Algorithmic Decisions and Transparency: Designing Remedies in View of the Principle of Accountability

Michael W. Monterossi[*]

Abstract

The lack of explainability of algorithms' decision-making processes raises numerous issues, both when used by the public administration and private subjects. The Council of State has intervened in this matter, by establishing some principles to be followed when using automated IT systems in executing administrative activity. However, these principles, to some extent, have been pondered in the 2016 EU General Data Protection Regulation. The pivotal point towards which the legal discussion is heading regards the necessity to develop algorithms in a manner that renders their decisions transparent. In this respect, the principle of accountability, as foreseen by the Regulation, may acquire ever more relevance, as a tool for re-adapting the rules governing diverse areas of Private Law to the new 'smart' technological scenario.

I. Governing Algorithmic Decisions

In a recent sentence, the Italian Council of State has coped with some of the critical issues which stem from the use of Information Technology (IT) systems based on algorithms, in order to execute the activity of the public administration.[1]

The ruling inserts itself, as a further thread, into a thick fabric of administrative sentences, which wraps around the activity performed by a 'mindless' algorithm.[2] The legal case originates from the complaints filed by a multitude of teachers, whose public administration hiring procedure was entrusted entirely to a system managed by an algorithm. More precisely, the algorithm was assigned the task of managing the placement phase for the teachers within the national territory. The assignment of posts was based on certain parameters among which, in particular, the preferences expressed by the teachers regarding the location of hiring as well as the subject to be taught and the school level and grade. These preferences were to be satisfied according to the order of merit ranking, as

[*] Research Fellow in Private Law, University of Lucerne, Switzerland.

[1] Consiglio di Stato 8 April 2019 no 2270, available at www.leggiditaliaprofessionale.it.

[2] See in particular Tribunale amministrativo regionale Lazio-Roma 10 September 2018 no 9224; Tribunale amministrativo regionale Lazio-Roma 9 November 2018 no 10828; Tribunale amministrativo regionale Lazio-Roma 13 September 2019 no 10963 and 10964; Tribunale amministrativo regionale Lazio-Roma 27 May 2019 no 6606, all available at www.giustiziaamministrativa.it.

established by law. However, the algorithm decided to act in its own way: it sent the teachers ranked the highest far from their provinces of residence and assigned them subjects and levels of schools which they had not requested. On the contrary, teachers with lower scores, and thus lower in the same ranking, managed to benefit from the assignments of teaching posts in their areas of residence and according to the other preferences expressed in their relative applications.

The Council of State recognized that the results of the automatized procedure were 'illogical' and 'irrational' and that, consequently, there had been a violation of the principles and norms of law which were to be applied. Thus, by reforming the sentence handed down by the court of first instance, it established that the teachers should be assigned to available posts in places which respected the ranking order and the teachers' preferences.

The case provided the opportunity for the Council of State to face the insidious question of whether, and within which limits, the public administration can make use of algorithms – defined by the court as an 'ordered sequence of calculations' – in order to expedite its activity.

According to the Council of State, the use of algorithms, especially when carrying out 'serial and standardized procedures',[3] is not only possible but must also be encouraged. In fact, the use of an automatized IT procedure, when compared to activity carried out by humans, guarantees a twofold advantage. On one hand, the algorithm – like all machines – enhances human ability by ensuring a reduction in the time needed to reach a final decision; on the other, and at the same time, it limits 'human risk' factors (to a certain extent inevitable) associated with possible negligence, if not outright malice, on the part of public officials – those in the flesh and blood – in charge of the administrative activity.

In light of this, the Council of State points out that the technological alignment within the public administration is in accordance with the canons of efficiency and cost-effectiveness for administrative action which, in compliance with the principles of the Italian Constitution regarding the good functioning of administrative action (Art 97 Constitution), impose on the administration the pursuit of its own ends with the least possible expenditure of time and resources.

At any rate, the use of IT systems-based procedures must always comply with the principles that regulate administrative activity, among which, in particular, that of publicity and transparency (Art 1, legge 7 August 1990 no 241).[4] To such an end, the court holds that two requirements must be satisfied. Firstly, the mechanism through which the 'robotic decision' is put into effect must be 'knowable'. Secondly, the algorithmic rule must be subject to the full cognition of and review by the administrative judge. Both requirements are instrumental

[3] This observation recalls the remarks offered by F. Patroni Griffi, 'La decisione robotica e il giudice amministrativo', speech given at the 'Decisione robotica' conference, organized as part of the 'Leibniz' Seminari per la teoria e la logica del diritto – Roma, Accademia dei Lincei, 5 July 2018, available at https://tinyurl.com/scglzey (last visited 30 December 2019).

[4] See Gazzetta ufficiale 18 August 1990 no 192.

in allowing the judge to examine how the administrative power was concretely exercised, by conducting a full assessment of the legitimacy of the decision.

However, the jurisprudence of the Regional Administrative Tribunal (TAR) seems to move in a different direction. Indeed, their decisions – both precedent and successive to the sentence under comment – seem, at first glance, to be in open contrast with the arguments developed by the Council of State.[5] The point of discord, which marks the difference between the opinions, is the necessary presence of human officers to accompany and guide the administrative activity carried out by the algorithm, as a prerequisite for guaranteeing compliance with the principles that regulate public administration activity.

According to the Council, in fact, entrusting an activity of mere automatic classification to an (efficient) electronic elaborator – even in the absence of human intervention – is nothing more than the consequence of the (necessary) updating of the principle of the good functioning of the public administration (Art 97, para 2, Constitution) to the new technological scenario. Conversely, the sentences handed down by the TAR placed emphasis on the fact that the use of algorithms within an administrative activity still requires the presence of a 'human' official as '*dominus*' of the procedure along with the employed computer system.[6] More in detail, the TAR judges hold that an algorithm cannot substitute *tout court* the cognitive and acquisitive activity as well as that of judgments which, in the ambit of the administrative procedure, is entrusted to the control and supervision of a human officer.[7]

The risk, in absence of such an intervention, is that the algorithm – owing to its 'impersonal' nature – undermines the institutes of participation, transparency and access that regulate the citizen-public administration relationship, which are all functionally oriented to allow the former to have knowledge of the activity conducted by the latter. Furthermore, and above all, what could be compromised is the duty to motivate administrative decisions, thus impeding the interested party, before, and the judge invoked, after, from understanding the logical-juridical *iter* followed to achieve these decisions.[8] A different solution would result in a violation of the constitutional values established by Arts 3, 24, 97 of the Italian Constitution as well as Art 6 of the European Convention on Human Rights.[9]

[5] See n 2 above.

