Navigazione» in Internet e acquisizione occulta dei dati' *Il diritto dell'informazione e dell'informatica*, 365 (2007) underlines 'Internet si trasforma (...) in un vero e proprio "mercato" di dati personali dalle caratteristiche però del tutto anomale perché ad una "domanda" non corrisponde una "offerta" veramente consapevole'.

[35] V. Caridi, 'La tutela dei dati personali in internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali' *Il diritto dell'informazione e dell'informatica*, 768 (2001); M. Viggiani, '«Navigazione» in internet' n 34 above, 365 observes 'nella maggior parte dei casi, l'utente non sa di stare cedendo un prodotto avente valore economico'. In the past, this evidence was pointed out by S. Rodotà, *Tecnologie e diritti* (Bologna: il Mulino, 1995), 82-83.

[36] On the lack of transparency in the 'hidden data collection', see M. Viggiani, '«Navigazione» in internet' n 34 above, 371-372.

and the personal data.[37] This exchange appears to be free of charge[38] and, even if there is no fee for the use of the service, a legal transaction takes place. In this case, consent takes the form of a counter-performance and is a legal basis for the processing of personal data. Its function is to protect the user's informational self-determination and the inviolability of his or her identity from possible intrusions and/or alterations. However, this personal data collection model is problematic.[39] The expression of consent is given unconsciously for other purposes that are not necessary for the provision of the service (for example, online behavioural advertising, web marketing, trading online).

More problematic is the case of personal information collected invisibly during navigation through 'hidden data collection'. This process uses spy programs, invisible bugs ('web bugs'), hidden identifiers and other similar devices, such as 'web cookies'. Network operators enter the users' personal devices unawares to access information and track them.[40]

While surfing the web, users leave 'digital traces'. Everyone constantly leaves behind a large amount of personal data that can be collected, processed and matched, creating new information that can be used to violate users' privacy. Some of these are intentional, visible, and potentially harmless, while others are invisible and often unintentional. Examples are traffic data, relating to the transmission of communication, static and dynamic IP addresses, the time and duration of the connection, or the websites visited. Although such information does not

[37] 'Nella prassi, (…), sempre piú spesso accade che la stessa prestazione principale è offerta gratuitamente al consumatore a condizione che questi acconsenta alla raccolta e al trattamento dei dati personali per le finalità indicate dal titolare (solitamente di profilazione o di marketing). In questi casi sembrerebbe che i dati personali conferiti siano il «corrispettivo» della prestazione offerta, in luogo della controprestazione economica non richiesta, e che il carattere necessario del trattamento rispetto alla conclusione o esecuzione del contratto (ipotesi nella quale il trattamento può essere effettuato senza il consenso) ben possa essere, oltre che di natura funzionale (in relazione alla fattispecie negoziale), anche di fonte volontaria, legato a un particolare interesse di uno dei contraenti': these remarks belong to F.G. Viterbo, *Protezione dei dati personali* n 14 above, 223-224.

[38] Cf M. Atelli, *Il Diritto alla tranquillità individuale. Dalla rete internet al «door to door»* (Napoli: Edizioni Scientifiche Italiane, 2001), 234; 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' *Il diritto dell'informazione e dell'informatica*, 1093 (2002). Counterwise, F. Astone, 'Il rapporto tra gestore e singolo utente: questioni generali' *Annali italiani del diritto d'autore*, 114 (2011); R. Caterina, 'Cyberspazio, social network e teoria generale del contratto' *AIDA*, 96 (2011) and G. Sartor, 'Social networks e responsabilità del provider' *AIDA*, 42 (2011). This dichotomy is surpassed by C. Perlingieri, *Social networks and private law* (Napoli: Edizioni Scientifiche Italiane, 2017), 61-62. On the lack of awareness of the data subject about the value of his or her data, see V. Caridi, *La tutela dei dati personali in internet* n 35 above, 768 and F.G. Viterbo, *Protezione dei dati personali* n 14 above, 201.

[39] Cf S. Patti, 'Il consenso dell'interessato al trattamento dei dati personali' *Rivista di diritto civile*, 455, 461 (1999). In the recent literature S. Thobani, *I requisiti del consenso* n 8 above. See the Italian Data Protection Authority ruling, 15 July 2010, *Raccolta di dati via Internet per finalità promozionali: sempre necessario il consenso degli interessati*, doc. web n. 1741998.

