A Quest for Efficacy in Data Protection:

a Legal and Behavioural Analysis

Ilaria Amelia Caggiano

Prof. Associato di Diritto Privato

Università degli Studi Suor Orsola Benincasa

Working Paper

10/2017

WORKING PAPERS
JEAN MONNET CHAIR
EUROPEAN PRIVATE LAW

Universitat de Barcelona

Abstract: The article questions the role of consent to the processing of personal data, especially in the technological context, as a tool of self-determination or protection of the data subject. The work draws on some results from behavioural studies and some Italian judgements regarding other private actions in data protection law (liability for damages). Some suggestions towards an alternative scenario are finally suggested.

Title: A quest for efficacy in data protection: a legal and behavioural analysis

Keywords: Protection of personal data, information society, Big Data, consent to personal data processing, liability for damages

***Resumen**: El artículo cuestiona el rol del consentimiento en el tratamiento de datos personales, particularmente en el contexto tecnológico como herramienta de la autodeterminación o protección del interesado. Este trabajo analiza algunas conclusiones de estudios comportamentales y determinadas resoluciones judiciales del ordenamiento italiano respecto del ejercicio de acciones privadas en el derecho de protección de datos (responsabilidad por daños). Finalmente se exponen algunas recomendaciones de un escenario alternativo*

***Título**: Una búsqueda de la eficacia en la protección de datos: un análisis jurídico y conductual*

***Palabras clave**: Protección de datos personales, sociedad de la información, Big Data, consentimiento al tratamiento de datos, responsabilidad por daños*

Index

1. The protection of personal data in the information society and in the context of big data. The scope of the paper

The exponential development of technology has led to profound changes in social relations and in law.

One of the unifying aspects of our time is the centrality and spreading of information, which is now in itself a consumed and exchanged good. In the technological era, information is massively collected and quickly transmitted through the Internet. Through this new mode of communication, marketable information is gathered from users of the internet by bots with no regard for people as such: personal data as discussed in this paper being a fragment of information related to natural persons.

It is clear that the flow of information pertaining to individuals has modified social habits, freedoms and rights[1]. A new autonomous right to personal data has been vested in natural persons, as independent from the right to personal identity or their privacy as the right to be left alone[2]. But, the situation is still evolving[3].

Digital data can be aggregated from a vast constellation of sources (databases, search engines, virtual stores, e-mail, social networks, cloud-storage services, things in the Internet of Things[4]). Once processed, they are able to profile individuals, global society, or any large community. This is the world of big data: datasets which, by volume, speed and variety, allow the extraction of additional information so as to determine business models, markets or scientific uses of this digital knowledge[5]. Personal data,

[1] Rodotà, *Tecnologie e diritti*, Bologna (Il Mulino), 1995; Id., *Intervista su Privacy e libertà*, a cura di P. Conti, Bari (Laterza), 2005. Parlano, efficacemente, di sistema "dato-centrico" Montelero, *The Future of Consumer Data Protection in the E.U. Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics* (2014) 30 (6) *Computer Law & Security Rev.* 643 ff. ; O. Pollicino, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. info*., 2014, p. 569 ss.

[2] The idea that the individual not only has the right to a living space that cannot be invaded by third parties (Article 7 of the Charter of Fundamental Rights of the EU), but that he has the right to "govern", or at least have access to, Every fragment of identity that is held by third parties interprets the formalization of the individual's interest in not exposing one's own person to the invasion of his or her sphere by third parties.

[3] Lucidly identifies the link between the different phases of technological development and the content of the personal data protection regulation MONTELERO, The Future of Consumer Data Protection cit.

[4] On the IOT, preliminarily, PAGANINI, *Verso l'Internet delle cose*, in Dir. Ind., 2015, p. 107 ff.

[5] Value extraction in big data takes place through analytical methods of data mining (algorithms). Analytics are data tracking tools: software that lets you find correlation between data, analyse historical series, determine trends and seasonal behaviours, simulate economic scenarios, segment customers, and conduct data and text mining activities to better understand a wide range of phenomena Of business. These are tools that enable private and public decision-makers to make better decisions. Providing budget indicators based on historical series, understanding customers and employees' behavior in advance, assessing the degree of risk of funding, are some practical examples of analytics use. On the subject, see: R. MORO VISCONTI, Evaluation of the Big Data and Impact on Innovation and Digital Branding, in Industrial Law, 2016, p. 46 ss.

which is available to public and private entities, is most effectively processed by those companies with the most extensive databases, which are in a dominant or approaching monopolistic position. The massive amount of data allows for an increasingly pervasive profiling of individuals, through the history of their activities, their preferences, interactions, lifestyles, in order to: propose targeted products or advertisements (commercial purposes); predictively monitor larger social groups; and correlate the most disparate information with great accuracy[6].

