Comparative Law Review

Rescuing Comparative Law and Economics?
Exploring Successes and Failures of an Interdisciplinary Experiment

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Department of Law - University of Perugia
Via Pascoli, 33 - 06123 Perugia (PG) - Telephone 075.5852437
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
SPECIAL ISSUE – VOL. 12 /2

Edited by Giuseppe Bellantuono

Rescuing Comparative Law and Economics?
Exploring Successes and Failures of an Interdisciplinary Experiment

COMPARATIVE
LAW
REVIEW
SPECIAL ISSUE – VOL. 13/1

Edited by Giuseppe Bellantuono

Rescuing Comparative Law and Economics?
Exploring Successes and Failures of an Interdisciplinary Experiment

RELATIONAL DISCLOSURE AS A MEANS FOR DATA SUBJECTS' INFORMED CONSENT*

Antonio Davola & Ilaria Querci

TABLE OF CONTENT

Digital markets are flexible and developing, and so it is privacy law. Before and together the enactment of the GDPR, data protection rules have drawn contributions, amongst others, from sociology, anthropology, economics, and marketing. This happens, intuitively, because privacy has an inherent social dimension: the concepts of identity and autonomy, equality and freedom, the meaning of social relations and political relations all play a distinct role in privacy law. Undoubtedly, a central role in constructing privacy and data protection law has been played by decision-making studies: since its early days, individual protection has been structured according to the axioms of economic neoclassical theory. Accordingly, the attribution of rights in favor of users has been significantly affected by the view of individuals as homini oeconomici. Yet, as soon as deviations and diversions from the traditional paradigm emerged, law has been proven able to evolve as well, and progressively adjusted in order to encompass new approaches to online interaction that largely contrast with the rigidity of the conventional economic theory of individual behavior. Still, some axioms of the early neoclassical model as it was originally conceived are still present in consumer law, despite being widely debated amongst economic scholars. In particular, the assumption of a-social individualism still permeates the structure of user rights, and European privacy law rests on the implicit assumption that consent to the processing of personal data and the analysis of big data is a purely individual choice. Against this view, the paper investigates evidence emerging from studies and experiments that show that consent in data processing is not only – and often – partially irrational, but also inherently relational. Then, it observes that the regulatory framework laid down by the GDPR does not take into proper account this aspect and subsequently defends the development of a system of contextualized disclosure as a tool to promote informed consent. Lastly, the compatibility of such a system with the European and Californian data protection law is analyzed.

I. INTRODUCTION

It is widely acknowledged that the vast majority of B2C online interactions exploit users' profiling and that the "digital footprints" of individuals are employed as essential tools for

* Antonio Davola is Assistant Professor in Economic Law at the University of Bari "Aldo Moro". Ilaria Querci is Post-Doctoral Research Fellow in Management, at "Ca' Foscari" University of Venice. The present paper is the joint effort of all the authors. In particular, Antonio Davola contributed mostly to Sections 1, 2, 3, 4 and 6, whereas Ilaria Querci contributed mostly to Section 5. Section 7, lastly, was drafted jointly by the Authors. This article has been developed as part of the Marie-Sklodowska Curie Project "FairPersonalization" (MSCA-IF-2019-897310) with the support of the European Commission. The authors are thankful to the participants of the Italian Society of Law and Economics 2021 conference for their insights and comments on previous versions of this paper. All errors rest with the authors.

elaborating and delivering products and services on the web.[1] As people unconsciously operate as "informative agents", they constantly share information via their online activity, as well as in their interaction with IoT products, and wearable devices: hence, with technology facilitating the free flow of information, the scale of the collection and sharing of personal data has increased exponentially.

As a result, users' data analysis is nowadays a fundamental resource for web operators and platforms, and being able to obtain, process (and sell) information is one of the main drivers for economic success in the digital environment. Alongside personal data becoming economically valuable assets, also comes the increased exposition of users to requests to provide information when they surf the internet, and the risks of data being misused by data processors and controllers.[2]

The joint outcome of these two aspects is, indeed, that users are oftentimes unaware of how their personal information is acquired, and then managed, by companies. The advent of digitalization entails, therefore, a growing risk, that citizens are deprived of control and lack awareness regarding which information about them is available on the web, as an inner corollary of computerization.

