CHANGES IN THE LEGAL SPHERE: RETHINKING TRANSPARENCY

*Michele Cozzio**

Abstract

The development of digital technologies and networks is changing social and economic frameworks with repercussions that involve the entire legal sphere. The changes will affect whole systems of models and rules and will lead to processes of legal evolution. The effects of these transformations are viewed from the perspective of transparency with respect to relationships; be they interpersonal, contractual or with the public authority. There are instances where, due to their complexity, the mechanisms and workings of these new technologies are unknowable to the legal systems whose job it is to maintain the changing needs for protection, especially when these technologies affect the more important aspects of public life. In this new digital landscape, the need to guarantee fundamental rights and freedom (*in primis* the dignity and right to self-determination of the individual) gives transparency renewed importance, to the point that it may be necessary to reevaluate its role in the ambit of common goods. In this context, with the analysis of various approaches, we would like to offer some subjects for reflection and suggest some paths of research that could be followed using legal and other instruments.

TABLE OF CONTENTS

* Contract professor, University of Trento.

1. Digitalization of society and pervasiveness of the changes

The 1970s marked the end of the industrial society and the start of the *information society*[1]. The latter of the two is characterized by the production non-material goods and the increasing ease with which they can be transferred.

Over the same period, innovation in information technology[2] together with the rapidity of its diffusion on a global scale started a second wave of changes. These changes quickly affected all social and economic aspects of society[3]. Today the convergence of three powerful technological trends is dictating

[1] The expression stems from the *post-industrial society*, concept developed (1973) by Daniel Bell, sociologist, professor at Harvard University (*The Coming of Post-Industrial Society: A Venture in Social Forecasting* (1973)). With the Information Society we refer to a vision of post-industrial society, in which the technological and information paradigm prevails, with the production of non-material services and the infrastructures for their distribution. See also N. Elkin-Koren, N. Weinstock Netanel (ed.), *The Commodification of Information* (2002); G. Sirilli, *Società dell'informazione*, in *Enciclopedia della Scienza e della Tecnica*, Vol. VIII, 422 (2008); V. Zeno-Zencovich, *Diritto di informazione e all'informazione*, in *Enciclopedia Italiana*, *XXI Secolo, Norme e idee*, 301 (2009), the Author shows the defining characteristics of the information age: the availability of information, its circulation the use made of it and the importance this has on society.

[2] This refers to the advent of the personal computer and later, with the development of the World Wide Web, to social networks, mobile devices (so-called web 2.0), the cloud, artificial intelligence and the emergence of the digital economy(cd. web 4.0). See IT Media Consulting, ASK Research Center by Bocconi University, *L'economia dei dati. Tendenze di mercato e prospettive di policy* (2018), available online; L. Floridi, *The Fourth Revolution. How the Infosphere is Reshaping Human Reality* (2014).

[3] J. Tirole, *Économie du bien commun* (2016) highlights that the digitalization of society is governing the economic and social changes of the XX1century and reforming every aspect of human activity; R. Baldwin, *The Great Convergence. Information Technology and the New Globalization* (2016). See also European Commission, *A Digital Single Market Strategy for Europe*, COM/2015/192 and the accompanying Commission staff working document, *Analysis and Evidence*, SWD/2015/100, which contains the references for the factual information and more detail on the nature of the challenges addressed and evidence in support of the EU strategy. See, more in general, European Commission, *Towards a Thriving Data-Driven Economy*, COM/2014/442; Id., *Digitising European Industry Reaping the full benefits of a Digital Single Market*, COM/2016/180; Id., *Building a European Data Economy*, COM/2017/9; Id., *Towards a Common European Data Space*, COM/2018/232; IDC, Open Evidence, *European Data Market. Final Report* (2017). For a particular perspective see A. Baricco, *The Game* (2018).

how society develops: (i) internet and access to information, (ii) mobile devices with networks that offer permanent and ubiquitous connectivity, (iii) *cloud computing* with its computational power and dislocated distribution. Information, connectivity and computational power are showing themselves to be the principal sources of production of our times. As well as their convenience, access to them is becoming ever cheaper and they exist without territorial or physical limitations.

The after-shocks of these events are easily demonstrated: just in the European Union the digital transformation of manufacturing industry is expected to bring "benefits" worth euro 1.250bn by 2025[4]; in England business in the Sharing Economy is expected to grow by 60% by 2025 (euro 140bn. p.a.)[5]; already by 2020 90% of all jobs will require basic digital skills[6]. The biggest effects will be in the USA and even more so in South East Asia where the greatest use of digital technology is concentrated[7].

---

[4] Science and Technology Options Assessment (STOA), *Ethical Aspects of Cyber-Physical Systems. Scientific Foresight study* (2016), Annex 1, 36, and there the references, available online.

[5] R. Vaughan, R. Daverio, *Assessing the size and presence of the collaborative economy in Europe* (2016), study for European Commission (DG GROW); IDC, Open Evidence, *European Data Market*, cit.; IT Media Consulting, ASK Research Center by Bocconi University, *L'economia dei dati*, cit. at 71-92; see also M. Naldi, *Prospettive economiche dell'Intelligenza Artificale*, in F. Pizzetti (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione* (2018).

[6] European Parliament resolution of 16 February 2017 with *recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103)(INL); also EP resolution of 12 February 2019 *on a Comprehensive European Industrial Policy on Artificial Intelligence and Robotics* (2018/2088)(INI); McKinsey Global Institute, *Disruptive technologies: Advances that will transform life, business, and the global economy* (2013). See also the proposal for an European Regulation regarding *the Digital Europe Programme for the period 2021-2027*, COM/2018/434. The proposal aims to provide a spending instrument that is tailored to reinforcing Europe's capacity in high performance computing, artificial intelligence, cybersecurity, advanced digital skills, ensuring their wide use across the economy and society. The financial envelope for the implementation of the Programme shall be euro 9,194 billion (art. 4).

[7] See the report *Digital in 2019. Essential Insights Into How People Around The World Use Internet, Mobilke Devices, Social Media, and Ecommerce*, Jan. 2019. The data comes from 239 States and are based on information taken from the *GlobalWebIndex*, *GSMA Intelligence*, *Statista*, *Akamai*, *Google*, *StatCounter*, *Ericsson*, https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338; Accenture Institute for High Performance, Oxford Economics, *Digital Density Index. Guiding digital transformation* (2015).

The force and rate of change are overwhelming and it is difficult to grasp the scale, in its entirety, of the effects of these developments. It is not even easy to understand what social changes they have already brought[8] both with respect to personal relations (especially those to do with privacy and the diffusion of personal information) and with respect to other established aspects of society.

Such dynamism will inevitably have repercussions on the whole legal system: where notions, taxonomy, and whole classifications that, although consolidated, will need to be rethought. New methods will have to be formulated to deal with new issues and new models developed to cover social and economic changes.

Furthermore, what characterizes these changes is the rapidity with which they occur.

The speeding up of social and economic life (and with it the need for new rules, "*donc le droit s'est mis à courir*")[9] due to technology, is one of the defining factors of modern culture[10]. In the past, the evolution of legal systems was the result of slow processes with changes occurring over generations. Now, in the space of a few years, we see revolutionary systemic changes not just in systems and models but also in specific legal solutions.

They are processes that don't follow predefined patterns and schemes, and are not synchronized between them[11].

There are sectors where these changes happen sooner and with greater effect. Notably those with a higher level of

[8] T. Hylland Eriksen, *Overheating. An Antropology of Accelerated Change* (2016); see also M. Hindman, *The Internet Trap. How the Digital Economy Builds Monopolies and Undermines Democracy* (2018).

[9] F. Ost, *Le temps virtuel des lois postmodernes ou comment le droit se traite dans la société de l'information*, in J. Clam-G. Martin (ed.), *Les transformations de la regulation juridique* (1998); see also P. Gérard, F. Ost, M. Van De Kerchove (ed.), *L'accélération du temps juridique* (2000).

[10] H. Rosa, *Alienation and Acceleration: Towards a Critical Theory of Late-Modern Temporality* (2010).

[11] With reference "alla complessità come dimensione normale della giuridicità contemporanea" (to "complexity being a normal feature of contemporary lawmaking") see A. Gambaro, *Le fonti del diritto inglese. Riflessioni a margine della rinnovata edizione di un classico della letteratura comparatistica italiana*, in *Annuario di diritto comparato e di studi legislativi 2017*, 881 (2017); *ibidem* P. Rossi, *Le ambivalenze della globalizzazione giuridica: diversificazioni giuridiche e pervasività dell'informazione*, 499.

technological input are more dynamic and are subject to models and rules which soon become obsolete. These therefore are the most interesting areas on which to experiment new legal models, rules and solutions.