[6] Tribunale amministrativo regionale Lazio-Roma 13 September 2019 no 10963, available at www.giustiziaamministrativa.it.

[7] The necessary presence of a person in charge of the proceeding, known as 'responsabile del procedimento', is foreseen by Art 5, legge 7 August 1990 no 241. See for deeper analyses F. Patroni Griffi, 'La l. 7 agosto 1990 n. 241 a due anni dall'entrata in vigore. Termini e responsabile del procedimento; partecipazione procedimentale' *Foro italiano*, III, 66 (1993).

[8] ibid.

[9] Tribunale amministrativo regionale Lazio-Roma 10 September 2018 no 9224, available at www.giustiziaamministrativa.it. See L. Viola, 'L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte' *Foro italiano*, 1598 (2018); P. Otranto, 'Decisione amministrativa e digitalizzazione della p.a.' *federalismi.it*, 15 (2018).

After all, as noted by some authors in the legal doctrine,[10] the problem posed by algorithms in these cases does not directly regard the correctness of the decision but rather the correspondence of the decision-making process to the criteria of the just process. A position which seems to be shared by both legal doctrine and jurisprudence, even in other legal systems called upon to respond to similar issues,[11] due to the importance which, in case of algorithmic decisions, is acquired by judicial review.[12]

On closer inspection, in fact, the two orientations recalled are not so far apart as it may seem. The Council of State, in fact, does not exclude the necessity for the integration of human activity in the sphere of procedures performed by the algorithm, which, on the contrary, is considered essential to guarantee the respect of the principles governing administrative activity. The difference lies in the fact that, according to the Council of State, the co-operation between

[10] See D.U. Galetta and J.G. Corvalán, 'Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto' *federalismi.it*, 1, 18 (2019).

[11] Similar issues were faced by the French *Conseil constitutionnel*, in the Decision no 2018-765 DC of 12 June 2018, available at https://tinyurl.com/vmfyna8 (last visited 30 December 2019). The Council was called upon to evaluate the constitutional legitimacy of the dispositions introduced by Loi 20 June 2018 no 2018-493, which modified Loi 6 January 1978 no 78-17 *relative à l'informatique, aux fichiers et aux libertés* in order to adapt national legislation to the European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016) OJ L119/1.

The applicants contested the provisions that allowed the administration to adopt individual decisions having legal effects or decisions which significantly affect a person only on the basis of an algorithm (see Art 21 of Loi 20 June 2018 no 2018-493 which modified Art 10 of the aforementioned Loi 6 January 1978 no 78-17).

According to them, the use of self-learning algorithms, which entailed the constant revisions of the rules on the basis of which they operate, could make it impossible for the administration to comprehend the logic behind that decision-making process employed by the algorithms. Therefore, there would be no guarantee that the rules applied by the algorithms are in compliance with the law and the administration would no longer have any regulatory power over the algorithms to define their own rules.

However, the Council noted that, on one hand, there is no abandonment of the competence of regulatory power considering that the decision can only be taken on a legal basis and, on the other, the administration has in any case to comply with several conditions. In particular, the data processor must always be able to understand the functioning of the algorithmic process as well as the way in which it evolves, in order to explain to the person interested – in detail and in an intelligible manner – the way in which the processing was carried out. It follows that the public administration cannot use those algorithms whose automatic functioning is not understandable by the person in charge of processing. See on this regard Art R 311-3-1-1 and Art R. 311-3-1-1-2 of the Décret of 14 March 2017 no 2017-330 setting the conditions of application of Art L. 311-3-1 of Loi 6 January 1978 no 78-17.

[12] F. Patroni Griffi, 'La decisione' n 3 above, 4-5, who highlights that by making use of a robotic decision, the administration burdens the judge with its role of 'mediation' of the interests involved, of evaluation and at times of investigation into facts. Therefore, when evaluating the correctness of the algorithm, that is, of the decision-making process and of its factors, as well as the facts at the basis of the administrative provision the judge may have to make – for the first time on a 'human' plane – evaluations done directly by the algorithm.

automatized systems and humans,[13] is not to be pursued during the execution of the procedural activity, but before, at the time of the programming and developing phase of the algorithm.

The Court notes, in fact, that what characterizes the action of the algorithm as an 'IT administrative act' is precisely the technical rule – constructed by a man or a woman – which supports, by governing it, the decision-making process of the algorithm. Before it can be set in motion, this rule must be formulated in a manner that guarantees that the procedure is carried out legitimately. In view of this, it must first of all 'incorporate' the principles which regulate administrative activity, among which, in particular, those already mentioned of publicity and transparency. Furthermore, it must be formulated so as to reasonably foresee a definite solution for all possible cases, even the most improbable, as it is not possible for an electronic elaborator to make discretionary assessments. At the same time, the algorithmic rule must undergo continuous tests and updating, in order to allow for constant checking. Last but not least, it must allow the judge to be able to evaluate the correctness of the automatized process in all of its components. Such an aspect constitutes a pivotal element of the reasoning of the Council of State. According to the judges, allowing full cognition and full review by administrative judges of the technical rules which govern the algorithm responds to the need to evaluate the administrative decision under the profile of legitimacy, in that it allows the judge to examine how the power was concretely exercised. As a matter of fact, the impossibility of understanding how the teaching posts were assigned, by means of the algorithm referred to above, constitutes in and of itself an irregularity such as to invalidate the procedure.

II. Opaqueness as a Thread for Weaving the New 'Smart' Ecosystem

The issues faced by the court do not exclusively involve the execution of administrative activities. The growing tendency, both in the public and private sectors, to delegate decision-making processes – previously carried out only by humans – to algorithms raises multiple concerns, which the law is called upon to deal with.[14] Generally speaking, it is possible to distinguish two major issues, which are not separate from each other.