Against the wide-spreading feeling of disorientation and disempowerment emerging as a result of the structural power asymmetry created by digital infrastructures,[3] privacy and data protection law emerged as cornerstones of the regulation of the information society, operating as major tools to enhance individuals' protection and to ensure an effective oversight on information detained by third parties.

Whereas privacy has traditionally been seen as the "right to be let alone",[4] operating as a restricting tool against unwanted intrusion of individuals' private sphere and as a pre-condition to the exercise of fundamental rights, data privacy law aimed at further strengthening the effective (and, to a certain extent, proactive) power of individuals over intensive data collection and processing: in other terms, protecting the right of individuals to control their analogical and digital identities entirely.[5]

Historically, this trend can be traced (at least) back to the early 70's, with the first strand of legal scholarship pointing out how computers and large databases could introduce new risks

[1] *Inter alia* see I. Domurath, *Technological Totalitarianism: Data, Consumer Profiling, and the Law* in L. de Almeida, M. Cantero Gamito, M. Durovic and K. Purnhagen (eds) *The Transformation of Economic Law: Essays in Honour of Hans-W. Micklitz*, Hart, 2019, 66.
[2] R. Calo, *Digital Market Manipulation*, in 82 George Wash Law Rev, 2013, 995.
[3] See L.A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limit*, Kluwer, 2002, 117.
[4] S.D. Warren; L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 1890, Vol. 4, No. 5, 193-220.
[5] G. Gonzales Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014.

related to data processing for users; in Europe, the issue led to an early set of national laws and court decisions[6] establishing an individual right to informational self-determination, incompatible with a society where citizens do not know who knows what about them.

Yet, it cannot be doubted that contemporary technologic developments further augment the need for data protection: with the protection of personal data being identified as a fundamental right by Art. 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01)[7], individuals have been conferred dedicated rights in relation to the legal protection of their personal data and information, being therefore qualified as "data subjects".

II. DATA SUBJECTS' RIGHTS AND THE INFORMATIONAL PARADIGM

In the European Union, the qualification of an individual as a data subject represents the normative basis for the application of the set of rights currently awarded by the General Data Protection Regulation (Regulation 2016/679/EU, hereafter, GDPR): while being heterogeneously structured, the common trait of these entitlements lies in the assumption that, over digital-interactions, users are generally deprived of a satisfactory level of knowledge regarding the acquisition and processing of their data: therefore a substantive compensation of the power and information asymmetry existing between them and their counterparties is necessary in order to allow them to make punctual informed decisions on whether to provide consent to data-related practices[8] and to monitor that the data processing is conducted according to their will.

Accordingly, data subjects' empowerment measures operate through the award of *ex ante* and *ex post* rights, providing users with a set of powers to exercise before and after the data processing starts: this is functional to enable individuals' control over information throughout the whole personal data's lifecycle; some of the rights awarded to data subjects are prerequisites to others: for example, the right to access constitutes a pre-requisite to the

[6] E.g. in Germany see BVerfG, decision 15. December 1983 - 1 BvR 209/83 -, Rn. 1-215; also, Swiss Federal Court, 2019, BGE 146 I 11; Swiss Federal Supreme Court, 2017, BGE 143 I 253; Supreme Court of the Czech Republic, order of 12 December 2012, file no. 30 Cdo 3770/2011; Mosley v. United Kingdom, judgment of 10 May 2011, no. 48009/08, complaints valid September 15, 2011; European Court of Human Rights, judgment of 24 June 2004, no. 59320/00, Hannover v. Germany; and judgment of 31 January 1995, no. 15225/89, Friedl v. Austria.

[7] "(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

[8] See G. Gonzales Fuster, *How Uninformed is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection*, in Revista de Internet, Derecho Y Politica, 2014, 9.

(different) right to the rectification of incomplete or untruthful data.[9] In addition, all data subjects' rights are to be interpreted in light of the general principles of transparency and fairness present in the GDPR,[10] and are implemented with the observations and considerations operated by the Court of Justice of the European Union.