To take a few examples, there is *Facebook*, accessible from most devices, it started at the beginning of the Millenium and after only a few years it had 2 billion users with over 45 billion messages being exchanged daily[12]. Then there is Google, with all its services, (*Google*, *Android*, *YouTube*, *Gmail*, *Google Maps and other services*) which has grown, in fifteen years, to be the highest value company in the world. Just as impressive are the commerce platforms such as *eBay*, *Amazon* and *Alibaba* in Asia, which had the biggest ever share flotation at US $ 25bn[13]. Finally, in general 90% of internet services supplied by search engines, social media, electronic commerce, *app store*, etc. have only been present since 2013[14].

These impressive numbers, although significant, do not really illuminate us as to the capacity of these instruments to redefine the social, economic or legal aspects of society.

The possibilities that they offer to transmit and receive data and information in any place instantly have changed and continue to change behavior, habits and attitudes: a typical example is the way that the differentiation between peoples' public life and private life is disappearing.

The unpredictable and paradoxical results of this are succinctly described in the expression *vetrinizzazione sociale* (*social showcasing*)[15]. This reflects the way in which every aspect of the

---

[12] Facebook as with other social networks is a technological platform which allows people to show themselves, with names, and their photos, their tastes, their friends, the events they are invloved in and the groups they are part of. In January 2007 Facebook and its subsiduaries *Instagram*, *WhatsApp* e *Messenger* registered a total of 4,37 billion users (report *Digital in 2017. Global Overview. A collection of Internet, Social Media, and Mobile Data from Around The World*), in January 2019 just the Facebook platform revealed that it had 2.271billion (report *Digital in 2019*, cit. at 9).

[13] P. Erisman, *Alibaba's World* (2015). For a global overview of the e-commerce markets, see https://www.remarkety.com/global-ecommerce-trends-2016, published June 18, 2017.

[14] European Commission, *A Digital Single Market Strategy for Europe*, cit. at 3.3.1.

[15] V. Codeluppi, *La vetrinizzazione sociale. Il processo di spettacolarizzazione degli individui e della società* (2007).

life of a person (physical, mental, public, private etc.) is subjected to the need to be posted and shared[16]. So too with sexuality which has, in many cultures, always been the strongest most solid and reliable of human ties and which represents the area of secret intimacy and greatest discretion[17].

No less is the shock wave that has overwhelmed the sector that controls, moves and uses the data regarding habits, behavior and personal tastes. This is due to the massive growth in the number of sources (tens of billions by 2020)[18] not only generating but transmitting data through the digital world coupled with the increase in computing power needed to assimilate and elaborate it into usable information[19].

The technological advances highlight the difficulties that regulatory models (and most in general, the legal formants) have in attaining the internationally[20] shared goal of ensuring that everyone has the right to control the flow of their own private data and information[21].

---

[16] J. Palfrey, U. Gasser, *Born Digital. Understanding the First generation of Digital Natives* (2008). See also Z. Bauman, D. Lyon, *Liquid Surveillance. A conversation* (2013), the Authors state that for the new generations social networks are the normal way to define their identity and their *status*; M. Aime, A. Cossetta, *Il dono al tempo di internet* (2010).

[17] A. Giddens, *The Transformation of Intimacy. Sexuality, Love, and Eroticism in Modern Societies* (1992); P. Paul, *Pornified. How Pornography Is Damaging Our Lives, Our Relationships and Our Families* (2005); B. McNair, *Striptease Culture. Sex, Media and the Democratisation of Desire* (2002).

[18] IT Media Consulting, ASK Research Center by Bocconi University, *L'economia dei dati*, cit., 47-48.

[19] See V. Mayer-Schönberger, K.N. Kenneth, N. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (2013).

[20] See *Fair Information Practice Principles* (FIPPs) elaborated in the U.S.; OCSE, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, published in 1980 and revised in 2013; Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, no. 108 in 1981. In the UE the protection of personal data is a fundamental right (art. 8, para. 1, *Charter of Fundamental Rights of the European Union*; art. 16, para. 1, *Treaty on the Functioning of the European Union*).

[21] See G. Pascuzzi, F. Giovannella, *Dal diritto alla riservatezza alla computer privacy*, in G. Pascuzzi (ed.), *Il diritto dell'era digitale* (2016). The authors observe that the digital revolution has brought changes to the notion and content of the right to privacy: no longer the right to be left alone but the right to control ones own information. See also B. Schermer, *The Limits of Privacy in Automated Profiling*, 1 *Computer L. Sec. Rev.* 27, 45-52 (2011); L. Floridi (ed.), *Protection of*

In particular what emerges are the inadequacies of the solutions of the two main legal systems. The European system with its laws and decrees based on personal data protection and the US system with its greater emphasis on a free market with less rigorous legislation.

The inadequacies show themselves not just in specific solutions but in the whole architecture on which these two systems are built, which is centered around the definition of what is personal data and the protection of its owner[22].

As already mentioned there is a tendency to share personal information (private or not) voluntarily on social media via mobile devices (smart… -phone, -watch, -car, -glasses, etc.) added to this is the *Internet of Things* (*IoT),* machines with their own connections to the web. These all generate enormous and growing amounts of data (*Big Data*) that can be stored and processed. Using psychometric and re-identification techniques this data can then be used to gather information disseminated around the web in order to build a personal profile that can be used to predict and manipulate the behavior of individuals or groups. All this can be done in the space of milliseconds[23].

---

information and the right to privacy. A new equilibrium? (2014); A. Tamò-Larrieux, *Designing for Privacy and its Legal Framework. Data Protection by Design and Default for the Internet of Things* (2018); F. Pizzetti (ed.), *Intelligenza artificiale, protezione dei dati personali e regolazione* (2018).

[22] One of the first academics to hypothesize the need to give up some types of definitions of personal data see P. Ohm, *Broken promises of privacy. Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010). For some of the Italian authors on this subject, see A. Principato, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, 1 *Contratto e impresa / Europa* 197-229 (2015); A. Mantelero, *Riforma della direttiva comunitaria sulla* data protection *e* privacy impact assessment*, verso una maggiore responsabilità dell'autore del trattamento?*, 1 *Dir. inform.* 145-153 (2012); R.Ducato, *La crisi della definizione di dato personale nell'era del web 3.0*, in F.Cortese, M.Tomasi (eds.), *Le definizioni nel diritto* (2016); A. Mantelero, *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, 1 *Contratto e impresa / Europa* 141 (2015); R. Caso, F. Giovanella (eds.), *Balancing Copyright Law in the Digital Age. Comp. Persp.* (2015).

[23] W. Christl, S. Spiekermann, *Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (2016). See also A. Mantelero, G. Vaciago, *The "Dark Side" of Big Data: Private and Public Interaction in Social Surveillance*, 1 Computer L. Rev. Int'l 161-169 (2013); A. Greenfield, *Radical Technologies. The Design of Everyday Life* (2017); E. Pellecchia, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità*

In spite of warnings from accademics (Lessig, Bauman, Lyon, Rodotà et al.), alarmist press articles on leaks (*Datagate* with Edward Snowden, Cambridge Analytica and Facebook) and cinema dramatics; the outlines of a consolidation, at juridic levels, is emerging, with Court decisions and orders from regulatory bodies being pronounced. (CJUE, C-362/14, *M. Schrems*; EC n. 39740/2017, *Google Search*; Commission Nationale de l'Informatique et des Libertés n. 1/2019 *Google LLC*; Supreme Court of Canada 34/2017, *Google Inc. v. Equustek Solutions Inc.*).

Most of the changes, moreover, do not have well defined boundaries and even established definitions are being overwhelmed. If we consider the subject of property law (goods & assets), which is one of the most important legal areas, we note that the impact of the new technologies is calling into question not just taxonomic classifications but whole areas of the complex and structured theory of property. The reasons can be traced to the emergence of economies based on intangible (digital) goods. This aspect - intangibility - has been recognized and valued even in the remotest of civilizations (e.g. *res incorporales)* but no one ever imagined that it could attain the potential value that it has today.

The consequences are many and nearly always more complicated than most discussions would lead us to believe. Just think of the property law models that cover "existing material goods that have been digitized (dematerialized)" as well as new models that cover "those (digital goods) that did not exist before" [24].