The collection of personal data is realized in various ways: by professionals, at the conclusion of a contract for further use, namely for selling the data to third parties; by social networks, where content users voluntarily share their personal information and deliberately express their social identity (data about their images, tastes, through the social display of appreciation or sharing); and by search engines[7].

The circulation of data, through the sale to third parties (also for advertising purposes), is a source of profit for the professional data controller[8]. Thus, the personal interests of the user function as negotiable intangible assets[9] are not only a matter of fundamental rights and freedoms, but because of their economic value, a matter of patrimonial rights.

The brief scenario above described allows for reflection on the reasons and efficacy of the right to the protection of personal data, with particular regard to the recent European legislative act (Regulation (UE) 2016/679).

---

[6] Google was able to predict the influenza in real time and 2 weeks before government institutions. On this point, BOGNI - DEFANT, *Big data: diritti IP e problemi della privacy*, in *Politica industriale*, 2015, p. 117 ff.

[7] PIPOLI, *Social Network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Dir. info*, 2014, p. 981 ff. Where the following text (nt. 40) states that "with the pressure of appreciation and sharing keys, data on racial or ethnic origin, religious, philosophical or other beliefs can be communicated to political opinions, [...] As well as data suitable for revealing the state of health and sex life, that is, sensitive data ...." (*our translation*) In the Declarations of Rights and Responsibilities of Facebook it reads that «the user grants to Facebook a non-exclusive, transferable license, which may be granted as royalty, free of charge and valid worldwide, for the use of any content IP published on Facebook or in connection with Facebook ».

[8] "The collection, analysis, and conversion of all relevant user data (including sensitive data), including through the license, fall within the User Data Profiling activity. [...] in order to generate segmentation of their users into homogeneous behavioural groups [...] to make Behavioural Advertising [...] in social networks are the users themselves to build a profile of them, which will be used for their own profiling" (*our translation*) PIPOLI, *Social Network*, cit. text up to nt. 84. In that regard, Facebook's social networking information clarifies how the so-called data use license is only used for editorial advertising purposes and not for sale to third parties. Though, in another place, it expressly says "We do not share your personal information (personal information includes name or email address that you can use to contact or identify you) with advertising, measurement or analysis partners, unless You do not grant us permission".

[9] One need only mention the fact that Google, which has become the world's second-largest value-for-money company - with $ 522 billion in capitalization, just under $ 587 billion, with sales growing in the first quarter of 2016. (fonte: www.corriere.it; http://www.corriere.it/economia/finanza_e_risparmio/16_aprile_26/wall-street-sorride-solo-gigante-google-2a13ebae-0b8f-11e6-a8d3-4c904844517f.shtml)

The level of analysis is threefold:

1. On the one hand, one must verify whether the current regulatory measures are functional to the intended objectives of protection (of fundamental rights)[10] (section 2). The next section 3 will focus on consent as a legal basis for the processing of personal data and as a doubtful tool to protect personal data, in terms of efficacy;

2. Section 4 shows some preliminary result of an experiment conducted at the University Suor Orsola Benincasa of Naples (IT) to verify the efficacy of consent to the processing of personal data;

3. Taking into account the outcome of the first two levels of analysis, the paper considers different protection mechanisms other than current ones, also taking into account some difficulties in compensation as a remedy for the protection of the right to personal data, provided by law.

2. Consent as a legitimate basis for the processing of personal data and Reg. (EU) 2016/679

As a consequence of the rapid technological developments, a new regulation on Data Protection has been recently enacted at a European level with the purpose of creating a stronger data protection framework in the Union as well as developing the digital economy and the internal market of personal data (rec. 7). According to the new Reg. (EU) 2016/679 (also called General Data Protection Regulation, GDPR) the data subject's consent to the processing of his/her personal data still plays a fundamental role as a prerequisite for the processing of personal data. Regulation 2016/679 modifies the basic system of rules about the processing of personal data, namely Directive 95/46 / EC (the so-called "mother directive"), with regard to organizational and entrepreneurial models, responsibilities of controllers and processors, thus shifting the risk of the activities carried out to them. This is the "accountability" model where the burden of proving compliance with law and no risk of data breach falls to the gatherer of data (rec. 86, article 5) .