Consistently with the abovementioned belief, that users' vulnerability is essentially due to the information gap they suffer from in their interaction with professional counterparties, data subjects' rights are mostly communication-based and inspired to an overall duty to enhance transparency and comprehensibility: accordingly, the General Data Protection Regulation requires information to be concise, transparent, intelligible, and expressed in an easily accessible form, using clear and plain language.[11]

In order to substantiate this claim into properly intended standards, data protection rules (before and) within the GDPR have drawn contributions, amongst others, from sociology, anthropology, economics and marketing. In addition, EU institutions increasingly engaged in attempts to encompass emerging empirical and theoretical findings in their regulatory processes and to accordingly shape the modes of users' rights in their interactions with business operators.

Such an interdisciplinary approach is particularly significant in this field, given the inherent social dimension of privacy: the consequences that digital media and the big data market have on individuals, their identity and anonymity, the transformation of social relationships, justice and equality, for democratic political procedures and for society in general all play a distinct role in the debate about the development of data protection law.[12]

Considering these aspects, the importance of privacy has mostly been justified by the individual interests and rights it protects, such as informational self-determination and autonomy;[13] it is, therefore, not surprising that a central role in constructing privacy and data protection law has been played by decision-making studies following the neoclassical approach.[14]

---

[9] See European Court of Justice, Case C-454/16, Peter Nowak v Data Protection Commissioner, EU:C:2014:317; Case C-73/16, College van burgemeester en wethouders van Rotterdam v Mee Rijkeboer, EU:C:2009:293.

[10] European court of justice, Case C-49/17, Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV, EU:C:2019:629, 102.

[11] See Art. 12. GDPR.

[12] B. Roessler D. Mokrosinska (eds), *Social Dimensions of Privacy Interdisciplinary Perspectives*, Cambridge University Press, 2015, *passim*.

[13] D. Solove, *Understanding Privacy*, Harvard University Press, 2008.

[14] *Ex multis* A. Acquisti, C. Taylor, and L. Wagman, *The Economics of Privacy*, in Journal of Economic Literature, 2016 54 (2): 442-92.

Following the well-established concept of individuals as *homini oeconomici*[15] and the expected utility theory for choices under certainty,[16] data protection has long been considering individuals as rational entities able to process the information at their disposal to reach logical conclusions and pursue their priorities.[17] As a consequence, users' empowerment heavily relied on employing disclosures, which are seen as the main tool to overcome the information asymmetry lying at the core of exploitation by professional counterparties.[18]

Even if the disclosure is not the only form of users' protection, operating *inter alia* alongside supervisory and structural obligations (such as the rules on Privacy by Design and by Default[19]), informational duties are still a primary mode of regulation.

Besides the influence of the neoclassical theory, several additional reasons can be identified to justify the primacy of disclosure obligations as regulatory tools. It has been observed, for example, that disclosure is a (relatively) low-cost form of intervention and that it is also a "transparent" one for all the parties involved: *ex ante* disclosure rules are prompt to enforce for supervisory authorities and, at the same time, allow companies to clearly identify whether they are complying or not with the relevant provisions. Lastly, it is often defended that disclosure obligations enjoy some sort of "bi-partisan" support, as they strike a convenient balance between paternalist and liberalist approaches to market regulation.[20]

III. THE CRITIQUES TO THE INFORMATIONAL PARADIGM. AN OVERVIEW

Against this background, it is well-known that a vast amount of research (and behavioral studies more in general) defends that individual decision-making often deviates from the neoclassical paradigm[21] and provides evidence of the dynamics of online interaction that are in contrast with the rigidity of the conventional economic theory of individual behavior, especially in cases involving standard form contracts.

---

[15] J.S. Mill, *On the Definition of Political Economy, and on the Method of Investigation Proper to It*, in London and Westminster Review, 1836; see also C.H. Hinnant, *The invention of homo oeconomicus: A reading of John Stuart Mill's "on the definition of political economy"*, in Prose Studies, 1998, 21, 3, 51-68.

[16] J. Von Neumann, O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, 2013 (1st ed. 1944); see, *amplius,* J. Levin., *Choices Under Uncertainty*, 2006, at https://web.stanford.edu/~jdlevin/Econ%20202/Uncertainty.pdf, accessed on 12 May 2022.

[17] S. Selikoff, *Understanding Neoclassical Consumer Theory*, 2011, at http://www.samselikoff.com/writing/economics/understanding-neoclassical-consumer-theory/, accessed on 12 May 2022. See also R.A. Epstein, *The Neoclassical Economics of Consumer Contracts*, in 92 Minnesota Law Review, 2007, 803; T. Zalega, *Consumer and Consumer Behaviour in the Neoclassical and Behavioural Economic Approach*, in 4 Konsumpcja I Rozwój, 2014, 9, 64-79.