[40] M. Viggiani, '«Navigazione» in internet' n 34 above, 371.

appear to identify the user, it can reveal social habits and preferences, the websites visited, and the number of connections.[41]

The concentration of large amounts of personal data implies the relative centralization of profiling onto one or, at any rate, just a few operators. This allows the transition from an initial model focusing on individual profiling to a model of mass analysis.[42] Profiling has always been the beating heart of marketing activities, focusing on the analysis of consumers' behaviour and their psychological profiles in order to classify customers according to their interests and preferences. For example, eating habits

> 'can betray religious beliefs, the presence of certain medical conditions (the use of food not containing substances that give rise to dietry intolerance), the possible composition of the family unit (including whether the household includes animals) and, above all, spending power'.[43]

This type of information, in combination with other data, contributes to the 'hetero-construction' of identities.

Therefore, when people visit e-commerce sites, search engines, or social media, profiling or data mining processes can penetrate deeply into users' lives and to dangerous levels.[44] By subscribing to social media or using cloud computing services, users supply large amounts of personal data about their age, gender, residence, profession, and family unit that make it easy to identify and profile them. They also provide ideal conditions for discrimination and stigmatization.[45] Empowered by the extraordinary development of technological tools, data analysis and data mining are well equipped to exacerbate pre-existing discrimination or stereotypes.

Until only a few years ago, scholars were divided as to how to regulate these technologies. Some played down the damaging effect of 'hidden data collection' mechanisms. In their view, it was impossible to identify the owner of the

[41] J. Rifkin, *L'era dell'accesso*, trad. it. P. Canton (Milano: Mondadori, 2001), 131. S. Rodotà, *Una scommessa impegnativa sul terreno dei diritti*, 18 May 2001, Relation 2001; Id, *Elaboratori elettronici e controllo sociale* (Bologna: il Mulino, 1973).

[42] A. Mantelero, 'Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo' *Il diritto dell'informazione e dell'informatica*, 135 (2012).

[43] R. De Meo, 'Autodeterminazione e consenso nella profilazione dei dati personali' *Il diritto dell'informazione e dell'informatica*, 588 (2013).

[44] A. Mantelero, 'Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies' *Il diritto dell'informazione e dell'informatica,* 781 (2012).

[45] Case 524/06, *Huber* v *Bundesrepublik Deutschland*, Judgment of 16 December 2008, available at www.eur-lex.europa.eu; Case 236/09, *Test-Achats et al* v *Conseils des Ministres*, Judgment of 1 March 2011, available at www.eur-lex.europa.eu. On this point, see the significant considerations by P. Femia, *Interessi e conflitti culturali nell'autonomia privata e nella responsabilità civile* (Napoli: Edizioni Scientifiche Italiane, 1996), 540, fn 843, points out 'la decisione di aggregare individui per una loro caratteristica rilevante deve essere controllata, come giudizio di valore, nella sua congruenza con l'intreccio di valori costituzionali richiamati nella fattispecie'.

information as the data are anonymous.[46] However, in only a short space of time, thanks to the evolution of technology, apparently neutral data – such as dynamic IP addresses – can now be linked to the user, adding them to other information.[47]

The most recent approach supersedes both of the above positions in accordance with European case law and the rulings of the Italian Data Protection Authority.[48] Firstly, all the information – IP addresses, traffic data, navigation data and others – is classified as personal data from which it is possible to draw a precise personal profile detailing habits and preferences using algorithmic technologies. Secondly, the potential identifiability of the user is a sufficient condition to put protective measures such as notice, consent, prohibition of transfer to third parties, the right to access, and the right to portability in place.[49]

On the legal front, Art 22 of the GDPR requires the explicit consent of the user for automated data processing (including profiling) to be considered lawful. In this way, Art 122 of the Italian Privacy Code requires express consent from users before information-gathering programs are installed on their devices. So, for consent to be 'express', data controllers must provide clear and complete information on profiling to ensure that users understand what they are consenting to; thus, they must provide for a 'granular consent' (also called 'stratified consent') where users can give their approval in a simple and intelligible form. They must actively seek the user's consent before any new and further processing, and finally, they must inform the data subject that they may revoke their consent at any time.[50]