However, the new act upholds the legitimate bases for this process.

[10] This first phase involves, in particular, the analysis of some of the results that draw on psycho-behavioural sciences with particular regard to the attitude of individuals regarding the demonstration of consent to the processing of personal data. In general on behavioural studies in legal doctrine, among others ARNAUDO, *Diritto cognitive. Prolegomeni per una ricerca,* in *Politica dir.* , 2010, p. 101 ff. ; LURGER, *Empiricism and Private Law: Behavioural Research as Part of a Legal-Empirical Governance Analysis and a Form of New Legal Realism*, in *Aust. Law Jour*. 2014, p. 19 ff.

Under the Regulation, controllers are required to bear the risk of processing by adopting a series of *ex ante* measures. Think of the data protection Impact Assessment (rec. 84), in case of a high risk to rights and freedoms for individuals; the design of systems and applications aimed at minimizing the use of personal data (so called *Privacy by design and by default* - Article 25), the technical and organizational measures to minimize the risk of personal data (such as pseudonymization); the mandatory appointment, in some cases, of a new figure, the Data Protection Officer (Article 37, p. 97), a manager in a third party position (at least, in principle) with the task of advising the manager / holder in order to ensure proper management of personal data in companies and bodies and act as contact point with Authorities. Such measures are accompanied by: the assertion of rights to natural persons (to erasure – to be forgotten, to data portability - Article 20); a uniform regulation within the European Union's data processing market[11], guaranteed by a European authority, the European Data Protection Board (Article 68); the limitation of the circulation of data outside Europe, on the basis of the conformity assessment of guaranteed measures for data transferred outside the EU.

The above-mentioned regulatory choices reveal an approach which favours the technological production of massive amounts of data, techniques which allow multiplication of the data, and regulate processing, minimize the risks of loss, dispersal, dissemination, for the purpose of protecting the data subjects. Technology (privacy by design, through anonymisation and pseudoanonymization) is called upon to regulate technology (since processing is now almost automated) according to the objectives set by the legislator, while legal rules gain their own important space as *ex post* measures.

As already said, in this context, consent is one of the "legitimate basis" (according to the terminology common to the Nice Charter) to initiate the processing of personal data[12]. With respect to personal data in general, consent is a condition of lawfulness

[11] Regarding the territorial scope of the legislation (Articles 3 to 5): no reference is made to the location of the terminal in the Member State but to the provision of services in EU states, so that the new framework applies in full to the undertakings located Outside the European Union offering services or products to persons located in the territory of the European Union

[12] Thus, it is confirmed that a wide area of data processing remains under the rules of consensus. Consent continues to represent only a legitimate basis for processing, required where it is not necessary for the performance of a contract or the pre-contractual stage, for the fulfillment of a legal obligation for the holder to safeguard vital interests, For the pursuit of a public interest or the exercise of public authority for the pursuit of a legitimate interest of the holder or a third party provided that they are not in conflict with the rights of the party concerned (Article 7 of the GDPR). A significant opening in the market, in this regard, is the possibility that the processing of personal data for direct marketing purposes is considered to be pursued by a legitimate interest of the data controller or third parties (cons. 47). As for the particular categories of data, further specific derogations are also foreseen in this case, with respect to the consensus (Article 9 GDPR). On the different structure of the legality conditions in the privacy code and in the Regulations (and in Directive 95/46 / EC), L. L. BOLOGNINI, E. PELINO,

under Article 6), and with regard to particular categories of data (sensitive data), it excludes the prohibition of processing (Article 9)[13].

Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". In the new legal terminology, consent must be an affirmative / positive (but not necessarily written) action (see Article 4, paragraph 1, n.11) Reg. 2016/679)[14]. Also when electronic means are used a positive acceptance action is required. In this regard, one should not only consider the use of digital instruments but, inevitably, the already widespread diffusion of sensors (e.g. motion detection software, touch sensing, etc.).

Consent must be explicit only with regard to sensitive data (Article 9 GDPR and Article 8 (2) (a) "mother directive"). Explicit consent is also required for the purposes of profiling (Article 22 GDPR) and in the case of transfer to a third country or an international organization (Article 49 (1) (a)). Explicit consent can be understood as consent to be clearly manifested. This is a further qualification, different from the affirmative consent (that is, not tacitly expressed), laid down as a general rule by the European legislator (rec. 32)[15].

