LUISS

Department of *Business and Management*

Management and Computer Science

Chair of *Business Cyberlaw*

Algorithmic Transparency Between Legal and Technical Issues

SUPERVISOR

Prof. Silvia Scalzini

CANDIDATE

Giovanna Di Toro

ID 230231

Academic year 2020/2021

TABLE OF CONTENTS

INTRODUCTION 3

1. THE ALGORITHMIC WORLD 5
   - 1.1. Artificial Intelligence (AI) and Machine Learning (ML) 5
   - 1.2. Algorithmic Decision making 6
   - 1.3. An oversight over society: the use of algorithms in the public realm and in the private realm 7
     - 1.3.1. The public realm 7
     - 1.3.2. The private realm 10
   - 1.4. The context: Big Data 12
   - 1.5. Challenges: Bias and Opacity and Black Box 14

2. TRANSPARENCY 16
   - 2.1. The notion 16
   - 2.2. The relation with accountability 18
   - 2.3. Challenges 21
     - 2.3.1. Some recent decisions within the Italian case-law 22
       - 2.3.1.1. Deliveroo Italia srl. case, Bologna Court 22
       - 2.3.1.2. MIUR case, TAR Lazio 24

3. THE NEED FOR TRANSPARENCY. LEGAL AND TECHNICAL ISSUES: SOME CASE STUDIES 26
   - 3.1. GDPR, AI and Transparency 26
     - 3.1.1. Legal Challenges 29
       - 3.1.1.1. Trade Secrets 30
     - 3.1.2. Technical Challenges 33
   - 3.2. Transparency within the Platform to Business (P2B) Regulation 35
     - 3.2.1. Legal Challenges 38
     - 3.2.2. Technical Challenges 40

4. TOWARDS MORE COMPREHENSIVE AND SPECIFIC SET OF RULES 43
   - 4.1. The proposals for the Digital Services Act and the Digital Markets Act 43
   - 4.2. The proposal for an Artificial Intelligence Act 47

CONCLUSION 50
REFERENCES 52

INTRODUCTION

Transparency represents a fundamental starting point for the algorithmic-based intelligence applications; the "right to decipher automated decision-making" comes to be a fundamental principle of the Fourth Industrial Revolution.[1]
Yet, it is not easy to achieve.

Modern society is built upon a flow of continuous technological innovation heading towards full digitization. Data is the "new oil"[2], since it constitutes the main resource of the new digital economy. In this setting, algorithms are central as they are equipped with powerful and rapid data processing skills.
In ways human intervention would not allow, algorithms are able to process, select and distribute huge quantities of data.
This is particularly relevant in terms of Artificial Intelligence (AI) and Machine Learning (ML) systems which have a certain degree of autonomy as they can "learn" from their "experience" and accordingly perform tasks and make decisions[3].

To date, it is possible to observe that the ubiquity of algorithms has potentially revolutionary effects in people's daily life, as well as in the business and administrative contexts. The activities of individuals are, indeed, scanned and often influenced by the results of the work done by algorithms. Also, the sudden expansion of networks and the web, with the consequent volume of content therein, requires the help of intermediaries, such as online platforms and search engines, to access services and navigate the information online.

In this framework, there is the need for a precise focus on the challenges and pitfalls associated with the algorithmic applications, as they may entail biases leading to flawed and discriminatory

[1] Bonafè M., Trevisi C., Intelligenza artificiale, l'algoritmo "trasparente": un rebus ancora da sciogliere, Agenda Digitale, 2019. https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-lalgoritmo-trasparente-un-rebus-ancora-da-sciogliere/#Diritto_alla_trasparenza_degli_algoritmi
[2] Parkins D., The world's most valuable resource is no longer oil, but data, The Economist, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data
[3] Italiano G. F., Le sfide interdisciplinari dell'intelligenza artificiale, in "Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa" eds. A. Nuzzo and G. Olivieri, 1/2019, pp. 9-20.

outcomes[4] or may be so opaque that it is very difficult to understand why and how a certain result was produced.

Faced with this situation, the notion of algorithmic transparency appears, therefore, necessary.

However, technical factors get in the way: algorithms' outcomes and decisions may not lend themselves to human interpretation. This is particularly relevant in the context of Machine Learning systems which behave as a "black box".[5]

On legal grounds, instead, the achievement of transparency must face an intricate setting where two main factors are at stake: several interests, including economic interests, related to trade secrets and other costs of information disclosure, must be balanced with transparency needs.

This work aims at examining in detail algorithmic transparency for businesses and its implications, by examining two case studies of algorithmic regulation within the EU legislation. The analysis of the current European legal framework on the matter goes hand in hand with the assessment of the technical specifications: a multidisciplinary proceeding enables a clear and comprehensive overview on an ever-expanding and evolving sector in order to be able to propose solutions encompassing interdisciplinary challenges.