Other questions arise from the link between intangible goods and knowledge as a common good[25], especially when

dell'algoritmo nella cornice della responsable research and innovation, 5 Le nuove leggi civili commentate 1209-1223 (2018); T. Cerquitelli, D. Quercia, F. Pasquale (eds.), *Transparent Data Mining for Big and Small Data* (2017); M. Moore, D. Tambini (eds.), *Digital Dominance. The Power of Google, Amazon, Facebook, and Apple* (2018). With a sociological approach, for all D. Lyon (eds.), *Surveillance as Social Sorting. Privacy, Risk, and Digital Discrimination* (2003); Id., *Surveillance Studies: An Overview* (2007), where the Author defines the concept of "surveillance in the digital age".

[24] A. Gambaro, *I beni*, in A. Cicu, F. Messineo, L. Mengoni (eds.), *Trattato di diritto civile e commerciale* (2012).

[25] Knowledge meant as "*la risorsa fondamentale ai fini delle produzioni più avanzate e quindi la risorsa sia individuale che collettiva più importante ai fini dello sviluppo*", A. Gambaro, *I beni*, cit. at 36-37.

trying to identify which property law frameworks apply (eg. copyright law or open source law). This may lead to an overhaul in the way we think about and how we discipline the subject of property[26].

The protection offered by the legal system for intellectual property is based on the need to encourage authorship and invention. This view, however, has been shaken by the processes of digitalization (dematerialization) which now allow for this new property to be copied and transmitted at practically no cost. This makes it difficult for any author or owner to enjoy the full rights to their ideas.

This has led to enormous[27] increases in the levels of legal protection through the widening of the categories to be protected as well as extensions to the scope and period of protection. The result is reduced societal benefits from work and this is hard to justify considering the whole point of protection is to incentivize intellectual creativity.

In spite of this increased protection it has become obvious that the traditional ideas of property are inadequate in dealing with knowledge whose creativity derives from processes with undefinable structure and incremental modifications and whose value increases every time it is shared[28]. Knowledge, defined as the result of a continuous accumulation of knowhow, is a collective work (often funded by the collective) and defined as a *relational common*[29]. From this perspective, the right to ownership in its traditional and protectionist form is more expropriative than

---

[26] A. Gambaro, *I beni*, cit. at 1-58; Id., *I beni immateriali nelle riflessioni della Commissione Rodotà*, in Mattei U., Reviglio E., Rodotà S. (eds.), *I beni pubblici. Dal governo democratico dell'economia alla riforma del codice civile* (2010).

[27] A. Pradi, *I beni comuni digitali nell'era della proprietà intellettuale*, in A. Pradi, A. Rossato (eds.), *I beni comuni digitali* (2014).

[28] U. Mattei, *voce Proprietà (nuove forme di)*, in *Enc. Dir.*, (2013). In Italy the subject was debated as part of the proposal to reform the Civil Code in 2017; see U.Mattei, E.Reviglio, S. Rodotà (eds.), *I beni pubblici*, cit., and also U.Mattei, E.Reviglio, S. Rodotà (eds.), *Invertire la rotta. Idee per una riforma della proprietà pubblica* (2007). See also D. Bollier, *Think Like a Commoner. A Short Introduction to the Life of the Commons* (2014).

[29] C. Hesse, E. Ostrom (eds.), *Understanding Knowledge As a Commons* (2007). See also Y. Benkler, *The Wealth of Networks. How Social Production Transforms Markets and Freedom* (2007); M. Nielsen, *Reinventing Discovery: The New Era of Network Science* (2012).

encouraging[30]. With this in mind it is easy to foresee that, legal structures have to will evolve to recognize the value not just of exchange but of more inclusive behaviors such as sharing and the encouragement of social input.

Successful social practices have been developed in order to "give back" to knowledge its social value. Referring to *open* solutions (*open access*, *open sources*, *open data*) the tragedy of the commons is not sufficient to justifiy copyright based legal models: it is the open or shared models which, today, are more prevalent[31].

It is not single innovations, but the entire digital environment, that affects the legal world especially with regards to transparency.

Any computer-generated work is a result of running programs (*software*) to which may be applied either traditional copyright models or open source models. We have already discussed the limitations of the former but the latter also have their problems when it comes to transparency.

Open source systems, which allow access to and the reuse of source codes, do not guarantee total transparency to all those involved in their use (how many of us are able to understand a source code or its workings and impact?)

So, *open source* is transparent to few but even for them, understanding the lines of code, of a program, does not necessarily help to understand the logic behind its applications or the derived results[32]. At least these processes should be rendered transparent, especially when they affect the lives of individuals or society.

Data analysis is becoming ever more automated with the use of machine learning. Programs are continuously acquiring not just data but knowledge giving them the capacity to make and act on decisions without human intervention. In this case it should be possible to have guarantees of continued transparency or at least to have a clear idea of the range of behavior or activity of any

[30] U. Mattei, *voce Proprietà (nuove forme di)*, in *Enc. Dir.*, cit.; Id., *Beni comuni. Un manifesto* (2011).

[31] F. Capra, U. Mattei, *The Ecology of Law. Toward a Legal System in Tune with Nature and Community* (2015).

[32] E. Pellecchia, *Profilazione e decisioni automatizzate*, cit. at 1218. See also J. A. Kroll, J. Huey, S. Barocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson, H. Yu, *Accountable Algorithms*, 165 U. Pennsylvania L. Rev. 633 (2017).

program (starting with the limits on learning imposed, from the start, on the machines by the programmers)[33].

These programs run on servers (maybe thousands of servers all working in parallel, their distributed locations being based on network needs and not on specific geographical ties) so they are physical entities subject to traditional rules of ownership or profit. Moreover, the derived results are often based on methods and systems developed at Universities or other academic bodies and easily accessed from published work (an example is the theory of the Big Five personality traits)[34]. Results are often obtained by programs using millions of bits of data which have been depersonalized, this makes it difficult to prove that the rights of the individual have been infringed.

In many cases the changing technology requires the legal world to adapt its approaches and its solutions but in other cases whole new practices are required: a few examples would be autonomous vehicles (including drones), production robots, machines used in medicine and social assistance, bioengineering, artificial intelligence and automated contracts (smart contracts and other blockchain based solutions).

All this, highlights a liquid environment for which the jurist will have to equip himself with the capacity to capture the trajectories and changes in direction necessary to develop new models, rules and solutions or adapt existing ones in ever shorter time frames.

2. Transparency as a key to understanding the changes

These technological changes will be analyzed from the perspective of transparency by evaluating the effects on the meanings, the contents and the significance of transparency,

[33] See E. Pellecchia, *Profilazione e decisioni automatizzate*, cit. at 1219; see also A. Greenfield, *Radical Technologies*, cit. at 214 ss.; M. Laukyte, *An interdisciplinari Approach to Multi-Agent Systems: Bridging the Gap Between Law and Computer Science*, 1 Informatica Dir. 223-241 (2013); P. Domingos, *The Master Algorithm. How the Quest for the Ultimate Learning Machine Will Remake Our World* (2015).

[34] R.R. McCrae, O.P. John, *An introduction to the five-factor model and its Applications*, 60 J. Personality 175-215 (1992); R. McCrae, P.T. Costa, *Personality in Adulthood, A Five-Factor Theory Perspective* (2002).

especially when dealing with interpersonal relationships, contractual matters and with public authorities.

The choice of this perspective is based on the fact that, for the most part, these changes produce effects that do not show the mechanisms by which they work, the logic used to guide their function nor the people who operate them (public or private) and stand to profit from them[35].

This is a good reason and an opportunity to study the changes in the light of transparency.

Transparency meant as the *condition to know*. It allows one to know that which is not visible or that which is not wished to be visible. We can associate transparency with that which surrounds or goes into a product, object, fact or event and determines how knowable or unknowable (secret) that object is.

2.1. (*Follows*) in interpersonal relation

In the area of interpersonal relations, the changes brought about by technological evolution have a particularly significant impact on the cession, distribution, manipulation and production of personal information.

These activities have been totally interconnected thanks to the internet. Data is ceded by users to websites to use the service (socially or commercially), they are immediately distributed to intermediaries where they are collected, processed and eventually put on the market. All this happens continuously and in the space of a few milliseconds, with revolutionary effects on the value chain of the traditional economies. However, this brings critical issues to the legal world that need careful evaluation.

The legal framework of reference here, is that on the control and protection of personal data.

The solutions, adopted in the principal models, makes the distinction between two types of data. The first are directly about individuals, their activities and their identities. The second are not about individuals but are linked to events, statistics, economics,

[35] F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information* (2015); A. Greenfield, *Radical Technologies*, cit. at 214-264; A. Tabarrok, *The Rise of Opaque Intelligence*, Marginal Revolution at February 20, 2015; E. Parisier, *The Filter Bubble. What The Internet Is Hiding From You* (2012); M. Hindman, *The Internet Trap*, cit. (2018); S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli* (2014).

metrics etc. On the first people can claim title and treat them as extensions of their personality/character, a condition that usually allows them to control, cede and oppose any action on them by third parties.