Transparent disclosure of any information or communication relating to the processing is provided as mandatory (rec. 39, art. 12). Consent, according to a pattern that recalls neoformalism in contract theories, cannot be obtained in the absence of a number of mandatory pieces of information provided to the data subject. However, information must be provided to the data subject even when it is not fundamental to a subsequent manifestation of will.

Condizioni di liceità, in L. BOLOGNINI, E. PELINO, C. BISTOLFI, *op. Cit*., p. 278, but it does not lead to appreciable consequences on.

[13] In maintaining the information mechanism + consent, the need for prior and unambiguous (explicit for sensitive data) and on request (as in the consumer case are excluded from the pre-ticked boxes) is confirmed, favored by the presence of icons (identical In the EU), also with regard to the transfer of non-EU data and the existence of a revocation right (see paras 32-38, §§ 6 -8). The right to data protection as self-determination (such as control over collection, dissemination, processing of correctness and data removal) already in the pre-regulation system, G. SARTOR, *Privacy, reputazione, affidamento: dialettica e implicazioni per il trattamento dei dati personali,* in AA. VV., *Privacy digitale. Giuristi e informatici a confronto*, Torino (Giappichelli), 2005, p. 81 ff.

[14] Recital 32, «any other conduct which clearly indicates in this context that the data subject accepts the proposed processing . Therefore, withholding of information, inactivity or preselection should be allowed. [...] If the consent of the data subject is required by electronic means, the request must be clear, concise and not interfere immutably with the service for which the consensus Is expressed.»

[15] Art. 23 Italian Privacy code: «Consent is valid only if it is expressly and specifically disclosed in relation to a clearly identified processing, if it is documented in writing, and if the information referred to in art. 13 »

3. Critics on the relevance of informed consent for protecting personal data

The consent of the data subject with regard to the processing of his/her personal data has a relevant position in the overall processing, according to the right to data protection (*privacy*) as a fundamental right in the European Union.

However, it is arguable that the informed consent-based regulatory approach is somewhat ineffective. Terms of Services or Privacy Policy Terms and Conditions are normally not read.

The problem of "empty ceremony"[16], which accompanies the subscription of any pre-arranged form, is emphasized in relation to the informed consent to processing of personal data, where the protection of personal data is perceived by the party as extraneous to the economic operation he or she is interested in at that point. «Users are formally called to make decisions concerning the disclosure of their personal information on the basis of a difficult trade-off between data protection and the advantages stemming from data sharing (eg. interacting with smart-transport or a health-care system)»[17].

It can be argued that in the case of data protection, disclosure can play a role different from that of addressing information asymmetries. Yet, it allows the data subject to initiate the control of processing[18]. However, it is arguable that as for asymmetry, so for the controlling function, the information provided is not capable of clearly signposting awareness of the individual's will.

In this regard, a broad literature on behavioural studies shows how data protection decisions completely prescind from the rational choice paradigm and that, in any case, data subjects are also willing to exchange their data for a minimal benefit or reward[19]. This tends to happen also in situations where they have previously stated that they want a high degree of protection for their data. Empirical evidence then demonstrates

[16] S. PATTI, *Consenso*, sub *art. 23)*, in AA. VV. *La protezione dei dati personali. Commentario* a cura di C.M. Bianca – F. D. Busnelli, t. I, Padova (Cedam), 2007, p. 541 ss.

[17] G. COMANDÈ, *Tortious privacy 3.0: a quest for resarch*, in in *Essays in Honour of Huldigingsbundel vir Johann Neethling*, LexisNexis, 2015, 121 ff. , 122

[18] MAZZAMUTO *Il principio del consenso e il potere della revoca* cit. at 1004.