[13] For some further reflections on the topic of human-machine cooperation see C. Misselhorn, 'Collective Agency and Cooperation in Natural and Artificial Systems', in C. Misselhorn ed, *Collective Agency and Cooperation in Natural and Artificial Systems: Explanation, Implementation and Simulation* (London: Springer, 2015), 3.

[14] For an overview of the diverse questions opened up by the use of algorithms in society see A. Carleo ed, *Decisione robotica* (Bologna: il Mulino, 2019); G. Resta, 'Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza' *Politica del diritto*, 199 (2019); S.C. Olhede and P.J. Wolfe, 'The Growing Ubiquity of Algorithms in Society: Implications, Impacts and Innovations' 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 1 (2018).

The first refers to the possibility that the decision-making processes by algorithms lead to discriminatory decisions, due to either defects in their structural functioning or, more often, to bias embedded in the data used to train the software program.[15] To provide some examples consider the case of algorithm-based systems, used by authorities in many US States in order to quantify the risk that an offender may repeat crimes, which results in bias against Afro-Americans;[16] or that of the software used by Amazon to determine areas to benefit from one-day delivery service, which ended up being prejudiced against poor and depressed neighborhoods.[17] In this regard, the need to regulate the gathering and use of data and, more generally, the techniques of data analytics emerges, so as to reduce the risk that the welding between economic and technological power produces decisions which are in violation of fundamental rights.[18]

The second issue, directly taken into consideration by the Council of State, concerns the lack of information regarding how the decisions taken by algorithms are produced, when their modes of functioning are opaque.

[15] F.Z. Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making* (Strasbourg: Council of Europe, 2018). Especially on the correctness of decisions as dependent on data quality see S. Barocas and A.D. Selbst, 'Big Data's Disparate Impact' 104 *California Law Review*, 671 (2016). On discrimination generated by algorithms in employment relationships see D.J. Dalenberg, 'Preventing discrimination in the automated targeting of job advertisements' 34 *Computer Law & Security Review*, 615 (2017); J.A. Kroll, 'The Fallacy of Inscrutability' 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences,* 2133 (2018). With special regards to the impact of algorithms on the public sphere see H. Shah, 'Algorithmic Accountability' 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2128 (2018). As for discriminations related to the creation of clusters by using personal data see A. Mantelero and D. Poletti eds, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (Pisa: Pisa University Press, 2018), 289.

[16] See Supreme Court of Wisconsin, *State of Wisconsin* v *Eric L. Loomis*, Case no 2015AP157-CR (2016). In determining a six-year term of imprisonment for the crime committed by Eric L. Loomis, the judges of the La Crosse circuit court had taken into account the results elaborated by the COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*) software program which identified Loomis as being at a high risk of recidivism. This program is used in various States to calculate recidivism over a two-year period, despite the fact that several studies found it to be systematically biased against African Americans.

The Court concluded that the use of COMPAS did not violate Loomis's right to due process. According to the Supreme Court justices, the risk factor calculated by the software was only one of many considerations taken into account to determine the penalty (and that these were not contested by Loomis). The Supreme Court observed that although the judges of La Crosse court made reference to the results of COMPAS, they had attributed little importance to the risk factor and that they would have reached the same decision in the absence of those results.

[17] The case refers to a study conducted by Bloomberg in 2016 with regards to some depressed areas, such as Bronx, New York and Roxbury, Boston whose inhabitants were denied the service in question. See D. Ingold and S. Soper, 'Amazon doesn't Consider the Race of its Customer. Should it?' *Bloomber*, available at https://tinyurl.com/k36cx4z (last visited 30 December 2019). Both examples are referred to by G. Resta, n 14 above, 215.

[18] G. Resta, n 14 above, 233. As for different modes of regulating data-driven algorithms see M. Hildebrandt, 'Algorithmic regulation and the rule of law' 376 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2128 (2018).

As far as this paper is concerned, the concept of opaqueness refers to the difficulty that a subject who has not taken part in the programming, production or training of the algorithm has in understanding the functioning of the relative software (eg the technical structure which connotes the system or type of data used in the training) and/or the outcome of the decision-making process. This could be caused by a multiplicity of factors. Opaqueness can be, so to speak, 'induced' by its creator/programmer, in order to protect a trade secret concerning the technical formula implemented by the algorithm, so as to reserve for itself the power to utilize and economically exploit the software. It can be associated with the lack of technical competency on the part of the subject (eg consumer or judge) who wants to or must become aware of the mechanism which underlies the algorithm's behavior. Finally, opaqueness can be connected to the unpredictability of the actions carried out by artificial intelligence systems capable of learning and actively interacting within their environment in a manner which can be unique and unforeseeable, even – to some extent – for its own developers.[19]

The problem of opaqueness of the algorithms is capable of affecting all of the relationships mediated by the intervention of 'intelligent' IT systems, whatever the nature – public or only private – of the legal subjects involved is.[20] This may not only impede the discovery of biased and discriminatory decisions, but also affect the correct functioning of the market. In fact, the 'inscrutability' of the algorithm may impinge on, by reducing it, the degree of effectiveness of the protection which, in the new 'smart' socio-economic context characterized by the exponential employment of algorithms, is granted to the citizen-consumer. Indeed, the lack of transparency of the algorithm operates as a sounding board for information asymmetry that, under a plurality of profiles, marks the distance between those market players who operate at the top or intermediate level of the value chain and consumers, who represent the final link in the chain. As a consequence, opaqueness can lead to a 'suspension' of the safeguards foreseen by the multiple norms which are intended to protect consumers within the European Union and to reinforce their (weak) position within the market. Some examples may be useful to clarify these remarks.

1. The Case of Anti-Competitive Algorithmic Behavior

The lack of algorithmic explainability can favor, by hiding it, anti-competitive behavior on the part of the economic actors. There is no doubt that the use of algorithms by the market players, as tools through which to act in the market,

[19] See E. Pellecchia, 'Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation' *Le nuove leggi civili commentate*, 5, 1209 (2018).