The protection given by the principal legal systems is based on the classification of data (eg. are they in the public domain, quasi personal or personal) and according to this measure there are different levels of consent that individuals must give before data can be ceded, distributed or processed.

At the moment of giving consent, transparency is considered to be instrumental in the protection of an individual's data. This transparency is guaranteed by rules that govern the formats and modes used when giving consent and is usually done at the first cession. The solutions used by the main legal systems (UE, US, Canada, etc.) tend to be the same as those used in contractual matters (*infra* § 2.2.) which assure informed consent from those who give their data. Transparency should therefore be guaranteed by the knowledge that a person acquires, on the use that will be made of their data.

The new EU rules - Regulation (EU) 2016/679, General Data Protection Regulation (GDPR)[36] - use this model based on disclosure regulation and on consent. In the initial recitals, it is clear that the way in which personal data is collected, processed and used should be transparent.

The principle of transparency also requires the subject to be informed as to who is processing their data and to what ends. It also requires that information and any communication pertaining to its processing "shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language"[37]. The choice is

[36] Regulation (EU) 2016/679 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data - General Data Protection Regulation* (in O.J.E.U. n. L 119 del May 4, 2016) enter in force on May 28, 2016. It shall apply from 25 May 2018. See G. Finocchiaro, *Introduzione al Regolamento Europeo sulla protezione dati*, 1 Le nuove leggi civili commentate 1 (2017); F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, 1 Le nuove leggi civili commentate 369 (2017); I. Kroener, D. Wright, *A Strategy for Operationalizing Privacy by Design*, 5 Info. Soc'y 355-365 (2014); E. Tosi (ed.), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy* (2019).

[37] Recital n. 39, artt. 12, 13 e 14, Regulation (EU) 2016/679.

rigorous: consent must come from an unequivocal and affirmative action, expressed as a truly free, specific and informed choice. There must also be no possibility of using inactivity, silence or solutions such as prefilled information fields as a way to gain consent[38].

When the duty to inform is neglected the protection afforded by the law is also very rigorous.

In fact, in the case of harm or damage, whether material or intangible, the controller or the processor for the data processing are held responsible, unless they can demonstrate that the damaging event was in no way attributable to them[39].

The criteria used to evaluate this responsibility refer to, on the one hand, the duty, for those who process data, to set up appropriate and effective measures of protection and validate their effectiveness and on the other hand (more generally) to demonstrate that their processing activities conform to the objectives of the regulation[40].

Other criteria are used, case by case, where the scope of the application, the context, the end use and the risk to personal liberty and rights must all be taken into account[41]. In this way, the burden of installing effective measures and carrying out risk analyses lies with the data processors etc. This burden can be seen as an expression of the principle of *good faith* in an objective sense.

This choice of responsibility offers high levels of protection. Furthemore, by including it in legislation (with an EU Regulation),

---

[38] The legal model used by the European regulation is based on the informed consent by the data subject: having received the necessary information the responsibility for the choices made falls to the data subject, a bit like saying that with the information you have, you are in a condition to make a responsible and informed decision; see different opinion by B. Goodman, S. Flaxman, *European Union regulations on algorithmic decision-making and a "right to explanation"*, 3 I Magazine (2017).

[39] Art. 82, par. 1 e 2, Regulation (EU) 2016/679.

[40] Recital n. 74, Regulation (EU) 2016/679.

[41] Recital n. 75 lists, by way of example, some of the risks that need to be evaluated. Such examples may refer to analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles or where processing involves a large amount of personal data and affects a large number of data subjects. See also A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679*, 1 Le nuove leggi civili commentate 144 (2017).

it shows the will to ensure the same level of protection in all the EU member States[42] and beyond[43].

When it comes to regulatory models of informed consent there are at least two critical issues with the transparency that derive from the technology.

(I) The first issue is to do with the level of knowledge that can be guaranteed after the first cession of personal data.

Consider a recent case at the European Court of Justice (15 Mar. 2017, C 536/15) where it was established that the phone companies who assign subscribers numbers cannot refuse to give them to businesses from other member states when requested.

The consent to publish data, given at the *first cession*, allows other transfers of data without the need for further consent[44].

The case, in itself, is not a complex one but it demonstrates a little-known aspect of informed consent; that the longer the chain of transfers is the more difficult it is to know, and thus to guarantee, where, what, and how the data will be used. In other words, the knowledge guaranteed at the first cession diminishes as the number of transfers increases. Added to this is the time

---

[42] See recitals from 10 to 13, Regulation (EU) 2016/679.

[43] European Regulation (EU) 2016/679 also applies to data processing carried out by companies outside the EU, when it concerns the supply of goods or services to residents in the Union, as well as the monitoring and control of their behavior. The European levels of protection in the processing of personal data therefore apply irrespective of the geographical location of the data controller. See S. Ricciardi, *Il nuovo regolamento europeo sulla protezione dei dati personali: il punto di vista di Microsoft*, 3 Contratto e Impresa /Europa 4 (2013).

[44] Judgment of the Court, Second Chamber, of 15 March 2017, C-536/15, *Tele2 (Netherlands) BV and others*, ECLI:EU:C:2017:214. See E. Adobati, *Reti e servizi di comunicazione elettronica : il consenso prestato dagli abbonati per l'inserimento in un elenco nazionale vale per l'inserimento in elenchi in tutta l'Unione europea*, 1 Dir. com. scambi internaz., 358 (2017). See also the judgment of the Court, Grand Chamber, of 6 October 2015, C-362/14, *M. Schrems*, ECLI:EU:C:2015:650, with many notes on academic writings, e.g. A. Mantelero, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per i cittadini ed imprese?*, 2 Contratto e impresa / Europa 719-733 (2015); R. Ferrario, *Lo EU-U.S. Privacy Shield. Una risposta insufficiente alle richieste della Corte di giustizia dell'Unione europea nella sentenza Safe Harbour?*, 3 Dir. Comm. Internaz. 635-650 (2017); G. Scarchillo, *Dal Safe Harbor al Privacy Shield. Il trasferimento di dati personali verso gli Stati Uniti dopo la sentenza Schrems*, 4 Dir. Comm. Internaz., 901-941 (2016); S. Carrera, E. Guild, *The End of Safe Harbor: What Future for EU-US Data Transfers?*, 22 Maastricht J.Eur. Comp. L. 651-655 (2015).

dimension, in that the transfers and processing practically happen in real time.

The duty to communicate, to the original data subject, further transfers of their information to third parties seems not to be the full solution[45], given the rapidity, frequency and number of parties involved.

Researchers in Germany found that of over 21 million websites pages visited 95 % of them monitored and transferred information to third parties[46]; another study of a million web sites found that there were 80 thousand "third parties" to whom information, relative to the visit, was transferred[47]. It is estimated that, on average, every time a subject visits a website or uses an application the information is transferred not only to the publishers of the software but to 30 third parties. This is discussed in detail in a report by W. Christl and S. Spiekermann *Networks of Control*[48] where they highlight that "users are often not aware of how many companies receive information about their everyday lives, and that our knowledge about how apps collect data and transfer it to third parties is limited, incomplete, and often outdated" (p. 52). In other words, "as data brokers often share data with others, it is virtually impossible for a consumer to determine how a data broker obtained their data (…) most consumers have no way of knowing that data brokers may be collecting their data" (p. 121-122).

We can add that if the amount of data that an individual releases online, with consent, is immense then the quantity of data or meta-data that is released unknowingly is just as impressive.

An example is the movement sensor in smartphones. This shows where we go, with what frequency and how fast we travel... all information that allows organizations to build a

[45] European Regulation (EU) 2016/679 establishes certain information obligations in case of transfer of personal data to third parties (artt. 3, 12-14, 44-50).

[46] Y. Zhonghao, S. Macbeth, K. Modi, J.M. Pujol, *Tracking the Trackers*, in *proceedings of the 25th International Conference on World Wide Web (IW3C2)*, 11-15 aprile 2016 at Montreal, 121-132.

[47] N. Arvind, D. Reisman, *The Princeton Web Transparency and Accountability Project*, in T. Cerquitelli, D. Quercia, F. Pasquale (eds.), *Transparent Data Mining for Big and Small Data*, cit. at 45-57.

[48] W. Christl, S. Spiekermann, *Networks of Control*, cit. at 45-52.

personal profile (emotional stability/instability) of every one of us.

(II) The second issue has to do with the level of knowledge that can actually be guaranteed to the data subjects about the data processing, the results that can be obtained and on the possible repercussions of these activities.