In brief, even if profiling and segmentation help companies gain a better understanding of their customers' characteristics and communicate with them more effectively, it is lawful only in direct relation to the exact knowledge – in terms of transparency – and to

[46] G. Ciacci, 'La tutela dei dati personali su Internet', in A. Loiodice and G. Santaniello eds, *La tutela della riservatezza*, *Trattato di diritto amministrativo* (Padova: CEDAM, 2000), 380.

[47] Case 582/14, *Patrick Breyer* v *Bundesrepublik Deutschland*, Judgment 19 October 2016, with commentary of A. Vivarelli, 'Privacy digitale e Corte di Giustizia' *Il Foro Napoletano*, 797 (2017).

[48] See, for all, the following Italian Data Protection rulings: 15 March 2012, Arricchimento dei dati personali della clientela nell'ambito dell'attività di profilazione (doc. web 1903026); 7 November 2013, Conservazione dei dati personali riguardanti la clientela per attività di profilazione e marketing. Verifica preliminare richiesta da Tod's S.p.A. (doc. web n. 2920245); 17 dicembre 2015, Verifica preliminare. Trattamenti di dati personali aggregati della clientela nell'ambito di una piú complessa ed articolata attività di profilazione (doc. web 4698620); 11 May 2017, Verifica preliminare. Trattamento dei dati personali riguardanti la clientela per attività di profilazione e promozionali (doc.web n. 6495144); 5 July 2017, Verifica preliminare. Trattamento di dati personali riferiti alla clientela per finalità di profilazione e promozionale (doc. web n. 6844421).

[49] M. Viggiani, '«Navigazione» in internet' n 34 above, 387.

[50] See *Guidelines on Consent under Regulation 2016/679* of the Working Group Art 29, 28 November 2017: 'if the controller has conflated several purposes for processing and has not attempted to seek separate consent for each purpose, there is a lack of freedom. This granularity is closely related to the need of consent to be specific (…). When data processing is done in pursuit of several purposes, the solution to comply with the conditions for valid consent lies in granularity, i.e. the separation of these purposes and obtaining consent for each purpose'. Cf recitals 43 e 32 GDPR.

> 'the "profiling" intention of the person who collects the data and clearly declares the purposes that s/he intends to pursue through profiling'.[51]

Making decisions based on sophisticated profiling activities, often without human involvement, risks leading to the extreme consequence of inhibiting the exercise of fundamental freedoms or limiting the provision of essential services. Full knowledge, freedom and specificity of consent are fundamental rules to which profiling practices must be subordinated. The protection of personal identity and privacy means that people are not 'built' by others, because the development of the human person presupposes not only the recognition of the '*habeas corpus*' but also of the '*habeas data*'.[52]

VI. Big Data Analytics and the 'Transformative Use' of Personal Data

Big Data analytics represents the latest challenge to personal data protection. The propulsive force of modern technologies, artificial intelligence, and algorithms finds in Big Data a unique expressive ability that is difficult to understand through the lens of human capabilities. Indeed it represents

> 'sets of data whose size is not compatible with the capacity for collection, management, archiving and analysis of the software commonly used to manage the databases'.[53]

Big Data means huge amounts of data held by companies, governments or other organizations, to be examined using powerful algorithms in order to

> 'extrapolate new indications or create new forms of value in ways that change markets, organizations and relationships between citizens and governments, and more'.[54]

Big Data consists of high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.[55]

The large scale of Big Data collection and analysis operations corresponds to the limited number of players evaluating them.[56] For some operators, the

[51] R. Di Meo, 'Autodeterminazione e consenso nella profilazione di dati personali' *Il diritto dell'informazione e dell'informatica*, 593 (2013).

[52] M. Viggiani, '«Navigazione» in internet' n 34 above, 356-357.

[53] N. Lettieri and M. Faro, 'Big Data e Internet delle cose: opportunità, rischi e nuove esigenze di tutela per gli utenti della Rete', in C. Perlingieri and L. Ruggeri eds, *Internet e Diritto Civile* (Napoli: Edizioni Scientifiche Italiane, 2015), 282.