[20] For a general overview of the problem see F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge MA: Harvard University Press, 2015).

can foster market efficiency and competition. Nevertheless, the intelligence of those artefacts – which is '*supra*-human' – can also be used by competing firms to enact collusive strategies, with the objective of raising profits to a higher level than the non-cooperative equilibrium.[21]

In a traditional non-algorithmic environment, a joint-profit maximization strategy can be sanctioned as anti-competitive behavior whenever there is proof of a direct or indirect contact, capable of demonstrating that firms have not acted independently from each other (the so-called *meeting of the minds*). However, by employing algorithms – especially in transparent markets with few sellers and homogenous products – firms acquire the capability to pursue anti-competitive strategies without the necessity to conclude formal agreements or, more generally, without the intervention of humans.[22]

In some cases, the algorithms can be utilized as devices intended as facilitators of coordinated behavior,[23] to the extent that they guarantee firms (or market players) the possibility of manifesting their will to undertake a collusive strategy and, at the same time, to implement it without any explicit communication among the players. As an example, the 'signalling algorithms' are software programmed to send – in a continuous and re-iterative way – an indication of market prices, monitor the reactions of other market players and then decide whether to confirm the price in case of alignment or, conversely, to indicate a new price. By means of such a mechanism, a firm can announce its intention to collude with other market players by disclosing information, such as an increase in price, on the basis of which, if followed by other competitors, a collusive strategy can be implemented. In such circumstances, independent and rational behavior – like that of the competitors who 'intelligently' adapt the price of their own goods to that indicated in order to maximize profits – can become part of a collusive strategy even without utilizing the means which are usually required in order to make the conduct sanctionable.

Under this profile, it has been pointed out[24] that in such cases, the behavior of the firm can lead to a 'concerted practice' intended as a form of more informal cooperation among firms, which, despite not being pursued by means of an

[21] See Organisation for Economic Co-operation and Development (OECD), 'Algorithms and Collusion: Competition Policy in the Digital Age' (2017), available at https://tinyurl.com/yx3s4wdt (last visited 30 December 2019); A. Ezrachi and M. E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-driven Economy* (Cambridge, MA: Harvard University Press, 2016). As regards Italian legal literature see G. Pitruzzella, 'Big Data and Antitrust Enforcement' *Rivista italiana di Antitrust*, 77 (2017); P. Manzini, 'Algoritmi collusivi e diritto antitrust europeo' *Mercato concorrenza regole*, 163-164 (2019); A.M. Gambino and M. Manzi, 'Intelligenza artificiale e tutela della concorrenza' *Giurisprudenza italiana*, 1744 (2019); L. Calzolari, 'La collusione fra algoritmi nell'era dei big data: l'imputabilità alle imprese delle "intese 4.0" ai sensi dell'art. 101 TFUE' *Rivista di diritto dei media*, 219 (2018); A. Minuto Rizzo, 'I profili antitrust del nuovo web e della nuova economia digitale' *Diritto Industriale*, 113 (2019).

[22] OECD, n 21 above, 19.

[23] L. Calzolari, n 21 above, 221.

[24] P. Manzini, n 21 above, 171. OECD, n 21 above, 20.

agreement, still produces the effect of eliminating or reducing market competition.[25] More in detail, the use of algorithms allows the firms to undertake those

> 'direct or indirect contacts (...) the object or effect whereof is either to influence the conduct on the market of an actual or potential competitor or to disclose to such a competitor the course of conduct which they themselves have decided to adopt or contemplate adopting on the market',[26]

which are capable of putting the market players in virtual yet effective contact, thus committing an infringement of Art 101 TFUE.[27]

However, the use of algorithms may lead to a restriction of competition, even in the absence of a structure – such as that of 'signalling algorithms' – created by managers to facilitate collusion.[28] Indeed, in the case of algorithms based on machine-learning and deep-learning technologies, they may not even be aware of such a restriction. Differently from traditional algorithms, which are programmed to automatically execute a precise and deterministic series of pre-programmed instructions in order to reach well-defined decisions, 'self-learning algorithms' take their decisions on the basis of data and experience gleaned from their environment, by using predictive models developed by programmers.[29] Such models, incorporated in a software module, are obtained by training the machine through a process of 'trial and error', according to the fundamental cybernetic principle of 'feedback'.[30] In such a way, the machine can adapt its actions to an external environment and produce decisions without the burden of providing complete domain knowledge *a priori*.

When such algorithms are used by companies to maximize their profits, the goal will be pursued by learning from the environment in which they operate and adapting themselves to the actions of other competitors, by for instance automatically setting prices. Therefore, the optimal output – ie the maximization of profit – is achieved without displacing the strategy behind the decisional process, which may be contrary to the rules governing competition law.

Before and besides the issues concerning who should respond for the infringement caused by the algorithm, the opaqueness which characterizes such algorithms can limit the detection of an infringement of competition law norms.

[25] See for example Case C-8/08 *T-Mobile Netherlands BV and Others*, (2009) ECR I-4529; Joint cases 40 to 48, 50, 54 to 56, 111, 113 and 114/73 *Coöperatieve Vereniging "Suiker Unie" UA et al* v *Commission*, (1975) ECR 1663.

[26] See, among others, Case 49/92 P *Commission* v *Anic Partecipazioni*, (1999) ERC I-4162.

[27] To this regard see P. Manzini, n 21 above, 171.

[28] OECD, n 21 above, 19.

[29] For deeper insights into the structure and functioning of these technologies see, among others, N. J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (New York: Cambridge University Press, 2010); R. Calo, 'Robotics and the Lessons of Cyberlaw' 103 *California Law Review*, 513 (2015).

[30] See N. Wiener, *Cybernetics: Or Control and Communication in the Animal and the Machine* (Paris: Herman & Cie, 1948).

If this can result in an obstacle for the public authority, called upon to supervise the behavior of market actors, it will be even more complex for consumers to initiate actions for damages, especially when they 'stand-alone'.[31] Considering that the consumer may not even be aware of the use of algorithms by competitors and, in any case, will lack information about their mode of functioning, the capacity of private antitrust enforcement to play a role in contrasting collusive behavior or the concentration of power among a reduced number of (technologically empowered) market players may be curtailed, even more than it is at present.