[19] STRAHILEVITZ, *Toward a Positive Theory of Privacy Law*, 113 *Harv. Law Rev*. (1999) 1; SOLOVE, *Privacy self-management and the Consent Dilemma* 126 *Harv. Law Rev.* (2013) 1880; BORGESIUS, *Informed consent: We Can Do Better to Defend Privacy*, *IEE, 2015 (Vol. 13, p. 103 - 107)* – recommended cit.; ID. *Behavioural Sciences and the Regulation of Privacy on the Internet, Amsterd. Law School Research Paper no*. 2014 – 54; ACQUISTI, *Privacy*, in *Riv. pol. Econ*., 2005, p. 319; BAROCAS – NISEMBAUM, *On Notice: the Trouble with Notice and Consent*, *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, October 2009. Available at SSRN: https://ssrn.com/abstract=256740; BENSHAHAR – CHILTON, *Simplification of Privacy Disclosure: An Experimental Test 2015* 45 *Journ. Legal Studies* (S2):S41-S67 (2015).

how, given a confused perception of the meaning and scope of data protection in social conscience, consent to the processing of personal data is formed by heuristics or other cognitive shortcuts that are totally detached from the world of informed and conscientious consent, which presupposes behaviour inspired by rationality[20].

It is doubtful then that consent can be a mechanism that has any function in protecting individuals' right to personal information. These considerations require some attention by the legal actors and the legislator (!), who should finally acknowledge it[21].

As anticipated, the consent of the data subject, where required, is only the foundation of a much more articulated procedure, which allows the data subject to control the controller's activity. It could be assumed, then, that the consent, as a seal to the information provided, can at least recall the attention of the actors involved (controller, processor) to the processing. However, even as far as this aim is concerned, it is not clear how by providing information on his/her own duties, one can be compelled to obey such duties.

Assuming – as it is – that these considerations are somehow known, what is the legislators (and other regulators)' attitude?

For example, the Italian Data Protection Authority decisions and guidelines stress the promotion of a better disclosure, multi-layered information etc. as it has been recently requested to a non-EU business (Google case)[22]. However, it is questionable whether even ameliorated information can really be capable of affecting the users' awareness, as evidenced by recent studies dealing with Google's own information[23].

[20] S. PATTI, *Consenso*, cited above. In a legal perspective, if one considers irrationality of common cognitive perception in order to invalidate the consensus, this would result in all consents being spoiled. Without coming to accept such eccentric prospects, which would also be a serious problem of coordination with the system of legal acts, the analysis here provided seems to demonstrate, however, the ineffectiveness of the law with respect to the interest intended to be protected.

[21] G. COMANDÈ, *op. cit.*, p. 123 unveils the mask of EU recognition of privacy as a fundamental right: it «*de facto* enable (s) ample commodification of personal data, shifting […] to private deregulation via contract rules (terms of services and privacy policies)».

[22] Google, who has agreed to comply with the requirements of the Italian Authority in 2013 in relation to the information provided: improvement and differentiation of the privacy policy in relation to the various services provided, prior consent for profiling, filing and deletion of data. More details are available at the link http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3740038 The number of measures taken by the Authority on disclosure (Articles 13 and 161 privacy codes) are 642 (source: GarantePrivacy site)

[23] O. BENSHAHAR – A. CHILTON, *op. cit.* where it is shown that none of the techniques of simplifying information through best practices or warnings has changed the behaviour of the "stakeholders"; L. J. STRAHILEVITZ – M. B. KUGLER, *Is Privacy Policy Irrelevant to Consumers?* 45 *Journ. Legal Studies S2*, pp. S69 - S95 (2017) conducted another experiment on more than 1,000 Americans by submitting them (at random) two text versions of Google and Facebook privacy information, one clear and the other vague, to authorize facial recognition and processing of data. The results of the experiment confirmed that the users' choices, which also considered that highly intrusive

It seems obvious that if one persists within the logic of the information disclosure or its progressive, minimal improvements, chances are that this exercise does not lead to significant results[24].

Moreover, the *ex ante* provision of the consent to processing, which embodies the idea of self-determination of the individual with regards to the relevant information, in accordance with the theoretical model of fundamental rights, cannot limit the risks of data dissemination, given also the complexity of market's self-governance.

In any case, the current state of surveillance and technology does not prevent violation of data protection (think of spamming). This is true, as the experience teaches, with regard also to the case of a user, singly and especially reluctant to give consent to the processing of his/her data, and may be explained by the massive requests for data dissemination and the processing through algorithms[25].

As described above (sect. 1), in the world of big data, technical regulations hardly make pertinent data controllable and comprehensible to the end user.

The online processing of personal data accentuates the problem of controlling the flow of personal information in borderless cyberspace. The data subject easily loses track of the consent given and remains unable to understand which data controller has provided his/her data to subjects the data subject does not want to share with[26].