[54] V. Mayer-Schoenberger and K. Cukier, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere – e già minaccia la nostra libertà* (Milano: Garzanti Editore, 2013), 17.

[55] Gartner IT glossary.

[56] A. Mantelero, 'Big Data: i rischi della concentrazione del potere informativo digitale e

concentration of this immense amount of information is not new, but their scale and the global nature of the growing phenomenon generate concerns over their impact on people's rights and freedoms.[57]

Moreover, predictive analysis capability and data inferences mean that the power of Big Data analytics is entirely different from mere profiling or data mining. Consequently, the transition from a static to a dynamic view of personal data shifts the focus from the collection and storage phases to those where a deep and obscure analysis of data takes place, culminating in the so-called 'transformative use' of personal data.[58] This shift means that the data are not used quantitatively but qualitatively. In effect, these processes make it possible to extract new knowledge, to identify personal profiles, and to make predictive hypotheses from the data.

While Big Data analytics now makes projects of the utmost importance possible, its impact on privacy and personal identity is, at the same time, highly dangerous.[59] First of all, the traditional distinction between personal and non-personal data disappears, because analysis, inferences, and neutral information combinations can point to the user's identity as well as to his or her personal and sensitive data. Thanks to 'granularity', the value of the data no longer lies simply in the purpose for which they were originally collected but in the multiplicity of other potential uses later on. This is, in effet, one of the peculiarities of the new digital landscape: data mining and data analysis techniques make it possible to obtain a multiplicity of data from a single piece of information.[60]

The use of Big Data Analytics contrasts with some of the fundamental principles of the European legal framework on the protection of personal data, such as the principles of purpose limitation and informed and unambiguous consent. In fact, according to European and national law,[61] data must be collected for specific, explicit and legitimate purposes and then processed in a compatible way. Conversely, the ontological nature of Big Data analytics clashes with this legal provision because the analysis leads to results produced from obscure and

gli strumenti di controllo' *Il diritto dell'informazione e dell'informatica*, 135-136 (2012).

[57] A.C. Nazzaro, 'L'utilizzo dei Big Data e i problemi di tutela della persona' *Rassegna di diritto civile,* 1261 (2018); Id, 'Privacy e Big Data' *Le corti fiorentine,* 13-25 (2018).

[58] On the 'transformative use' of Big Data see O. Tene and J. Polonetsky, 'Privacy in the Age of Big Data: A Time for Big Decisions' *Stanford Law Review Online,* 64 (2012) according to whose 'the uses of big data can be transformative, and the possible uses of the data can be difficult to anticipate at the time of initial collection'; in the Italian scholarship, see di G. d'Ippolito, 'Il principio di limitazione della finalità del trattamento tra data protection e antitrust. Il caso dell'uso secondario di big data' *Il diritto dell'informazione e dell'informatica,* 943 (2018).

[59] I. Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' *International Data Privacy Law*, 74-87 (2013).

[60] D. Messina, 'Online platforms, profiling, and artificial intelligence: new challenges for the GDPR and, in particular, for the informed and unambiguous data subject's consent' *Media Laws*, 159, 170 (2019).

[61] Convention no 108, Art 9 and Directive 95/46/CE Art 6, lett b). Working Group Art 29, on the *Opinion on purpose limitation*, 2 aprile 2003, no 3. Cf G. d'Ippolito, 'Il principio di limitazione della finalità del trattamento' n 58 above, 943.

unexpected inferences and connections. It is therefore impossible for users to know the precise purposes to which the processing will be be put from the moment the data are collected.

The 'transformative use' of Big Data analytics leads to a result that differentiates itself from individual data. This process is summarized in Aristotle's principle: 'the whole is greater than the sum of its parts'.[62] This is a critical issue and impinges on freely given, informed, and unambiguous consent. In fact, the difficulty of understanding the results of Big Data analytics implies that information regarding the purposes of the processing is vague and generic or may not even exist; the impact of their results on peoples' rights and freedoms is unexpected.