The actions, on data, of these technologies is characteristically "*continuous*", "*ubiquitous*", "*invisible*" and "*pervasive*"[49] and it is no surprise that this processing is done unbeknownst to the subjects. It is untraceable and without any transparency.

As an example, the data given to social media platforms (name, address, postcode email, etc.) are processed to the point where they can identify the devices (phone, computer, appliances and anything connected to the web or held in digital memories or databases) linked to that information, allowing an intimate knowledge of the people who use them[50]. From then on, the "digital" life of that data is constantly monitored. This example is one of many but the results are always the same: use the data to measure, group, predict and advertise to the individual whose data it is. These operations allow this to be done continuously and instantaneously (e.g. *real time bidding*).

During the processing stage, information and data can flow in separate packages, they are then aggregated to other information and processed by algorithms able to conduct sophisticated analyses of behavior, preferences and opinions of individuals or groups.

These effects are well summarized in the widely cited academic paper *Computer-based personality judgments are more*

---

[49] W. Christl, S. Spiekermann, *Networks of Control*, cit. at 118. The authors highlight that "Consumers are often neither aware of what personal information about them and their behavior is collected, nor how this data is processed, with whom it is shared or sold, which conclusions can be drawn from it, and which decisions are then based on such conclusions. Both dominant platforms and smaller providers of websites, services, apps and platforms - generally speaking - act in a largely non-transparent way when it comes to the storage, processing and the utilization of personal data" (at 122).

[50] W. Christl, S. Spiekermann, *Networks of Control*, cit. at 94-116, describe the monitoring techniques carried out by companies such as: Oracle, Acxiom, Experian, MasterCard, LexixNexis, etc.

accurate than those made by humans[51]. In 2012 the Author demonstrated that with on average of 68 "likes" on Facebook it is possible to deduce the skin colour (with 95% accuracy), sexual inclination (with 88% accuracy) and political preference between Democratic or Republican party (with 85% accuracy) of a user. Other attributes that can be deduced are IQ, religious faith, use of alcohol, cigarettes and drugs etc. In 2015 the author showed that with 150-300 clics it is possible to know a person better than their friends, partners or parents know them. Advances in psychology, neuroscience and psychometry combined with computational power all lead to results that are cause for reflection

Personal profiles, shopping habits and opinions are all reconstructed by the "lords of data"[52] making it possible to predict and orientate the choices of individuals, groups, companies and public authorities[53]. The applications are many with socio-economic implications which, in the absence of adequate regulation and effective protection, can lead to discrimination[54]

---

[51] W. Youyou, M. Kosinski, D. Stillwell, *Computer-based personality judgments are more accurate than those made by humans*, 4 proceedings of the National Academy of Sciences 1036-1040 (2015); see also M. Kosinski, Y. Wang, H. Lakkaraju, J. Leskovec, *Mining Big Data to Extract Patterns and Predict Real-Life Outcomes*, 4 Psychological Methods 493-506 (2016); R. Lambiotte, M. Kosinski, *Tracking the Digital Footprints of Personality*, 12 proceedings of the Institute of Electrical and Electronics Engineers 1934-1939 (2014).

[52] A. Mantelero, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, 1 Dir. Inform. 135 (2012) highlights the fact that the power to control this data is in the hands of a small group of people who weald such power over information that they evoke the idea of being the "*lords of data*". See also I. Graef, *When Data Evolves into Market Power. Data Concentration and Data Abuse under Competition Law*, in M. Moore, D. Tambini (eds.), *Digital Dominance*, cit. at 71-97; L.S. Morais, *Competition in Digital Markets and Innovation. Dominant Platforms and Competition Law Remedies*, in G. Colangelo, V. Falce (eds.), *Concorrenza e comportamenti escludenti nei mercati dell'innovazione* (2017); M. Andrejevic, *The Big Data Divide*, 8 Int'l J. Comm. 1673-1689 (2014); M. Hindman, *The Internet Trap*, cit. at 203.

[53] These are operations of *mass personalization* including *instant personalization, predictive marketing, personalized pricing, dynamicprincing and election campaigns*, etc.; W. Christl, *Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* (2017).

[54] Amongst the most relevant : differences in price and scope, limits to access to insurance, health, financial and career services, presenting things out of context; see D.J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (2004). See also O. Lynskey, *The Power of Providence: The Role of Platforms in*

and manipulation with subsequent risks to security, secrecy, independence of thought, and market manipulation.

These issues have not escaped the attention of Institutions and Authorities at an international level[55] but the regulatory answers in spite of being strengthened (eg *privacy by design*, *privacy by default*, international cooperation, giving authorities greater powers, etc.), are finding it hard to cope[56].

More generally, the data circulation and processing phases seem to have remained on the margins of regulatory activity. Yet these are the areas of greatest impact and where transparency (and its guarantee) is practically absent. What is emerging, in particular, is a need to consider new levels of protection of personal information but at a "*collective level*"[57] where the powers

---

Leveraging the Legibility of Users to Accentuate Inequality, in M. Moore, D. Tambini (eds.), *Digital Dominance*, cit. at 176-201; J. Lerman, *Big Data and Its Exclusions*, Stan. L. Rev. Online (2013); E. Pellecchia, *Profilazione e decisioni automatizzate*, cit. at 1211.

[55] Consider the European Parliament resolution of 16 February 2017 with r*ecommendations to the Commission on Civil Law Rules on Robotics sub* lett. O "whereas the developments in robotics and AI can and should be designed in such a way that they preserve the dignity, autonomy and self-determination of the individual" and *sub* lett. Q "whereas further development and increased use of automated and algorithmic decision-making undoubtedly has an impact on the choices that a private person (such as a business or an internet user) and an administrative, judicial or other public authority take in rendering their final decision of a consumer, business or authoritative nature"; consider also the recitals 6 and 8 of the Regulation (EU) 2016/679; and finally consider the European Commission decision of 27 June 2017 concluding that the total fine imposed on Alphabet Inc. and Google Inc. should be euro 2,42bl. for the manipulation by its own comparison shopping service, Case AT. 39740 - Google Search.

[56] On the topic see G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica* (2015); see a partially different opinion G. Malgieri, G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 4 International Data Privacy Law 249 (2017).

[57] See too A. Mantelero, *Rilevanza e tutela della dimensione collettiva*, cit. at 141; D. Tambini, *Social Media Power and Election Legitimacy*, in M. Moore, D. Tambini (edited by), *Digital Dominance*, cit. at 265-293; F. Bouhon, *Le droit à des élections libres et Internet*, in Q. Van Enis, C. De Terwangne (eds.), *L'Europe des droits de l'homme à l'heure d'Internet* (2019); B. Grofman, A.H. Trechsel, M. Franklin (eds.), *The Internet and Democracy in Global Perspective. Voters, Candidates, Parties, and Social Movements* (2014); see also B. Caravita, *Social network, formazione del*

of prediction and manipulation can affect things like voters' choices in elections[58].

The need is made more urgent by the natural market (data market) tendency to concentrate information, computational and economic power[59].

A balance has to be found between the economic benefits, generated by the free flow of information / data, and the personal and collective interests necessary to uphold the tenets of privacy and self-determination. This need to balance has been solved in some systems by using control and censorship (China) or by setting territorial restrictions (Russia). In the case of the Russian Federation the law was amended, in 2014[60], such that any company that wishes to hold information on Russian citizens must save and process that information on Russian soil in data centers also on Russian soil. The legislation does not prohibit foreign access to these data centers nor does it prohibit the copying of this information but it states that the gathering of this information must happen exclusively on Russian soil. As of yet there is not

consenso, istituzioni politiche: quale regolamentazione possibile?, Federalismi.it (2019); M. Calise, F. Musella, *Il principe digitale* (2019).

[58] There is no shortage of practical applications: in the 2016 US presidential elections the winners campaign was based on the behvioural knowledge, Big Data analysis and targeted advertising; see H. Grasseger, M. Krogerus, *La politica ai tempi di Facebook*, 1186 Internazionale 40-47 (2017). See also W. Christl, S. Spiekermann, *Networks of Control*, cit. at 26-27, "Scholars in communication studies have long challenged the idea of plain top-down manipulation as inappropriate and too simplistic, insisting that humans are able to use different individual appropriation of communication strategies. The shift to completely personalized interactions based on extensive individual profiles possibly creates new and unknown degrees of manipulation". See too R. Epstein, *Manipulating Minds: The Power of search Enginee to Influence Votes and Opinions,* in M. Moore, D. Tambini (ed.), *Digital Dominance*, cit. at 294-319; R. Davis, C. Holtz-Bacha, M.R. Just (eds.), *Twitter and Elections Around the World. Campaigning in 140 Characters or Less* (2016); in Italy, see M. Mezza, *Algoritmi di libertà. La Potenza del calcolo tra dominio e conflitto* (2018).