4. The legal and behavioural experiment at Unisob. Methodology and preliminary results

Following the outcomes reached by behavioural studies on the function of consent to personal data processing, in 2016 the Living Lab Utopia at the Suor Orsola Benincasa University of Naples (IT, Unisob) started an experiment to measure users' awareness and understanding of data protection in the digital context, whereby they gave their consent to data processing, at the downloading of a common operating system on an electronic device.

---

processing, have not changed because of the language of the information, but due to social norms and the technological experience. On this point, let me cite L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali. Un'analisi giuridico-comportamentale. Spunti di rifessione sull'effettività della protezione dei dati personali* Aa. Vv., *Nodi virtuali, legami informali. Internet alla ricerca delle regole*, edited by D. Poletti and P. Passagna, forthcoming, p. 53 ff.

[24] See SUNSTEIN, *Nudge Effect: The Politics of Liberal Paternalism*, trad. It. Edited by Barile, Milan (Aegea University Bocconi), 2015.

[25] In 2010, it is estimated that 90% of e-mails are nothing more than spam. BOCCHIOLA, Privacy, *Filosofia e politica di un concetto inesistente*, Roma (Luiss University Press), 2014, p. 46.

[26] G. COMANDÈ, *op. cit.*, 2015, 121 ff. , at 122 and 124.

This in order to verify whether the Italian legislation (which implements the European legislation still in force), focused on consensus and applied in this interactive system, is able to assure a certain degree of effective protection for users with regard to the processing of personal data and to identify the protection issues for users regarding their personal data where the processing request takes place in a digital environment.

The study is divided into two phases: an experimental part, based on the examination of the relationship between user and technology, and on the use of a Questionnaire for the collection and processing of digital data; another one, based on the examination of the data collected, aimed at better understanding if the current legislation on consent is successful in its objective of data protection.

To carry out the experiment, an Experimental Protocol and a Questionnaire have been developed. The Questionnaire is divided into in three macro-sections: a profiling part, a usability part and a legal one. As trial for each user lasted about an hour, the overall experiment required one and a half year before a significant quantitative data analysis was reached.

The study makes use of high-tech instruments as eye-tracker. In order to verify user's actions regarding privacy settings during the interaction with computer support, the dimensions evaluated are: attention (it can be analysed through graphic representations of heat map); execution time; reading order within the screens (thanks to gaze plot sequences); awareness and knowledge of the subject of data protection; usability.

Through this multi-instrumental analysis, the research aims at verifying whether the data subject of a potential data use agreement is capable of understanding, when the information is given and when he gives consent to the processing, who is the controller and whether he perceives any lack of comprehension as a lack of protection.

The methodological perspective adopted makes use of this analysis of behaviour, on the basis of cognitive psychology, as a test for the *efficacy*[27] of the law in force, placing the behavioural analysis in the legal domain.

The research is conducted in line with a multidisciplinary approach already present in non-Italian studies. However, with regard to the impact of the behavioural analysis, it should be noted that the project does not use the results within a normative economic model (as normally occurs in the context of behavioural economic analysis).

[27] The word *efficacy* is here used in its general meaning as the ability to produce a desired or intended result, which are the regulation's objectives. We preferred *efficacy* instead of *effectiveness,* which instead implies to measure a degree to which something is successful, lacking for now reliable tools for measurement.

Conversely, this study was carried out in order to ascertain the users' attitude towards achieving the regulatory objectives of protection of the individual user-physical person, in relation to the position of the professionals in the personal data market.

Below they will try to illustrate the results of the first 12 subjects, who submitted the test to the pilot (pilot). These are absolutely preliminary results from which significant conclusions cannot be drawn about the overall results of the experiment.

The proposed reading comprises only some preliminary observations with respect to some of the items being reviewed, but no definitive conclusion can be made.

The experiment is now concluded and was carried out on 97 subjects, of which:

- 12 subjects were tested for the pilot test;
- 12 subjects were for the final test, the results of which are commented on below;
- 53 tests have been conducted and will be further evaluated.

It is worth noting, however, that the composition of the sample consists mainly of young people (between the ages of 18 and 24), the majority of whom claimed to have received legal training or to be familiar with arguments of a legal nature and technology.

In general, there emerged a number of contradictions between behaviour and statements of interest regarding data protection and technology.