[18] P.D. Lunn, *Are Consumer Decision-Making Phenomena a Fourth Market Failure?,* in Journal of Consumer Policy, 2015 .

[19] L. Bygrave, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements,* in Oslo Law Review, Volume 4, No. 2, 2017.

[20] O. Ben-Shahar, C. Schneider, *The Failure of Mandated Disclosure*, in 159 University of Pennsylvania Law Review, 2011, 647 681-684.

[21] *Ex multis* C. Sunstein, Behavioural Law & Economics, Cambridge University Press 2000.

Accordingly, studies on information overload; on the influence and effects of the no-reading problem, and the framing and saliency bias in information provision show the inner weakness of – traditionally intended – information duties as a means to ingenerate genuine awareness[22] and, more specifically, as viable strategies for preserving users' control regarding the collection and processing of their data.

Data protection law has not been immune to these developments, and regulatory initiatives tried to accommodate behavioral findings within the structure of the GDPR, mainly by rethinking the traditional approach to the principle of transparency and promoting a substantive approach to disclosure as a means to stimulate informational self-determination. This can be observed, for instance, in the provisions of the GDPR mandating for information and communications regarding data processing to be easily accessible and easy to understand, and that clear and plain language is used for such disclosure.[23]

The growing attention to ensuring the awareness of consent – both by express statutory provisions[24] and by means of judicial decisions rendered by Member States' authorities and the European Commission[25] - further supports these considerations.

IV. The unspoken axiom of the "a-relationality" of decision-making

Despite these advancements, axioms that can be traced back to the conceptual underpinnings behind the neoclassical model seem to be still present and untouched in the GDPR structure. In particular, it should be observed that an underlying assumption of a-social individualism still permeates the structure of data subjects' rights: individuals' desires and preferences for privacy and data management are deemed to be essentially endogenous: allegedly, an individual's choice regarding how to manage her privacy settings will depend only on her

[22] I. Ayres, A. Schwartz, *The No-Reading Problem in Consumer Contract Law*, in Stanford Law Review, 2014, 66(3) pp. 545-609; Ben-Shahar (n 20); F. Cheng, C. Wu, *Debiasing the framing effect: The effect of warning and involvement*, in 49 Decision Support Systems, 3, 2010.

[23] Art. 5(1)(a) and Recital 58 GDPR.

[24] See Art. 7 GDPR, further discussed in Section 6.

[25] See, Autorità Garante della Concorrenza e del Mercato, 'Sanzioni per 20 milioni a Google e ad Apple per uso dei dati degli utenti a fini commerciali (PS11147)', 16 November 2021, https://www.agcm.it/media/comunicati-stampa/2021/11/PS11147-PS11150; Bundeskartellamt, decision no B6-22/16 of 6 February 2019.OLGDüsseldorf,26 Aug. 2019, VI-Kart 1/19 (V), Bundeskartellamt c. Facebook; Bundesgerichtshof, 23 Jun 2020, KVR 69/19; Datatilsynet, 'Grindr LLC (Administrative Fine)' (2021) https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine---grindr-llc.pdf; ECJ, Case 673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet49 GmbH, ECLI:EU:C:2019:801. For a comparative analysis of these decisions and their implications see A. Davola, G. Malgieri, *Data-Powerful*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4027370 (last accessed 12 May 2022).

personal preferences and (at most) by the quality of information disclosed by the counterparty in compliance to the GDPR. According to this view, users' choices are not supposed to be affected in any way by their ability to put the information "in context", which might include the observation of others' behaviors as well: the mere provision is already sufficient for reaching optimal decision-making.

Symptomatic of this conception of individual decision-making are, for example, the rules set in Articles 13 and 14 GDPR[26], as well as the notion of specific, informed, and unambiguous consent as developed in Recital 32 of the Regulation:[27] all these provisions ultimately rely on the idea of users operating as individual deciders, who can elaborate information and make choices without a need for contextualization.