2. The Case of Damage Caused by Fallible Algorithms

Similar problems seem to affect the area of liability law. Differently from previous hypotheses, in which opaqueness may constitute a 'desired' characteristic of the algorithm, being an expression of its correct functioning, in this second sphere the problem emerges as a consequence of the fallibility which can connote the actions of intelligent machines.

It is by now well-known, both on institutional and doctrinal planes, that the use of products endowed with 'intelligence' will increase not only the functional features of previously 'inanimate' objects, but also the occasions for damage that they can generate. It is equally clear, however, that when damage is associated with a smart product, above all when founded on self-learning systems, the application of the discipline intended to manage the re-allocation of risks among parties becomes more difficult.[32] Under this profile, attention is centered on the subject who should be burdened with the risk for damage caused by a decision that, being based on accumulated experience of the algorithm, may not appear to be ascribable to the manufacturer of the device. Thus, in the attempt to find a point of equilibrium between the need for consumer safety and technological-economic development, various solutions have been proposed which oscillate between the two extremes of the attribution of liability to the producer of the smart device,[33] of which the self-learning algorithm would constitute a component[34]

[31] As disciplined by European Parliament and Council Directive 2014/104/EU concerning actions for damages for infringements of the competition law provisions (Official Journal of the European Union, 5 December 2014, L 349/1), which was transposed in the Italian legal system by decreto legislativo 19 January 2017 no 3 (Gazzetta Ufficiale 19 January 2017 no 15).

[32] The liability problems posed by the use of smart products and artificial intelligence is currently under study by the European institutions. See in particular European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015) 2103(INL); Commission Staff Working Document, Liability for emerging digital technologies, Accompanying the document, Communication from the Commission, Artificial intelligence for Europe, Brussels, (2018) 137 final. For a deeper look into these issues see also U. Ruffolo, 'Intelligenza artificiale, machine learning e responsabilità da algoritmo' *Giurisprudenza italiana*, 1689 (2019); A. Amidei, 'Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione europea' *Giurisprudenza italiana*, 1715 (2019). E. Palmerini, 'Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea' *Responsabilità civile e previdenza*, 1816 (2016).

[33] See in this regard the insights offered by A. Bertolini, 'Robots as Products: The Case for

or to the machine itself.[35] However, even in this case, the aforesaid inscrutability of the algorithm could, indeed, render vain any choice of legislative policy. Machine failure could be connected to an inadequate or insufficient testing and training phase; to the use of information and records which were inadequate for the construction of the software model, in light of the functions for which it was designated; further still, it could be due to the development of software characterized by a low level of accuracy, so that, despite having been trained in an adequate way, it presents a wide margin of error. In light of this, the duty to prove the existence of a defect in the algorithm or, more in general, to demonstrate the illicitness of its conduct would risk inhibiting an effective protection of the consumer. In other words, it is to be asked how consumers can absolve the duty of demonstrating the elements at the basis of their claim, when they cannot have at their disposition – due to technical reasons – the information regarding the way in which the device functions.[36]

3. The Case of Automated Decision-Making Process in Data Protection

In the one case (correct functioning) or the other (poor functioning), the opaqueness of the algorithm may also affect the ability to effectively exercise the rights recognized for a physical person whose data is the object of automatized processing. EU Regulation no 679 of 2016 on the protection of natural persons with regard to the processing of personal data (GDPR)[37] contemplates the possibility for the controller to carry out the operations performed on personal data or sets of personal data, solely by automated means, that is, without human intervention.[38] This regards in particular, but not exclusively, the activity of profiling which is the 'automated processing of personal data' by which personal information or behavioral patterns of individuals or groups of individuals are

A Realistic Analysis of Robotic Applications and Liability Rules' *Law Innovation and Technology*, 214 (2013).

[34] A. Amidei, n 32 above, 35.

[35] A. Matthias, 'The responsibility gap: Ascribing Responsibility for the Actions of Learning Automata' 6 *Ethics and Information Technology*, 175 (2004); G. Teubner, 'Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten' 218 *Archiv für civilistische Praxis*, 155 (2018). Italian version: Id, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi* edited by P. Femia (Napoli: Edizioni Scientifiche Italiane, 2019).

[36] A. Amidei, n 32 above, 35.

[37] European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (2016) OJ L119/1. For a broad overview of the Regulation see G. Finocchiaro et al, *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101* (Bologna: Zanichelli, 2019); P. Voigt and A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (New York: Springer, 2017).

[38] Art 29 Data Protection Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 6 February 2018, available at https://tinyurl.com/r7kb8dx, 8 (last visited 30 December 2019).

gathered and analyzed, so as to create suitable clusters for the purpose of predicting human behavior and preferences (Art 4, para 4, GDPR). On this front, the Regulation establishes a general prohibition on subjecting the natural person to a decision based solely on automated processing, including profiling, which produces legal effects concerning the subject or significantly affects him or her in other ways (Art 22, para 1, GDPR). There are, however, some hypotheses in which the use of automated processing in the absence of human intervention is legitimate. In particular, the controller can use a fully automated, decision-making process when the data subject has explicitly expressed his or her consent or when such a tool is necessary for the controller to enter into, or for the performance of, a contract between the data controller and the data subject (eg, the selection of a great number of candidates (Art 22, para 2, GDPR).[39]

According to the legislator, however, the absence of human intervention in the decision-making process of the IT system, when admissible, cannot result in compromising or limiting the data subject's rights, freedoms and legitimate interests. The Regulation ensures that the controller implements suitable measures to safeguard such rights while guaranteeing, at least, a way for the data subject to obtain human intervention, express their point of view, and contest the decision.[40] However, the management and control, on the part of the data subject, of the data elaborated by the algorithm may be restricted by a lack of understanding of its functioning mechanisms. Consider the case in which an algorithm is given the task of deciding, without human intervention, whether to grant a loan to a subject based on imprecise projections; or, another still, the case in which such a loan is denied by a human being due to derived or inferred data such as the profile of the individual created by means of an algorithm (eg a credit score),[41] on the basis of an incorrect classification owing to biased data.[42] In such cases, it is clear that the effective possibility for the data subject to exercise his/her rights, depends on whether he or she has access to the evaluation processes which led to the imprecise projections or incorrect classifications.[43]

[39] The other hypothesis in which a solely automated decision-making process can be carried out regards the case in which the decision is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subjects rights and freedoms and legitimate interests (eg to combat tax evasion).