1. The majority of the sample affirms to be highly interested in protecting their data, and even when the sample was required to compare personal data protection and security, the majority of the group tended to prefer the first compared to the second;
2. However, only a small percentage (16%) disabled the "Quick Setup" function;
3. In relation to the task of changing the privacy setting already chosen, or automatically default, 58% of the sample did not read the privacy statement at the time of installation, even if it is in an induced situation. In any case, 100% of this sample section still modifies privacy settings. The data reveals how there is no link between the information and the self-determination of the user.

Among the privacy options modified in the task of changing the privacy setting, there are geo-localization and information given to the personal assistance software, though they were previously evaluated as of some utility or fully utilized by the same subjects.

Indeed, 75% of the sample had, in a previous question, expressed a judgement according to which position detection and vocal recognition functions were somewhat or very useful.

On the assumption that one cannot infer definitive results from the data, the following considerations can be made.

From the collected answers and users' activity observed, there is a general tendency to prefer operative choices that imply the simplest and shortest solution.

Specifically, as to the information and management on data processing, users were revealed to have misunderstood the information provided, although they perceived themselves to be aware and able to manage the privacy setting commands.

The experiment, although at its initial stage, shows that even those who care about their personal data (supra 1) generally do not pay attention to or outright disregard the privacy notice, even in a non-natural environment (the experiment) where subjects are specifically required to perform the task of reading the privacy policy. Consent to the processing of personal data is given simply following the activities to which the data processing is functional and it plays no role in decisions pertaining to daily activities, also considering that clauses on data processing in the digital environment are consistently "take it or leave it".

The perceived attitude of users towards information as well as the more general connection of data processing to the services and goods may lead one to consider whether improving the formulation and clarity of the information can yield significant changes in the level of awareness of users.

Indeed, the ineffectiveness of privacy warnings has been clearly demonstrated by economic and behavioural studies, taking into account the issue of aggregated data, that is, the number of bodies that collect and use personal data, especially in a digital environment. It renders impossible the management and control of the use of personal data by end users, which essentially relates to every aspect of the individual's life. These studies collectively show that, in a more or less conscious manner, the information is not read and therefore the consent given is not consciously provided.

5. The remedial issue. Some suggestions for a complex scenario

If the data subject's decision does not influence protection of personal data, this may call for a change of paradigm.

The EU Charter of Fundamental Rights already recognizes consent as only one of the legitimate bases for the processing of personal data. Hence, one might say that the consent is not a key requisite, as confirmed by the legislation that will apply from 2018, which includes the purpose of direct marketing as a legitimate interest pursued by the data controller (cons. 47), such as to exclude the consent by the data subject (Article 6, par. 1 *(f)*).

In this context, then, there may be room for a system where the consent rule is interpreted restrictively or, in a *de jure condendo* perspective, no longer required. The protection of data (if!) would be entrusted in principles and rules relating to the processing, as fairness, risk of loss minimization and security assessments according to the accountability principle, promoted by the new discipline, which reinforces the controller's responsibilities as regards to its organisation. It should also be pointed out that the fact that the processing can rely on legitimate bases other than consent does not, at least in principle, exclude the necessary balancing of these other interests with fundamental freedoms.

Such a scenario would unveil the "illusion of consent" where consent is considered as a tool for controlling one's data, and overcome the false perception of people able to independently control and protect their data.

More effective means for the purpose of protecting data (such as uncontrolled or inappropriately justifiable data dissemination), can be considered: rules of processing, limits (or prohibitions) for certain types of processing and / or for certain data, or more efficacious data anonymization guarantees and internal technical rules of processing [28].

From this point of view, it is appropriate to distinguish within the types of data and types of processing already present in European legislation.

As to the types of data, the Italian law refers to personal and sensitive data (special categories of personal data, according to art. 9 Reg. 2016/679, where fundamental rights of the person are at stake). Until the new Regulation is applicable in 2018, under Italian law in case of processing of sensitive data, a preliminary authorization by the national Data Protection Authority is still required. The new European regulation eliminates the bureaucracy of preventative authorization in case of special categories

[28] Prescription of technical rules and conformed technologies (regulation by technology) can be found in the GDPR - the so-called *Privacy by design* (Article 25) and the mechanisms and bodies for the certification of data protection (42). MANTELERO, *Privacy digitale: tecnologie conformate e regole giuridiche*, in AA. VV., *Privacy digitale. Giuristi e informatici a confronto*, Torino (Giappichelli), 2005, p. 19 ss. On the reversibility of anonymization procedures, OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Aninymization* 57 UCLA Law Rev. 1701 (2010); Article 29 Working Party on Data Protection, Opinion 05/2014 on anonymizing techniques, 10 April 2014.

of (*sensitive*) data, but retains the distinction of limiting, in principle, the number of cases in which this data can be processed without consent.