As a consequence, data protection and privacy scholars take into account the direct interaction between data processors and data subjects only; in addition, this approach does not change even when the modes of intervention depart from the traditional approach to regulation and disclosure - for instance when debiasing and nudging strategies are employed.[28]

Even those critiques recently addressing the structure of the data protection framework in the European Union, and arguing in favor of the introduction of some sort of "social" components in the consideration of decision-making's nature do not seem to contend with the ultimate individualized nature of this process: for example, remarks raised on the basis of game-theory analyses[29] criticize consent as a meaningful tool of protection given the structural cross-processing of personal data by companies and observe that denying consent is generally a non-profitable strategy to be followed (e.g. considering what other individuals might do in response to our conducts). Still, even this perspective is ultimately focused on the strategic analysis of other data subjects' expected behavior, rather than on the actual observation of peers' acting as a determinant for choice-making.

---

[26] Respectively regulating "Information to be provided where personal data are collected from the data subject" and "Information to be provided where personal data have not been obtained from the data subject".

[27] "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."

[28] C. Jolls, C.R. Sunstein, *Debiasing through Law*, in The Journal of Legal Studies, 2006, vol. 35, no. 1, 199–242.

[29] Y. Hermstrüwer, *Contracting Around Privacy. The (Behavioral) Law and Economics of Consent and Big Data*, in JIPITEC, 2017.

Also, scholarship who argues in favor of the promotion of a "relational" turn for privacy and data protection:[30] still – and as much as desirable it might be – this approach merely refers to the conceptual consideration of data protection as a social (rather than an individual) value, with specific regards to the societal consequences that can arise from unlawful data processing. Therefore, in this case, the relationality does not pertain to the users' decision-making but, rather, to the general understanding of the nature of the values protected by data protection and privacy law.

Against this bedrock, we argue that introduction of a model based on s.c. "relational disclosure"— i.e., the creation of a condition in which consumers are able to compare their own privacy terms to those presented to individuals with similar or different characteristics, and the envisaged consequences of those processing— can significantly improve data subjects' awareness and advance their degree of protection.

V. The case for relational disclosure for data acquisition: insights from sociological studies and model

If the idea of a "relational nature" of decision-making ultimately seems to be missing in the legal debate, this conception is not unknown to other fields of research: the analysis conducted by the Swiss sociologist Albert Badura in the late '90 – which then developed in a framework that is nowadays known as Social Cognitive Learning Theory (SCLT)[31] – defend that an essential part of individuals' learning process comes from developing behaviors and cognitive strategies by means of observing others who act in contexts that are similar and different from the ones the subject is experiencing.

Therefore, the question arises: if contextualization of information is a primary determinant of learning in general, is it possible, with specific reference to data protection, to improve the awareness of data subjects' choices (e.g. regarding the provision of the consent) by making individuals able to contextualize the consequences of their choice within the market state and in comparison to their peers, therefore introducing relational element in disclosure?

Moving from the consideration, that the shortcomings affecting consent in data processing cannot be entirely undertaken as long as they are interpreted in their individual dimension

[30] N.M. Richards, W. Hartzog, *A Relational Turn for Data Protection?*, in 4 European Data Protection Law Review 1, 2020.

[31] A. Bandura, *Social foundations of thought and action: A social cognitive theory*, Prentice Hall, 1986; Id. *Social Learning Theory*, Prenctice Hall, 1977.

only, it is reasonable to defend that currently existing, individually segmented disclosure on parameters and determinants for data processing could be integrated by an outcome-oriented disclosure, exploiting elements from legal design[32] and providing relational information to data subjects.