In conclusion, Big Data analytics techniques lead to risks for people, such as misuse of data, monitoring, or stalking.[63] In the worst case scenario, these risky operations may lead to erroneous conclusions about a person who becomes the product of an automated decision where human evaluation is ruled out altogether.[64]

VII. The GDPR's Privacy by Design Solution: Is It Enough?

The GDPR solution to the consent crisis is the gradual empowerment of the data subjects' decision-making process through a user-centred approach. This new paradigm allows

> 'a more correct and modern way of incorporating personal data protection into IT products. This is because in the development of such products, the possibilities of choice regarding online privacy would be made more accessible and comprehensible, also paying attention (...) to those social dynamics that lead to a voluntary and sometimes irresponsible sharing of information on the Internet, characterized by the fact that the information is shared by the user himself in the unfaithful replication of the same social relations that characterize life outside the Internet'.[65]

From the perspective of a 'shared web', privacy-by-design tools (provided for under Art 25 GDPR) enhance the 'front-end moment' of protection, when the user interfaces with the service offered.[66] These tools promote the so-called

[62] V. Mayer-Schönberger and K. Cukier, *Big Data* n 54 above, 108 observe 'the sum is more valuable than its parts, and when we recombine the sums of multiple datasets together, that sum too is worth more than its individual ingredients'.

[63] N. Lettieri and M. Faro, 'Big Data e Internet delle cose' n 53 above, 299-300.

[64] On the algorithm tyranny, see for all S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli* (Roma-Bari: Edizioni Laterza, 2014), 38.

[65] A. Principato, 'Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings' *Contratto e impresa/Europa*, 199, 209 (2015).

[66] See I.A. Rubisten, 'Privacy by design: a conterfactual analysis of Google and Facebook

'user-experience design' and take their cue from the development of web architecture.[67] Thus, interaction between users and the computer system needs to be user-friendly for better and safer Internet navigation. This model promotes user empowerment, making informational flows more transparent in addition to increasing users' awareness and ability to control what they share and in which contexts.[68]

It is a solution that satisfies the regulatory provisions of the GDPR, which moves the protection forward to system design level (in line with privacy by design and privacy by default criteria) and, at the same time, emphasizes the precautionary element. From this perspective, users can set privacy settings designed and implemented with the aim of a conscious approch to the management of their personal data in mind.[69]

Furthermore, the solution safeguards consent and self-determination. Indeed,

> 'if – in theory – the so-called technical standards for system design or architectural configuration appear neutral, they lose this characteristic when they become the logical structure of personal interconnections'.[70]

Ensuring the expression of consent and its implementation in the architectural structures of websites means not disrupting the functional relationship between the person and his or her informational flows on the one hand and his or her virtual and social projection on the other. It follows, therefore, that the total denial of consent entails a human being giving up his or her right to informational self-determination and dynamic identity.

Consequently, when data processing is under the control of the data subject, who is able to control personal data, this protection paradigm loses its sole purpose and becomes a private self-protection device. According to this hypothesis, consent implemented in architectural configuration is a mechanism of self-defence and has a precautionary and inhibitory function.

Including consent in privacy-by-design structures is a projection of personal

privacy incidents' *Berkeley Technology Law Journal*, 1333 (2003).

[67] See the *Opinion 9/2016 European Data Protection Supervisor* (EDPS), in which the new concept of a 'personal information management system' ('PIMS') creates a paradigm shift in personal data management and processing, with social and economic consequences. The core idea behind the PIMS concept is to create a new digital ecosystem where individuals can manage and control their on line identity, transforming the current provider-centric system into a human-centric system where individuals are able to manage their on line identity and are protected against unlawful processing of their data. PIMS can be considered intermediaries within the online market.

[68] Cf H.V. Lipford, 'Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites' *International Conference on Computational Science and Engineering* (2009), available at tinyurl.com/yd3947oy (last visited 7 July 2020).

[69] See L. Belli et al, 'Selling your soul while negotiating the conditions: from notice and consent to data control by design' *Health Technology*, 459 (2017).