In a *de jure condendo* perspective, this distinction could open a differentiated process between personal data and sensitive data. Consent could be maintained for limited sensitive data types, for which the abstract possibility of effective attention by the data subject at the time of request is conceivable. At the same time, the only alternative to the existing scenario would be to impose limits to processing that may also cause injury as a result of the processing and combining of multiple personal / sensitive types of data (as in case of profiling).

This perspective would mean that the European legislator takes a stand with regard to the development of the data markets and the long-term impact on the rights of the person by regulating the dissemination of information.

The central issue therefore is about rules and limitations of processing, given the lack of *normative efficacy* (effectiveness) of *ex ante* selection mechanisms by the party (consent).

Personal data protection, from the point of view of private law, is also limited in the remedial phase *i.d. ex post* remedies, represented at the private law level by compensation for damage (Article 82 GDPR).

Italian judgements are scarce in this regard and in any case not unequivocal[29]. There appears to be a substantial rejection of claims for damages, where there is a difficulty in proving damages if they do not concern any fundamental right (eg. right to privacy in the strict sense; right to identity) different from the right to the protection of personal data.

The development of technology has imposed or induced us to "surrender" personal information, which are then stored and processed for the most diverse purposes: economic interests, sharing and manifestation of personality, of public interest. As already seen, people have their own personal data processed, without being aware of any misuse.

However, even if a person comes to know of the illegitimate processing of his or her own personal data, he/she may fail in effecting a legal remedy. This can happen for a number of reasons:

– A more general difficulty in liquidating non patrimonial losses;

[29] A recent research on a major Italian database (*De Jure*), based on the corresponding Italian article of the Data protection code (art. 15 d. lgs. 196/2003), without any restriction, comes up with 156 results.

- Trivial amount of damages (think of spamming)[30];
- Difficulty of tracing the processing that has given rise to or is involved in the production of the harmful event (it may be the case of unauthorized profiling leading to the personal tastes of the individual he intends to keep confidential).

Even in cases where it is possible to envisage a non-pecuniary loss for personal data breach, there are issues related to the liquidation of the damage, as evidenced in recent cases. The remedial shortage of private law remedies for the violation of the right to personal data *tout cour*, tends to confirm that the right to data protection is not effectively upheld for the private individual.

These considerations lead to two alternative scenarios.

In the first view, it is arguable that the real purpose of protecting the right to personal data (when not sensitive) concerns the protection of the markets or the protection of a more general condition of human existence, but it is not controllable or closely referable to natural person, in a *ex ante* (consent) or *ex post* (damages) perspective.

In the second view, given the lack of protection but with the purpose of enhancing remedies for data protection, data breach would allow for punitive damages in favour of the data subject, even when serious damages are not incurred, but the breach led to gain for the offender[31]. However, even in this case, given the aggregation of personal data, a careful evaluation of the criteria for determining the recoverable amount would be needed.

However, this is another story, which contributes to dissatisfaction with the current legal framework[32].

[30] Italian Cass., January 11, 2016, no. 222, in *DeJure* commented in *Dir. Giust*., 2016, p. 3, denying eventual damage, clarifies that the violation of the right to the protection of personal data must exceed the minimum tolerance threshold imposed by the duties of solidarity according to art. 2 of the Constitution, which provides for the recognition and safeguarding of the inviolable rights of man, both as a single person and in the social formations where his person acts, and demands the fulfillment of the indispensable duties of political, economic and social solidarity. A violation of the right to personal data can therefore only occur in the event of a significant offense to the effective scope of the law. Likewise, with regard to so-called supersensitive data (sex rectification), Cass. May 13, 2015, 9785 in *Fam Dir*., 2016, p. 469 ss.

[31] SIRENA, *La gestione di affari altrui. Ingerenze altruistiche, ingerenze egoistiche e restituzione del profitto,* Torino, 1999, p. 277.

32 Suggests a different set of remedies A. MANTELERO, *Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection,* 32 *Comp. Law & Secur. Rev*. (2016) 238 ff.