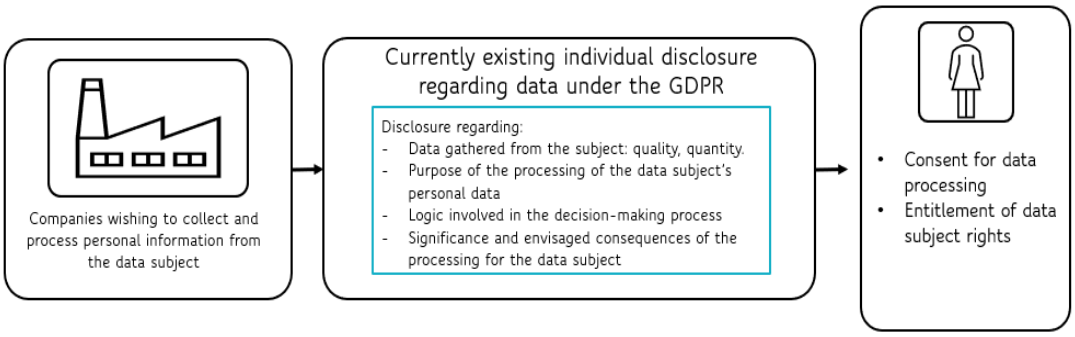
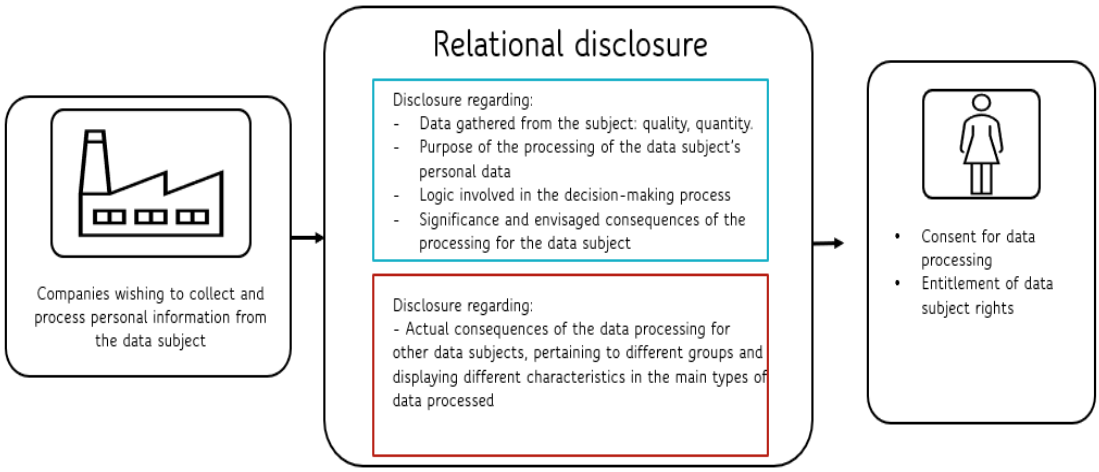


Figure 1 provides a theoretical overview of the traditional, non-relational, regulatory mode of disclosure within the GDPR framework:

As it can be observed, existing information obligations pertain to different aspects involved in the data processing (quantity and quality of the data, storage mechanisms, purpose of the processing and, when specific hypotheses occur – e.g. an algorithmic decision-making system is involved – the logic and the envisaged consequences of the automated processing), which shall be transmitted to the data subject to empower her to properly exercise her consent, as well as the other rights provided by the GDPR. Yet, all those information refers to the individual relationship existing between the data subject and her counterparty, without the first being able to contextualize the statement provided.

On the other hand, *Figure 2* displays a graphical representation of a hypothetical model based on the relational disclosure paradigm:

[32] H. Haapio, M. Hagan, M. Palmirani and A. Rossi, *Legal Design Patterns for Privacy*, in E Schweighofer et al. (eds), *Data Protection / LegalTech. Proceedings of the 21th International Legal Informatics Symposium IRIS 2018*. Editions Weblaw, Bern 2018, pp. 445–450.



A relational disclosure model provides a set of additional obligations, which do not describe aspects of the specific data processing involving the users: in particular, the second block of disclosure mandates to inform the data subject regarding the consequence of data processing for other individuals showing different – and yet, statistically significant – characteristics. This kind of information could be, for example, provided by the companies by extracting historical data about previous processing, in order to illustrate the consequence and outcomes for (in hypothesis) the main demographic group considered, or for subjects displaying characteristics that are deemed essential for the analysis. Considering, e.g., the use of data for advertising purposes, it would be possible for instance to illustrate how key-characteristics displayed by other data subjects impacted on the offerings that were presented to them, or more in general how the different advertisements vary on the basis of specific characteristics of clustered groups considered in the data processing.

VI. Comparative investigation of the normative foundations of a relational disclosure model: considerations on consent amidst GDPR and CCPA

Ideally – and as some empirical investigations already seem to suggest[33] – the introduction of a relational disclosure model could empower users' awareness in providing consent for data processing activities and, subsequently, activating their rights as data subjects.