[59] With reference to the situation in Italy see the decision n. 146/15/CONS (Autorità per le Garanzie nelle Comunicazioni) regarding *Indagine conoscitiva sul settore dei servizi internet e sulla pubblicità online*, in particular Annex A (available online at https://www.agcom.it/indagine-conoscitiva-informazione-e-internet-in-italia.-modelli-di-business-consumi-professioni-).

[60] Federal Law No. 242-FZ on *Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunication Networks* (New Data Protection Law) del 2014.

enough evidence to understand what effect this solution has had (in force since 2016) even although it seems to be at odds with the need, of the digital market, for the free flow of data (globally)[61].

What emerges in the end is a variety of situations where we can state that: (i) there is a lack of transparency on the circulation, the content and on the results during the processing of all this data; (ii) there is a lack of transparency on the processing of data especially when it affects the individual in the collective sphere; (iii) that it is difficult to attribute responsibility and liability for activities that are carried out across the globe.

2.2. (*Follows*) contractual dealings

In the area of contractual relationships, issues of transparency have to be considered during the initial formulation of the contract where, in the name of fairness, both parties are obliged to fully inform the other.

The right to information is especially important in European consumer contract law[62]. European Union legislation describes in detail the nature of the information that must be given to the consumer so that they can make a pondered evaluation of the contract (type and characteristics of goods,

[61] Consider the different solution adopted by recent European Regulation (EU) 2018/1807, *on a framework for the free flow of non-personal data in the European Union* (in O.J.E.U. L 303, November 28, 2018) that will be apply from June 2019 (art. 9). This Regulation aims to ensure the free movement of data other than personal data within the Union by laying: - data localisation requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality (art. 4); - the powers of authorities to access to data for the performance of their official duties in accordance with Union or national law, in particular the access to data may not be refused on the basis that the data are processed in another Member State (art. 5); - the Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to a competitive data economy, based on the principles of transparency and interoperability and taking due account of open standards (art. 6).

[62] See Directive 2011/83/EU of 25 October 2011, on consumer rights (in O.J.E.U. L 304, of 22 November 2011) and the duty of Member States to adopt and publish, by 13 December 2013, the laws, regulations and administrative provisions necessary to comply with this Directive. On this topic, see C. Twigg-Flesner (eds.), *Research Handbook on EU Consumer and Contract Law* (2016); also G. Straetmans (ed.), *Information Obligations and Disinformation of Consumers* (2019).

identity of the trader, the economic aspects, arrangements for performance, conditions, time limit and procedures for exercising the measures of protection). This information must be given before any contract is signed so that the consumer can compare various offers.

What can be seen is that European consumer legislation has a two sided approach: one side is there to protect the consumer's economic interests while at the same time the other side is there to ensure that market competition continues to thrive[63]. There are also two sides to transparency. By being informed, the consumer is not only better able to select goods from a range of commercial offers but acts as a distributed monitoring system on the behavior of companies. This generates or at least encourages a system of trust that in turn encourages more commerce.

Still in the European model, the requirement for information comes with conditions regarding the way in which it is given. In fact, the information given must be exhaustive, clear, intelligible, in good faith (in line with the ideas of good faith, truth, transparency and fairness even in the pre-contractual phase) and accessible. With these parameters, the duties of honesty and behavior of traders are important and there are defined forms of pre-contractual responsibility and liability based on good faith and the guarantee of transparency.

In this context, the impact of technology on transparency has been minimal, being, in this case, tied to the informative model.

In other words, transparency and the duty to inform continue to represent the way to guarantee, *informed contracts, qualified consent* and *a knowledgeable consumer.*

Legal solutions do not go beyond the *click* with which the consumer confirms that (i) they have read the information relative to the contract (even although it is never certain that the rights and duties that tied to the contract have been understood); (ii) they have understood that they will have to pay; (iii) they have accepted the conditions under which their information/data will be used to fulfil the contract.

[63] Judgment of the CJUE, Grand Chambre, of 16 December 2008, C-205/07, *Lodewijk Gysbrechts*, ECLI:EU:C:2008:730, pt. 53.

For example, European legislation on distance contracts concluded with electronic means (web sites, e-mail, etc.), has imposed on the trader to make the principal elements of the contract visible to the consumer in the immediate vicinity of the point of confirmation of the order[64] showing, unequivocally, at what moment one accepts the duty to pay[65]. If the vendor does not respect these duties the consumer is completely free of any contractual obligations.

There are more significant changes in the growing market of online sharing and circular economies[66] where some of the biggest operators are *Amazon, Airbnb*, *eBay*, *Lyft*, *Uber*, *Friendsurance*, etc. These companies work simply by offering a platform where consumers and traders can carry out a transaction. The owners profit by (i) taking a commission on each transaction, (ii) by selling the data collected on the users, and (iii) promoting relevant products (personalized advertising). The users profit by having the convenience of finding products in one place and optimized way of selling their products[67].

Other more traditional (but no less important) forms of digital economy are those of on-line commerce. Where goods and services are often attached to systems that compare the specifications and prices from a wide range of offers. The fields of application are many and include, insurance, travel, holidays, phones, utilities and consumer goods.

---

[64] Recital 39, Directive 2011/83/EU.

[65] Art. 8, par. 2, Directive 2011/83/EU.

[66] The *collaborative economy* is a complex ecosystem of on-demand services and temporary use of assets based on exchanges via online platforms; this system is changing rapidly and is developing at a fast pace. See European Commission, *Upgrading the Single Market: more opportunities for people and business*, COM/2015/550 of 28 October 2015, pt. 2.1, where "according to a recent study, the five main collaborative economy sectors (peer-to-peer finance, online staffing, peer-to-peer accommodation, car sharing and music video streaming) have the potential to increase global revenues from around euro 13 billion now to euro 300 billion by 2025. See also European Commission, *A European agenda for the collaborative economy*, COM/2016/356 of 2 June 2016; European Parliament Resolution of 15 June 2017 on *A European Agenda for the collaborative economy* (2017/2003/INI).

[67] G. Smorto, *Economia della condivisione e antropologia dello scambio*, 1 Diritto pubblico comparato ed europeo 119-138 (2017); Id. , *Reputazione, fiducia e mercati*, 1 Europa e diritto privato 199 (2016); Id., *La tutela del contraente debole nella* platform economy, 2 Giorn. dir. lav. rel. indust. 424 (2018).

Both the collaborative economy and on-line commerce are made possible by the digital platforms and their associated infrastructure which exploit applications on mobile devices, social networks and geolocation services [68].

When we look at the impact of the new technologies on these market with respect to transparency there are two critical issues.

(I) The first issue regards the lack of clarity (i.e. transparency) on the way in which these platforms use information that they have acquired during the course of a transaction or mediation.

When dealing with these platforms the web sites or mobile applications through which these activities are executed purport to have information privacy policies (rarely read and almost never understood) they also declare that they will install cookies in the computer and, more generally, guarantee maximum transparency.

In reality users do not pay particular attention to how they are giving up their data or how that data will be processed. With a few *clics* (if that), they go ahead and formalize their consent on how their data will be used and processed just to be able to proceed with the transaction.

Users show that they have neither the time nor the competence to understand the consequences of the terms of data protection that they have just agreed to and what complex implications these will have (often at a much later date). In other words, we have gone form *informed consent* to *informatics* or *digitalized consent* without adequate adjustments[69]. So as in the

[68] In recent years some platforms have become so large as to control access to the markets influencing the activities to the financial operators; see I. Graef, *When Data Evolves into Market Power -Data Concentration and Data Abuse under Competition Law*, in M. Moore, D. Tambini (eds.), *Digital Dominance*, cit. at 71-97; L.S. Morais, *Competition in Digital Markets and Innovation. Dominant Platforms and Competition Law Remedies*, cit. at 27-44; Italian Competition Authority, *Annual Report*, March 2017, 54 ff.

[69] G.A. Benacchio, *Information et transparence dans la protection des consommateurs: une réalisation difficile*, in *Annuario di diritto comparato e studi legislativi*, special edition with Italian National Reports of International Academy of Comparative Law, XX° International Congress in Fukuoka (2018), argues that "*le contrat liant les usagers aux plateformes du web est, selon la terminologie des économistes, un contrat incomplet puisque les usagers ne sont pas en mesure de connaître exactement le*

area of personal relationships where it is possible to know, predict and manipulate the behavior of individuals, there is a need for regulations that can guarantee adequate transparency and information to the users.