[40] Art 29 Data Protection Working Party, n 38 above, 42.

[41] See in this regard D.K. Citron and F. Pasquale, 'The Scored Society: Due Process for Automated Predictions' 89 *Washington Law Review*, 1 (2014).

[42] See in particular A. Mantelero and D. Poletti eds, n 15 above. F. Pizzetti, 'La protezione dei dati personali e la sfida dell'Intelligenza Artificiale', in Id ed, *Intelligenza artificiale, protezione dei dati personali e regolazione* (Torino: Giappichelli, 2018), 30; M. Temme, 'Algorithms and Transparency in View of the New General Data Protection Regulation' 3 *European Data Protection Law Review*, 473, 481 (2017).

[43] Art 29 Data Protection Working Party, n 38 above, 27.

III. Transparency in the General Data Protection Regulation

From the observations expressed so far, it is easy to note how the lack of complete information associated with more or less autonomous IT systems can compromise, to the point of sabotaging them, the principles and rules that govern the discipline set down to safeguard consumers and their role as market actors placed at the end of the value chain. To be sure, the consequent loss of faith on the part of consumers can create a significant obstacle to the construction of a single, digital market.[44]

If, at least at the legislative level, the debate regarding (tacit) collusion as well as liability for damage caused by algorithms is still in an embryonic stage, some interesting insights as to how foster transparency can be drawn from the set of rules introduced by the GDPR. The Regulation has, in fact, outlined some provisions intended to face the problems associated with the opaqueness of automatic processes.

1. The Right to Explanation

The theme of transparency, in the perspective of the GDPR, runs on a twofold track. The first one has, so to speak, a substantial nature and concerns the breadth and the content of the right, recognized for the data subject, to be informed of the processing of his or her data. From this angle, the focal point of the discussion revolves around the question of whether, in cases regarding processing carried out by means of automated mechanisms, such a right implies an actual claim to explanation of the decision taken by the algorithm.[45] What causes the various interpretations on this matter to differ is the circumstance for which the European legislator – as a result of the negotiation that characterized the legislative process which culminated in the final text – has explicitly recognized a right 'to obtain an explanation of the decision reached after such assessment and to challenge the decision'; however, this provision was inserted into a Recital – the 71st, thus depriving it of the strength of a binding rule. According to some researchers,[46]

[44] All of the legislative efforts of the European Union aim to enhance the trust of consumers, so as to foster the new data economy. See European Commission, A Digital Single Market Strategy for Europe (Communication), Brussels, (2015) 192 final. See also European Commission, Artificial intelligence for Europe, Brussels (Communication), (2018) 237 final, where it is stated that in order to strengthen trust, citizens 'need to understand how the technology works'. Hence, the Commission points out the importance of research into the explainability of AI systems.

[45] See S. Wachter et al, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' 7 *International Data Privacy Law*, 76 (2017); G. Comandé and G. Malgieri, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' 7 *International Data Privacy Law*, 243 (2017); G. Finocchiaro et al, n 37 above; E. Pellecchia, n 19 above.

[46] See for example A. D. Selbst and J. Powles, 'Meaningful information and the right to explanation' 7 *International Data Privacy Law*, 233 (2017); B. Goodman and S. Flaxman, 'European Union regulations on algorithmic decision-making and a "right to explanation" ' *ArXiv:1606.08813*, available at https://tinyurl.com/wccrg29 (last visited 30 December 2019).

such a provision should acquire a binding nature on the basis of a systematic interpretation of the GDPR and, in particular, of Artt 13, para 2, lett (f), 14, para 2, lett (g) and 15, para 1, lett (h) of the GDPR. These provisions foresee, in the case of an automatized decision-making process pursuant to Article 22, the right of the person involved to receive 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'. As noted by the (ex) Article 29 Data Protection Working Party, such information is of particular relevance whenever the understanding of the purposes for collecting personal data and by whom they are being collected is rendered difficult due to technological complexity.[47] In light of this, the (growing) complexity – associated with machine learning based algorithms – should not exempt the data controller from providing such pieces of information.

According to other scholars, the actual existence of the right to explanation in the GDPR depends on the way in which such a right is understood, as concerns the object and timing of the explanation.[48] In particular, the wording of the abovementioned articles – which refer to 'the envisaged consequences of the processing' – would entail that the data subject's right to be informed is to be exercised prior to automated decision-making taking place. However, such an *ex ante* explanation may only refer to the usage and the *system functionality* of the algorithm, intended as the general and abstract mode of producing decisions starting from given datasets of information. This would include, for example, the system's requirement specifications, classification structures and pre-defined models. However, the information would not encompass an explanation of the rationale, reasons and circumstances surrounding the specific, individual outcome of the algorithmic process. Indeed, such an explanation, which would require, for example, the disclosure of the specific information as regards data or profile groups used by the algorithm, can only be offered after the decision has been made.[49] Conversely, other scholars argue that the formulation of the text, as used by the legislator to describe the information to be provided to the data subject, implies, when specifically referred to the right of access (Art 15, para 1 (h) GDPR), the possibility of requesting the disclosure of information at any time and, thus, even after the decision has been made. [50] Consequently, the data subject shall have the right to be informed not only about the (abstract) architecture of the algorithm used, but also about the contextual implementation in which the algorithm performed its tasks in order to reach the specific decision involving a data subject.

In any case, such an explanation – even where it is recognized by way of interpretation – would face other difficulties in order to be offered. As noted

[47] Art 29 Data Protection Working Party, n 38 above, 25.

[48] See S. Wachter et al, n 45 above, 78.

[49] ibid.

[50] See G. Comandé and G. Malgieri, n 45 above, 246.

above, the right to receive an explanation may be limited – or should be balanced – with the interest (or right) of the producer of the algorithm not to disclose the formula (source-code) on which the software is based, so as not to lose the competitive advantage to be gained through his investments in software development.[51] Furthermore, as noted above, the investigation into the decisional process may turn out to be particularly difficult – especially with regards to machine-learning systems – due to both the technicality of the machine programming language or to other technical factors, such as the use of self-learning systems, whose outcome may be – to a certain limit – unpredictable. The subsequent unintelligibility for individuals of the algorithmic modes of production of actions may impede – *de facto* – not only the exercise of the (asserted) right to explanation, but also the possibility of charging the controller with the responsibility for an error in the algorithmic decision.