[33] A. Davola, I. Querci, S. Romani, *No consumer is an island. Relational disclosure as a regulatory strategy to advance consumer protection against microtargeting,* available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4068548 (accessed 12 May 2022); S. Larsson, *Algorithmic governance and the need for consumer empowerment in data-driven markets*, in 7 Internet Policy Review, 2018, 2.

In order for such a system to be introduced, though, its compatibility with current data protection provisions should be first assessed, with specific reference to the rules regulating the provision of consent for data acquisition and processing.

Considering the potential normative foundations of such a claim, the GDPR seems, indeed, to provide a *prima facie* fruitful margin of maneuver: by analyzing the wording present in the provisions existing in the Regulation it is possible to observe, for example, that in those cases in which data processing is based on profiling or implies an automated component, the GDPR mandates data processors and controllers to provide data subjects with specific information about the processing (along with rights to objection and to request for human intervention and for challenging decisions), the logic involved in the decision-making process, and the significance and envisaged consequences for the individual.[34]

As it can be observed, the content of the disclosure operated pursuant to the provision is open-ended, and the quality of the information provided is to be appreciated from a teleological perspective, considering its adequacy to advise the data subject regarding some key aspects of the data processing.[35]

Analogously, the structure of the other rules of the GDPR enlisting data subjects' rights is generally interpreted as functional to enable individuals' effective control over information throughout the whole personal data's lifecycle in light of the general principles of transparency and fairness present in the GDPR,[36] as well as inspired to an overall duty to enhance comprehensibility.[37] These considerations, *inter alia*, inspired those researchers who tried to hypothesize and inspect the existence of a properly intended right to explanation within the GDPR,[38] focusing their investigation on the opportunity for information to promote actual, rather than merely formal, awareness in data subjects.[39]

In the aftermath of the enactment of the GDPR, and in light of the increasing automation of data processing, many debated regarding what constitutes a meaningful, aware, and informed consent according to Art. 5 and if the GDPR also includes an implicit right to an explanation as its intrinsic corollary.[40] As the European Data Protection Board underlined

[34] Art. 22 GDPR

[35] See also P. Hacker, J.H. Passoth, *Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond*, in A. Holzinger, R. Goebel, R. Fong, T. Moon, K.R. Müller, W. Samek, (eds) xxAI - Beyond Explainable AI. xxAI 2020. Lecture Notes in Computer Science, Springer, 2022.

[36] European court of justice, Case C-49/17, Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV, EU:C:2019:629, 102.

[37] See abovementioned Art. 12 GDPR.

[38] M. Kaminsky, *The right to explanation, explained,* in 34 Berkeley Technology Law Journal, 2019 1, 189-218.

[39] See also O. Seizov, A. Wulf, J. Luzak, The Transparent Trap. Analyzing Transparency in Information Obligations from a Multidisciplinary Empirical Perspective, in Journal of Consumer Policy, 2019, 42(1), 149-173.

[40] See Kaminsky (n 38).

that consent can be deemed informed when the data subject is provided those "elements that are crucial to make a choice",[41] Art29 Data Protection Working Party further clarifies that the way the information is given plays a crucial role in assessing whether the consent can actually be deemed informed and, subsequently, aware. In particular, the way in which information must be provided to the data subject must be specifically declined on the basis of the context of the provision, in order to always allow for a regular/average user to be able to understand what she is consenting to, and for what purposes.[42]

Whereas such indication is often identified as only referring to the usage of a clear, transparent, and plain jargon in communicating the conditions and relevant elements pertaining to the data processing, it should also be observed that the data subject's understanding is explicitly qualified as "contextual",[43] which subtends the idea that information could be modulated in order to allow the user to compare her condition to her peers, to other data subjects, or to an external dimension more in general, as long as this procedure is functional to promote consciousness in the exercise of her rights.

Interestingly, this functional interpretation of the notion of informed consent is not present in the GDPR only and can be, indeed, observed in other *corpora* outside the European Union as well, therefore identifying some conceptual common ground for policy recommendations. As far as the United States are concerned, it is widely known that a major characteristic of North American jurisdictions lies in the absence of a unitary federal law regulating data protection; rather, currently, several vertically-focused federal privacy laws exist, which take into account data processing and privacy challenges that arise in different fields.