The counterpart, especially if a consumer, should be able to have access to their personal profiles or "virtual doubles"[70] that result from the activities of the data mining algorithms and which are stored by many digital platforms and market / data operators.

At the present, there is no public or private place where a counterpart can access their virtual double.

This means that there is no possibility to correct the information to give, what they feel is, a truer representation of themselves. Nor are they able to ask for corrections, updates or comment on mistakes. Errors made by processing algorithms are all but intangible in that they can have serious effects on real life events like credit ratings, insurance premiums, healthcare and almost all consumer goods. Not only are these affected, but depending on the available data, so too are offers (or refusals) for work, loans, healthcare, love, etc.[71]

(II) The other critical issue is the lack of transparency with regards to the ways the reputation of the operators on the various platforms is measured and calculated.

In on-line trade one of the determining factors for doing business is trust. The most common system is to use the reputations of operators as a gauge of trustworthiness. In fact, reputation is one of the most effective tools for a consumer to

---

risque auquel ils s'exposent (…) *Les clauses qui interdisent la revente à des tiers ou le partage des données restant presque toujours nébuleuses, la manière dont les plateformes utilisent les informations que communiquent les vendeurs et les consommateurs pour la réalisation de l'opération commerciale pèche pour le manque de claret*". Exemplary is the case of Facebook's CEO Mark Zuckerberg who in April 2018 was called by the *United States Senate Committee on Commerce, Science, and Transportation* and in May 2018 by the *European Parliament* in relation to the Facebook-Cambridge Analytica data breach.

[70] S. Turkle, *Reclaiming Conversation. The Power of Talk in a Digital Age* (2015); see also C. O'Neil, *Weapons of Math Destruction. How Big Data Increases Inequality and Threatens democracy* (2016).

[71] See A. Greenfield, *Radical Technologies*, cit. at 250; also C. Busch, *The future of pre-contractual information duties: from behavioural insights to big data*, in C. Twigg-Flesner (ed.), *Research Handbook on EU Consumer*, cit. at 231-239.

choose a vendor. In many cases this reputation is *quantified* using reviews left by other consumers who give points or leave other indicators of positive or negative feedback[72].

However, there is nothing to guarantee the "genuine or true nature" of the feedback on which depends the reputation, so important for business, of an operator[73].

The way in which these scores (for reputation) are arrived at are rarely publicized and when they are (by stating that the average of all the reviews is taken) there is no guarantee of provenance, the number of reviews or their contents.

Yet again there is an "information asymmetry" for the consumer which is overcome by using reviews or ratings to assess a vendor[74]. All this trust with no way to prove it. This solution gives insufficient guarantees for an online commerce environment and suggests that there is a need for new regulations[75], standards

---

[72] See *Behavioural Study on the Transparency of Online Platforms. Final Report*, produced by European Commission, 2018; the study found that when consumers are informed that the ranking is based on a specific criterion such as popularity, the probability of selecting the product is 115% higher; furthermore, providing the additional information compared to having no user reviews or ratings, a review in a prominent position on the website leads to a 200% increase in the probability of choosing the product.

[73] See the case on the false reviews by online companies TripAdvisor LLC and TripAdvisor Italy S.r.l. fined by the Italian Competition Authority for eur 500.000, with decision n. 25237 of 19 December 2014 and then canceled by administrative Court. See also G. Smorto, *Reputazione, fiducia e mercati*, cit. at 423 ss.; L. Carota, *Diffusione di informazioni in rete e affidamento sulla reputazione digitale dell'impresa*, 4 Giur. comm. 624 (2017); M. Colangelo, *Le piattaforme del settore alberghiero online: parity clauses, modelli di business e concorrenza*, in G. Colangelo, V. Falce (a cura di), *Concorrenza e comportamenti escludenti*, cit. at 111-138; S. Ranchordás, *Online Reputation and the Regulation of Information Asymmetries in the Platform Economy*, 1 Critical Analysis L. 127-147 (2018).

[74] See European Commission, *A New Deal for Consumers*, COM/2018/183. See also J.E. Cohen, *Law for the Platform Economy*, in 51 UC Davis L. Rev. 135 (2017); G. Resta, *Digital platforms and the law: contested issues*, 1 Media Laws 232 (2018).

[75] See, for example, the proposal for a new EU Directive *regards better enforcement and modernisation of EU consumer protection rules*, COM(2018) 185 final; the proposal introduces additional information required to online marketplaces to clearly inform consumers about: (i) the main parameters determining ranking of the different offers, (ii) whether the contract is concluded with a trader or an individual, (iii) whether consumer protection legislation applies and (iv) which trader is responsible for ensuring consumer rights related to the contract. Furthermore, these provisions should clarify

and certification, maybe using the same models as is used for the companies that offer credit card payment services.

2.3. (*Follows*) dealings with public authority

When it comes to relations with public authorities, transparency is "one of the socio-political myths of our times"[76], being presented as the basis on which radical changes have been made in the views and workings of authorities and their behavior towards the population[77].

What has changed is the bipolar view that many Public administration models have where the authority is in a position of supremacy over its citizens and is thus the only guardian of the public interest. The authority and the individual represent opposite poles in an asymmetric, and conflictual relationship with divergent interests that legitimize secrecy in public affairs[78].

The recognition of transparency as "the essence"[79] of the authorities is the culmination of a process that has, in a short time, redefined the terms transparency/secrecy when considering authorities and their behavior[80].

---

when online platforms must indicate search results that contain "paid placements" or "paid inclusion".

[76] See G. Quadri, *Riservatezza e trasparenza nell'esperienza costituzionale*, in AA.VV., *L'amministrazione pubblica tra riservatezza e trasparenza* (1991).

[77] See a global overview and statutory goal on access to information laws at http://www.right2info.org/access-to-information-laws; see also M. Savino, *The Right to Open Public Administrations in Europe: Emerging Legal Standards* (2010); M. Savino, *La nuova disciplina della trasparenza amministrativa*, 8-9 Giorn. dir. amm. (2013); D.-U. Galetta, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un analisi storico-evolutiva, in una prospettiva di diritto comparato ed europeo*, 5 Riv. it. dir. pubbl. com. 1019-1065 (2016).

[78] S. Cassese, *L'arena pubblica. Nuovi paradigmi per lo Stato*, 1 Riv. trim. dir. pubbl. 601 (2001); G. Arena, *Trasparenza amministrativa*, in S. Cassese (ed.), *Dizionario di diritto pubblico* (2006); G. Lentini, *Il segreto e la trasparenza: dall'amministrazione chiusa all'amministrazione aperta. Le tappe dell'evoluzione dei rapporti tra i pubblici poteri ed i cittadini*, 1-2 Amministrativ@mente 3-36 (2017).

[79] See G. Arena, *Trasparenza amministrativa*, cit. at 5946.

[80] See N. Bobbio, *La democrazia e il potere invisibile*, in 2 Riv. it. scienza pol. 181 (1980), yet also in *Il futuro della democrazia* (2014); furthermore M. Catanzariti, *Segreto e potere. I limiti della democrazia* (2014).

In Italy for example the general idea publicizing the workings of the administration was only introduced in 1990[81], after a century and a half of enforcing, on departments and employees, a generalized and rigid "segreto d'ufficio" duty of official secrecy[82].

Without going through a detailed study of the theories of transparency in the regulation of public administrations[83] we can study it in three key situations.

The first situation is to do with the knowledge of decision making processes.

Transparency is ensured by the authority's duty to publish documents[84]. This duty, depending on the legal model chosen, may cover the publication of regulations as well as information to do with: (a) the organization of a body (offices, personnel, deliberations of council groups, winning contracts, interests in companies) personnel information (councilors, executives, bonuses, performance reviews); (b) budget management (balances, tenders, grants, economic beneficiaries); (c) the way the services work and simplification (charter of services, the supply of services, payment terms and forms and paperwork). Working this way means that authorities are being asked to work in the 'glass house'.

In the Italian system, a breach of this duty brings with it penalties against the authority in the form of public employee responsibility and other liabilities for damage to the reputation of the public administration.

The second situation is to do with access to public documents[85].

---

81 With reference to the Italian legal system see Legge 7 agosto 1990 n. 241, *Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi* (in O.J. n. 192 of 18 August 1990).

82 See G. Arena, *Il segreto amministrativo. Profili teorici* (1983).

83 About the italian legal system see F. Merloni, G. Arena, G. Corso, G. Gardini, C. Marzuoli (eds.), *La trasparenza amministrativa* (2008).

84 M. Bombardelli, *La trasparenza e gli obblighi di pubblicazione*, in R. Garofoli, T. Treu (eds.), *Treccani. Il libro dell'anno del diritto 2014* (2014); F. Di Donato, *Lo stato trasparente. Linked open data e cittadinanza attiva* (2010).