2. The Intersection Between the Principles of Accountability and Transparency by Design

Along with and beyond the recognition of a right to explanation, the theme of opaqueness takes on, in the sphere of EU Regulation 2016/679, a second declination which has been less investigated by legal doctrine, even though it is perhaps more decisive. Under close inspection, the discipline drawn up by the legislator – if observed from the perspective of the obligations imposed on the controller rather than the rights of the data subjects – outlines the fundamental points of a remedial approach which, under certain profiles, mirrors the rationale of the arguments set down by the Council of State.

What shines light on this second interpretative path is the intertwining of the principles of transparency and accountability. The principle of transparency constitutes, along with that of lawfulness and fairness, one of the cardinal principles which must underlie any processing activity as defined by the Regulation (Art 5, para 1, lett (a) GDPR). Such a principle is strengthened by some provisions which are meant to ensure (*ex ante*) that the processing is carried out in a transparent manner.

First of all, the transferal of knowledge from the controller to the data subject – which is the ultimate goal of transparency – should be executed by taking appropriate measures to render the information in ‘a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]’ (Art 12 GDPR). This reinforced declination of the principle of transparency finds confirmation also with reference to the set of information that the controller shall supply in order to ensure the fairness and transparency of the process executed by means of an automated decision-making process. Indeed, the wording

[51] As explicitly stated by the Regulation (EU) 2016/679, in Recital 63, the right of the data subject to receive information ‘should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software’.

used by the legislator in Artt 13, para 2, lett (f), 14, para 2, lett (g) and 15, para 1, lett (h) of the GDPR, and in particular the expression 'meaningful information', suggests that the principle of transparency – whether it is substantiated as the right to receive mere information or to an effective explanation about the decision made – should be combined with that of 'comprehensibility' of the algorithm, so as to guarantee the capability of individuals to autonomously understand the functioning and the impact of algorithms used to process their data.[52] In this sense, for example, the mere release of the source code of an algorithmic system would not provide 'meaningful' transparency.[53]

This also appears coherent with the disposition foreseen by Art 22, para 3, of the GDPR. The paragraph recognizes the right of the data subject to challenge the decision, thus making, at least under this profile, the *ex post* approach of Recital 71 binding. It is evident that a decision can be challenged by the data subject only to the extent to which he/she can have full understanding of how and on what basis the decision was made.[54] From this angle, it is possible to observe how the rationale followed by the GDPR reappears in the ruling of the Council of State: both unveil the essential necessity to translate the technical rule that guides the machine into a language that is comprehensible for citizens and/or judges.

However, there is more. The legislator does not merely shed light on the necessity to render the algorithm 'comprehensible'. Rather, the Regulation under examination also seems to establish the modes by which such a requirement shall be fulfilled, in order to avoid sanctions. In fact, the controller is not simply burdened with the obligation to guarantee transparency; he/she must also demonstrate that the necessary measures have been adopted in order to guarantee such transparency. What determines the latter duty is the principle of accountability introduced by the Regulation.

The term accountability is polysemous and appears, in turn, opaque.[55] Generally speaking, the term refers to the ability to account for a certain action. In the specific ambit of the EU Regulation on data protection, this concept is split into two parts, as emerges from the same notion put forth in para 2, of the

[52] See G. Comandé and G. Malgieri, n 45 above, 245, who refer to such a concept as *legibility*.

[53] European Parliamentary Research Service, 'A Governance Framework for Algorithmic Accountability and Transparency', Study managed by the Scientific Foresight Unit, within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, Brussels, March 2019, available at https://tinyurl.com/tes3903 (last visited 30 December 2019).

[54] Art 29 Data Protection Working Party, n 38 above, 27.

[55] As highlighted by the Art 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability', WP 173, 13 July 2010, available at https://tinyurl.com/r7kb8dx, 7 (last visited 30 December 2019). The difficulties in finding the precise meaning of the term are compounded by translation. In Italian the term is usually translated as *responsabilizzazione*, a term which lacks the nuances of English. See also on this concept, G. Finocchiaro, 'Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali', in Id et al, n 37 above, 1.

above-mentioned Art 5: 'the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1'. On one hand, this disposition implies 'the need for a controller to take appropriate and effective measures to implement data protection principles', among which, indeed, is the principle of transparency; on the other, the controller must be able to demonstrate – by providing evidence – that those appropriate and effective measures have been taken.[56]

In this light, the concept of accountability would seem to take on a technical-IT meaning. The proof of transparent processing appears to be dependent on the possibility of demonstrating that the algorithm has been programmed to be transparent. Indeed, several technical methods exist which may reduce opaqueness or 'extract' an explanation for the machine's behavior.[57] These mechanisms need to be designed into systems and, thus, require the intervention of their system developers and operators.[58]

To be sure, the adoption of these systems can be a challenging task in practice, especially when facing black-box algorithms that make inherently autonomous decisions and might contain implicit bias.[59] Yet, the principle of accountability, as interpreted herein, can stimulate the responsible development (in addition to responsible use) of such intelligent systems, in view of the protection of citizens.[60]

After all, this perspective appears to be coherent with – by giving it application – the principle of 'privacy by design' which characterizes the regulatory framework laid down by the legislator. This concept imposes that controllers find technical solutions, in addition to organizational ones, to be adopted both at the time of the determination of the means for processing and at the time of the processing itself, so as to satisfy the principles underlying data processing. More precisely, Article 25 requires the controller to provide for

> 'appropriate technical and organisational measures [...] which are designed to implement data-protection principles [...] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects'.

[56] Art 29 Data Protection Working Party, 'Opinion 3/2010' n 55 above, 9.