Yet, besides the body of federal law, in recent years a minor number of states (namely, Colorado, California, and Virginia) have been introducing harmonized privacy laws, that are meant to operate horizontally. Amongst national laws, the recently enacted California Consumer Privacy Act (CCPA) is of particular relevance: the CCPA was first introduced in 2018, and in the subsequent years has been significantly amended to take into account technological developments and new risks emerging from intensive data processing activities, with the last step of this process being represented by the California Privacy Rights Act (CPRA) of 2020, which will take effect from the beginning of 2023 onwards.Differently from

[41] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, available at https://edpb.europa.eu, last accessed on 12 May 2022.
[42] Art. 29 DPWP, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011 01197/11/EN WP187, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, last accessed on 12 May 2022.
[43] Art. 29 DPWP, Opinion 15/2011 on the definition of consent, p 35.

the GDPR, the CCPA and the CPRA do not require explicit *ex ante* consent by users in order for their data to be processed by a business operator: indeed, Californian law only requires a privacy notice to be made available informing consumers of their right to opt-out from data collection, and eventually correct inaccurate data.

Still – and considering that an evaluation regarding whether or not the actual opt-out system regulated by the CCPA establishes a robust means of protection for American citizens is beyond the scope of this paper - it shall be observed that under the disclosure requirements set by the CCPA consumers must still receive notice "as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used".[44] As no indication is provided regarding the specific format of the disclosure, it is not implausible to hypothesize the utilization of a relational model in an *ex post* format as well; this solution might even operate with major effectiveness if the consequences of the data processing for the users are actually displayed in comparison with the outcomes of the processing for other individuals.

Also, given the current framework of both EU and US data protection regulations, it is relevant to observe that the introduction of a system of relational disclosure might operate as a resource to harmonize cross-country data processing best practices, operating a step towards the establishment of common standards for advancing users' protection, which currently represents a major challenge for the EU-US relationship in the aftermath of the Schrems judgments.[45]

VII. PRELIMINARY CONCLUSIONS AND FORTHCOMING ANALYSES.

Whereas the rethinking of disclosure models in order to empower users in exercising their consent for data acquisition and processing constitutes an already rather robust strand of research, European law still rests on the implicit assumption that consent to data processing (and, more in general, decision-making) is a purely individual choice. Accordingly, regulatory interventions – and the GDPR itself – mainly focus on how to overcome informational asymmetry by providing the user with additional information about her relationship with the professional counterparty. Even those studies that criticized this approach, addressed the shortcomings of the information paradigm as a whole, without questioning the individual nature of decision-making as a matrix for developing users' rights.

[44] Cal. Cov. Code §178.100(b)

[45] Case C-362/14, Maximillian Schrems v Data Protection Commissioner [2018] ECLI:EU:C:2015:650 and case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems (Schrems II) [2020], ECLI:EU:C:2020:559.

Against this view, the research defends that prompting people to reflect on a contextual dimension of data processing—by means of a simple framing intervention, which is here presented in its theorical structure—could boost their awareness and ability to manage their privacy preferences.

These considerations resonate with the recent findings that interventions based on relational disclosure – such as studies investigating the functioning and effectiveness of recommending systems in the streaming services market[46] – can help to increase people's subjective understanding regarding data processing activities, as well as the impact on their willingness to disclose personal data.

On the basis of this preliminary theoretical framing, future research should first and foremost explore the adaptability of contextual disclosures to heterogeneous frameworks for data processing that can be observed in the digital environment: different services might indeed require different modes of disclosure, to be developed according to the relational paradigm. At the same time, and building on the foundations of Social Cognitive Learning Theory,[47] additional analyses should inspect the cognitive mechanisms underlying the functioning of relational decision-making. Lastly, in order to move from conceptual and experimental evidence to an actual policy proposal, further investigations – beyond the overview provided in this paper – exploring the regulatory margins for such a system to be implemented seems advisable.

Waiting for these developments, our research attempts to shed a light – considering evidence emerging from studies and experiments – on the fact that consent in data processing is not only (and often) partially irrational, but also inherently relational, in order to provide a first conceptual basis that can inform future interventions aiming at enhancing data subjects' understanding regarding the modes and functioning of data processing phenomena

[46] See A. Davola, I. Querci, S. Romani (n 33).
[47] See *supra* (n. 31).