85 See H. Kranenborg, W. Voermans, *Access to Information in the European Union. A Comparative Analysis of EC and Member State Legislation* (2005); D.C. Dragos, P. Kovač, A.T. Marseille (eds.), *The Laws of Transparency in Action: A European*

Transparency assumes different levels of importance depending on the values and policy choices of each legal system. The possible levels go from restricted access (for individuals who need to defend their rights e.g. legal evidence), to open access to all documents subject to publication and on to total access (as with the US FOIA) where anyone can access any document held by public administrations, so-called civic access, except for specific limitations, e.g., personal privacy, State secrecy, etc.[86] In this way, it is easier to have a form of distributed surveillance on the behavior of authorities and in the end to prevent malpractices and maladministration.

The third situation is in the participation of decision making processes.

The first to experiment this were Sweden and Finland[87]. The entrance of these countries into the EU in 1995 coincided with initiative to bring more openness to EU institutions. This was by encouraging forms of participation and consultation in the formative stages of policy and legislation.

Dialogue and participation have since become key words in the european governance reform program launched in 2001[88] which is based on five principles (openness, participation, accountability, effectiveness and coherence). From this moment, in Europe, ordinary people, who were once very much on the

Perspective (2019); S. Foà, *La nuova trasparenza amministrativa*, 1 Dir. amm. 65 (2017).

[86] See P. Savona, A. Simonati, *Transparency in Action in Italy: The Triple Right of access and Its Complicated Life*, in D.C. Dragos, P. Kovač, A.T. Marseille (eds.), *The Laws of Transparency in Action: A European Perspective*, cit. at 255-294; E. Carloni, *Se questo è un FOIA. Il diritto a conoscere tra modelli e tradimenti*, 4 rassegna Astrid 1-12 (2016); A. Marchetti, *Le nuove disposizioni in tema di pubblicità e trasparenza amministrativa dopo la riforma "Madia": anche l'Italia ha adottato il proprio "Foia"? Una comparazione con il modello statunitense*, 10 Federalismi.it 1-33 (2017); A. Moliterni, *La via italiana al FOIA: bilancio e prospettive*, 1 Giorn. dir. amm. 23-34 (2019).

[87] Sul tema A. Santini, *Il principio di trasparenza nell'ordinamento dell'Unione europea* (2004); M.C. Statella, *Trasparenza, informazione e apertura. Il Trattato di Amsterdam e i diritti degli individui nel procedimento di formazione degli atti comunitari*, in U. Draetta, N. Parisi (eds.), *Trasparenza, Riservatezza. Impresa. Studi su democrazia rappresentativa, diritti dell'uomo e attività economica nell'Unione europea* (2001).

[88] European Commission, *European governance - A white paper*, COM/2001/428, of 5 August 2001.

margins of the decision-making processes, start to become involved in it.

The technological innovations have significant effects on all three of the above situations: (i) they make the requirement of publishing the documents cheaper, traceable and faster, (ii) they facilitate access to documents and information and, more generally, they help speed up the process towards providing to total access, (iii) encouraging public consultation in a wider and more traceable way.

These are processes that stem from the digitalization of the administrations[89] which was set at a European level and described in specific initiatives (first *eGovernment*, then *Open Government*)[90]. On this point, it is worth noting that use of technology has led to a growth in some automated administration, with certification and official documents, as a prelude to automating some juridic functions[91].

Another important innovation in this field is in public contract systems using e-procurement methods (where goods and services can be acquired using a digital platform) and the use of data mining to monitor and ensure fairness and legality[92].

---

[89] See F. Faini, *Data society. Governo dei dati e tutela dei diritti nell'era digitale* (2019); G. Carullo, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa* (2017); L. Sartori, *Open Government: what else?*, 3-4 Le istituzioni del federalismo 753-776 (2013); F. Costantino, *Open Government*, in *Digesto discipline pubblicistiche* (2015).

[90] See European Commission Final Report, *Towards faster implementation and uptake of open government*, 2016, available online at http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40861; see also European Commission, *Open data. An engine for innovation, growth and transparent governance*, COM/2011/882 of 12 December 2011 and *eGovernment Action Plan 2016-2020. Accelerating the digital transformation of government*, COM/2016/179, of 19 April 2016; *eGovernment Benchmark 2019. Empowering Europeans through trusted digital public services*, study prepared for the European Commission, October 2019.

[91] See P. Otranto, *Decisione amministrativa e digitalizzazione della p.a.*, 2 Federalismi.it 15-25 (2018); also U. Morera, *Behavioural economics e valutazione giudiziale del rapporto contrattuale regolato* (2017); F. Patroni Griffi, *La decisione robotica e il giudice amministrativo*, conference at "Leibniz Seminars 2018", 5 July 2018, Accademia dei Lincei - Roma; S. Lepidi, *Algoritmi nelle procedure amministrative, i principi da rispettare e le prospettive future*, AgendaDigitale.eu 27 December 2019.

[92] See European Commission, *Making Public Procurement work in and for Europe*, COM/2017/572, 3 October 2017; also European Commission, *End-to-end e-*

3. Conclusions

Transparency is one important key for understanding the social, economic and cultural transformations that the technology is introducing.

These transformations are shaking established patterns with tensions that run deep even in the legal sphere, with changes emerging at system, model and regulatory level.

In the framework of a global economy based on the production of intangible goods, where the main resources are information and knowledge and where these resources are exchanged rapidly and frequently, there is a special emphasis on the value of transparency. It must be the starting point for new rules. There will be more of these than in the past and many of them are yet to be defined.

We can see this in the field of AI (artificial intelligence) driven automation where programs can make decisions without external guidance by learning continuously from huge quantities of data. This brings economic benefits but it also has worrying consequences for individuals and for society. Thus, there is a growing number of calls for greater transparency and guarantees to respect fundamental rights and liberty.

At a higher level, the declaration of principle, shared by States, Authorities, big corporations and social movements, "it should always be possible to supply the rationale behind any decision taken with the aid of AI that can have a substantive impact on one or more persons' lives", "it should always be possible to reduce the AI system´s computations to a form comprehensible by humans".

At a lower level transparency is being woven into, more or less consolidated, codes / rules of conduct and duties of honesty which are forming the base of forms of responsibility and liability based on good faith in an objective sense. Some of these forms of responsibility are innovative like algorithmic responsibility.

The idea of transparency as a value woven into codes of conduct along with responsibility and forms of protection and remedy exemplifies the steps that have so far been taken in the

---

procurement to modernise public administration, COM/2013/453, 26 June 2013. See also M. Cozzio, *La nuova strategia europea in materia di appalti pubblici*, 1 Giorn. dir. amm. 53-62 (2019).

principal legal systems. The new technologies and emerging interests have necessitated a search for new equilibria which has led to changes in rules, in their interpretation and in their application.

Many of the technological innovations are governable by existing values of transparency and codes of conduct as has already been mentioned. We have seen this in the three situations already analyzed.

Other, more profound, innovations escape this possibility, and will require so much change that it will be necessary to build new legal frameworks to deal with them. Just modifying the rules in existing frameworks will not be enough.

We have already seen these premises in the section on the movement and processing of data and information. The knowledge that can be gained from the enormous collections of data allows for a network that monitors every aspect of our lives. This network exists without any guarantee of us knowing the logic behind its workings or who controls it.

The reaction to this situation has lead to the introduction of new rules and technical standards, such as *privacy by default*, *privacy by design*.

They are useful solutions but they do not offer sufficient guarantees of protection, especially when the effects have implications at the *collective level.* In other words, it is all very well to have brand new rules but without protection there remain questions such as: "what is the point in having elections if the algorithms not only know how each person will vote but also what that person's underlying neurological reasons are for their choice"[93].

There are circumstances where the role, meaning and functions of transparency could be redefined to fit a new world reality where our data (source of knowledge and wealth) could be the new atoms, generating a global asset available to all but controlled by no one.

In such a framework where all data (both personal and not) is accessible, the right of the individual to know and control his data loses its importance. What does become important is the absence of transparency on the way in which the technology (and

[93] Y.N. Harari, *Homo Deus. A Brief History of Tomorrow* (2016).

its managers) are able to extract information which reveals things about our lives. This information can be used not just for marketing but for the manipulation of public affairs such as elections, judicial processes and administrative processes.

There emerges a need to have a coherent classification of transparency- special guarantees of knowability about the programs, the workings and the results that process this mass of data- to protect fundamental individual rights. So, transparency becomes a new *common good* which, as such, will influence the system of property rights applied to these technologies, making their internal workings and ends knowable not just their owners but to all.