[57] European Parliamentary Research Service, 'Understanding Algorithmic Decision-making: Opportunities and Challenges', March 2019 available at https://tinyurl.com/v4p902f, 51 (last visited 30 December 2019). J.A. Kroll et al, 'Accountable Algorithms' 165 *University of Pennsylvenia Law Review*, 633 (2017), available at https://tinyurl.com/qnstj2f (last visited 30 December 2019). See also D. Pedreschi et al, 'Open the Black Box Data-Driven Explanation of Black Box Decision Systems' *Arxiv abs/1806.09936* (2018).

[58] European Parliamentary Research Service, 'Understanding' n 57 above, 34. See also OECD, n 21 above, 47.

[59] It has been suggested that data controllers may be obliged to use, in some cases, human interpretable decision-making methods. See for example J. Burrell, 'How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms' *Big Data & Society,* 1 (2016). In this sense see also S. Wachter et al, n 45 above.

[60] H. Nissenbaum, 'Computing and Accountability', in D. G. Johnson and H. Nissenbaum eds, *Computers, Ethics and Social Values* (London: Pearson, 1995), 526.

These measures, as expressly specified in Recital 78, also include those intended to offer transparency as regards the functioning and processing of data. At the same time, Article 24 foresees the responsibility of the controller, should he not ensure and be able to demonstrate that he/she implemented such measures.

Moving backwards along the observations put forward, it is possible to detect how the problem connected to the transparency of algorithms, when analyzed from the obligation imposed on the controller, transcends, at least in part, the distinctions which have emerged with respect to the right to explanation of algorithmic behavior. Indeed, the principle of accountability, when applied to the hypothesis of automated decision-making processes, such as those conducted by algorithmic systems, would seem to indicate that the data controller – beyond consideration of the breadth of the data subject's right to be informed – is required to develop the algorithm in such a way that the decision can then be explained. Under this profile, the normative framework of the GDPR exhibits a tendency to make the fulfillment of the obligation on the part of the data controller dependent on how the IT systems used to implement the processing were developed and programmed. From this point of view, the relevance given to the human-machine cooperation during the developmental stage seems to mirror the logic of the decision adopted by the Council of State.

IV. Towards a New Remedial Perspective?

These final elucidations, though they may seem subtle at first, offer significant insights, in a prospective sense, into facing the problem of algorithms' opaqueness even beyond the sphere of the GDPR. That the model drawn up by the Regulation – and structured on the transparency by design and accountability binomial – has expansionary potential is witnessed by numerous documents published by European institutions. It is sufficient to note that in the 'Artificial Intelligence for Europe' communication released in 2018, the Commission affirmed that in order to increase transparency and minimize the risk of bias or error, 'AI systems should be developed in a manner which allows humans to understand (the basis of) their actions'.[61] Then again, in the more recent communication on 'Building Trust in Human-Centric Artificial Intelligence',[62] it has been pointed out that persons affected by an algorithmic decision-making process should be provided with an explanation of the same to the furthest extent possible. To this end, the Commission has emphasized that research to develop explainability mechanisms should be pursued. Moreover, the perspective of 'compliance by design' appears to be envisaged at the institutional level in the specific realm of competition law

[61] European Commission, 'Artificial' n 44 above, point 3.3.

[62] European Commission, 'Building Trust in Human-Centric Artificial Intelligence' (Communication), Brussels (2019), 168 final.

regulation.[63] On a doctrinal level, it has been pointed out that the most promising solutions to governing algorithmic decisions include instruments intended to regulate the programming phase, according to a sort of 'legality by design'.[64] This perspective seems to be able to find fertile ground not only when fundamental rights are involved, but also in those fields in which the protection of private actors also permits fostering more general interests.

What has been little investigated are the consequences of what a re-reading of the previously discussed legal disciplines in light of the combination of accountability and transparency by design principles could produce on the front of attribution of liability for actions or decisions carried out by algorithms. According to general principles of law, liability for the adverse effects provoked by an algorithm (regardless of which person – whether physical or legal – is called upon to respond) would require proof that those effects were the consequence of the automated decision-making process. However, as noted in the previous sections, finding that proof can end up being particularly complex, when the opaqueness of the algorithm does not make it possible to explain how the relative decision was reached.

In this scenario, the introduction of the concept of accountability of the algorithm could lead, so to say, to an anticipation of the threshold of protection. Should the rationale and logic introduced by the GDPR be extended to other areas, liability would be assigned to the responsible party, not only in the case of an infringement of law and damage caused by algorithmic decisions, but also whenever he/she is not able to account for the relative decision-making processes. In other words, the party could be held responsible for decisions made by the algorithms employed, even if – and due to the fact that – it is not possible to explain how the algorithms produce their results.[65] To be sure, provisions of this kind would need to be fashioned differently according to the context in which the algorithm is used as well as the sort of technology employed to execute the decision-making process. Furthermore, they would have to take into account the need to defend competitive advantages for the creators of the software code and formulas, when protected by intellectual property and trade secrets law.[66]

[63] According to EU Commissioner Vestager, an obligation to program algorithms so as to comply – by design – not only with the set of rules concerning data protection but also with antitrust law should be imposed on companies. See OECD, n 21 above, 47. With respect to competition law, some authors proposed establishing a series of rules, to be followed in the development phase of the software, so as to ensure more transparency. See A. M. Gambino and M. Manzi, n 21 above.

[64] G. Resta, n 14 above, 234.

[65] See in this regard the principles set down by the Association for Computing Machinery, US Public Policy Council (USACM), 'Statement on Algorithmic Transparency and Accountability', l, Washington, DC, 2017, available at https://tinyurl.com/qkslara (last visited 30 December 2019).

[66] This necessity is expressly stated in the EU Regulation on data protection, Recital 63, in which it is also affirmed that such rights or freedoms should not lead to a refusal to provide all information to the data subject. See for further analysis on this topic S. Wachter, B. Mittelstadt and L. Floridi, n 45 above, 90.

However, what is worth noting is that such an approach seems to indicate a re-centering of the axis of liability. The risk, from a legal point of view, would not (only) be associated with the decision made by the algorithm, but (also) with that of the subjects who are involved in the programming and development stage: the latter would be burdened with the costs, to a certain extent inevitable, of unexplainable decisions.

In the final analysis, the concept of accountability emerges as a device (even if not the only one) through which the legal system, having realized the complexity of algorithms, re-adapts its rules in order to make their ineluctable uncertainty tolerable.