[70] C. Perlingieri, 'La tutela dei minori di età nei social networks' *Rassegna di diritto civile*, 1330-1331 (2016); Id, *Profili civilistici dei social networks* n 38 above, 23.

autonomy for the realization of interests worthy of protection and is in line with the principles of transparency and lawfulness.[71] Autonomy is thus conceived as a functional aspect of self-protection, serving above all to set up tools for the protection and preventive defence of legally significant interests. The data subject exercises his or her power of self-protection to safeguard a certain legal asset, which is the set of his or her existential situations: dynamic identity, privacy, and intimacy.[72]

VIII. Final Remarks

The user-centred approach shows that, despite an awareness of the crisis of consent, the human person cannot be deprived of the ability to make his or her own decisions in terms of informational power. Users cannot be abandoned to the autocratic power of private powers or public institutions. The centrality of human persons, their free development, and their fundamental rights must be guaranteed at all times.

> 'Right now that processing of personal data are becoming more complex and obscure, with the risk of excluding from the decision-making process the majority of those concerned in favour of technological elites holding power over the data, it is necessary to reaffirm the central role of individuals'.[73]

In any case, as mentioned above, the question of consent presents several critical issues. The downward spiral towards 'informational hetero-determination',[74] the failure of the 'notice and choice' paradigm, and the spread of the 'privacy paradox' are all problematic aspects in the data protection scenario, especially for people's fundamental rights and freedoms. For these reasons, a fair compromise is one that can ensure the self-determination of the human person – incorporating consent in website architectures – but, at the same time, one that will make users aware of the insufficiency of this principle in all types of processing, including the uncertainty of transparency.

From this standpoint, privacy-by-design models are not enough to offer

[71] N. Bobbio, 'Sulla funzione promozionale del diritto' *Rivista trimestrale di diritto e procedura civile*, 1313 (1969).

[72] See A. Dagnino, *Contributo allo studio dell'autotutela private* (Milano: Giuffrè, 1983), 65-66.

[73] See A. Mantelero, 'Responsabilità e rischio nel Regolamento 679/2016' *Nuove leggi civili commentate*, 147, 149 (2017), according to whom 'the question of how to advance the development of digital services, particularly considering the rise of the Internet' of Things and of Big Data analytics, without compromising individual freedoms, privacy, and autonomy has spurred a movement toward a new kind of data control that empowers individuals. See L. Belli et al, 'Selling your soul while negotiating the conditions: from notice and consent to data control by design' *Health Technology*, 459 (2017).

[74] F.G. Viterbo, *Protezione dei dati personali e autonomia negoziale* n 14 above, 215.

protection on their own, so architectural web design[75] should be able to influence users' behaviour.[76] Data Protection Authority control thus becomes a necessity, hand in hand with that of the Courts, to verify whether a given web architecture (ie, check-boxes) makes the act of giving consent user friendly or whether the font and the positioning of the information appear 'intelligible'.[77]

The obscurity of the current inferential and algorithmic processes relating to personal data is an issue that cannot be solved by simply guaranteeing informed and preventive consent. However, making users aware of how their personal data serves the market's interests is important for the preservation of their right to informational self-determination. From this perspective, self-determination (consent implemented in privacy-by-design paradigms) together with the profiles of control and compliance must be combined with the principles and values of the legal framework (the Data Protection Authority and Courts) in order to promote a critical review process for algorithms and transparency in the way they work.[78]

[75] A.E. Waldman, 'Privacy, Notice and Design' *Stanford Technological Law Review*, 134 (2018) underlines 'policy design can manipulate users into handing over personal information, policy design requirements, including mandating a notice designed specifically to convey information to ordinary users, should be included in state and federal statutes that mandate privacy policies. The FTC should also investigate internet companies that design their privacy policies to deceive users. With respect to the practical implementation of notice and choice, this research recommends several strategies for online platforms, including increasing collaboration between privacy counsel and technologists and committing to embedding privacy protection into the corporate ethos'.

[76] ibid 155.

[77] See *Guidelines on transparency under Regulation 2016/679*, available at tinyurl.com/ydz52dmk (last visited 7 July 2020).

[78] E. Giorgini, 'Algorithms and Law' *The Italian Law Journal*, 131 (2019). See, also, P. Perlingieri, 'Privacy digitale e protezione dei dati personali tra persona e mercato' *Il Foro napoletano*, 481 (2018).