Such an approach is useful not only to the scope of this research. When applied to the development of new regulatory frameworks, it may drive to terrific achievements. It may, indeed, allow for the setup of an efficient balancing system which encompasses social and technological advancements, as well as the safeguard of commercial interests and of fundamental rights in terms of privacy and non-discrimination.

The European Union is moving steps towards this direction in its effort to build up a comprehensive strategy to implement transparency and boosting innovation.

In this sense, then, transparency would become factual, other than just fundamental.

[4] Scalzini S., Alcune questioni a proposito di Algoritmi, Dati, Etica e Ricerca, in Rivista Italiana di Medicina Legale e del Diritto in campo sanitario 1/2019, Focus. Tutela dei dati personali concernenti la salute e attività di ricerca: considerazioni interdisciplinari nella prospettiva etico-giuridica, 2019. pp.169-178.

[5] Pedreschi D., Giannotti F., Guidotti R., Monreale A., Pappalardo L., Ruggieri S., Turini F., Open the Black Box Data-Driven Explanation of Black Box Decision Systems, in ArXiv Preprint, N. 1/2018.
Pasquale F., The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015.

1. THE ALGORITHMIC WORLD

1.1. Artificial Intelligence (AI) and Machine Learning (ML)

There is a lack of a precise, universally accepted definition of AI. The notion of "intelligence lies on a multi-dimensional spectrum"[6]. This makes reasonable to choose the human intelligence as the benchmark for the progress of AI[7]. For this reason, AI is usually conceived as the capability of a machine to imitate intelligent human behaviour[8], and also describes the section of computer science that handles the simulation of intelligent behaviour in machines[9].

There are different types of applications. The most basic AI is typically useful to improve the performance of business analytics solutions, since it embeds some cognitive abilities such as memory and language. It is also capable of basic decision-making. Some applications are chatbots or smart speakers.

More advanced AI goes further by closely mimicking the human brain and allows for the analysis of unstructured data such as texts, images, and audio data. Application domains include facial and speech recognition, medical diagnoses, urban planning, as well as logistics, transportation and security.

The direction undertaken is leading towards autonomous forms, with AI becoming self-aware and able to interact with human beings and learn on its own, thereby augmenting humans both in private and in public environments.[10]

AI performance has been massively enhanced by ML.

[6] Stone P., Brooks R., Brynjolfsson E., Calo R., Etzioni O., Hager G., Hirschberg J., Kalyanakrishnan S., Kamar E., Kraus S., Leyton-Brown K., Parkes D., Press W., Saxenian A., Shah J., Tambe M., Teller A., Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University, 2016. http://ai100.stanford.edu/2016-report.
[7] Stone et al. 2016, supra, note 6.
[8] Italiano G. F., Le sfide interdisciplinari dell'intelligenza artificiale, in "Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa" eds. A. Nuzzo and G. Olivieri, 1/2019, pp. 9-20.
[9] Artificial Intelligence. (n.d.). The Merriam-Webster.Com Dictionary. Retrieved June 5, 2021, from https://www.merriam-webster.com/dictionary/artificial%20intelligence
[10] Strusani D., Houngbonon, G. V., The Role of Artificial Intelligence in Supporting Development in Emerging Markets, 2019.

Rule-based algorithmic systems work with predefined instructions by a simple "if → then" logic. As such, their abilities limit to predictable outcomes and they are not capable of efficient performances out of sample.

Machine learning, instead, is an AI component that provides systems with the capacity to improve through experience. The learning process is based on observations of data, generally in large amounts, in order to identify patterns, make better predictions and come up with another algorithm, which can be referred to as model.

Basic learning algorithms are suitable for analysing structured data like price, quantity, or time. They are useful to predict an outcome given a set of inputs or to cluster items according to their features. For example, they are used for fraud detection in financial transactions.

A higher degree of complexity, instead, is embedded in deep learning algorithms. These involve several learning stages and are able to analyse unstructured data such as images, audio recordings, or texts. They are indeed useful for face recognition, speech-to-text transcription, or text reconstitution.

These types of algorithms utterly open new avenues for data-driven decision-making.

1.2. Algorithmic Decision making

The aforementioned technologies appear to be significantly modifying decision-making processes, innovating their rationale as well as the intrinsic power relationships, with a remarkable impact not only on privacy and human rights, but also, more generally, on the economic and social development.[11]

The success and the growing diffusion of automated decision systems based on algorithms is due to their tendential greater efficiency with respect to the analytical human capacities: predictive algorithms are capable of analysing huge quantities of data, even heterogeneous from the qualitative point of view, detecting useful correlations that the human mind would miss.

[11] Olhede S.C., Wolfe P.J., The growing ubiquity of algorithms in society: implications, impacts and innovations, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2018, 376.2128: 20170364.

The relationships, the correlations, the inferences and patterns used by the algorithm with predictive decisional purpose, sign a vertical increment of the quantitative element which implies in terms of probability, a substantial quality leap with respect to human forecasting.

Moreover, although there exists the chance that an algorithm is biased[12], such bias often occurs because automated decision-making systems were trained using biased human decisions.

The impact of AI systems should be considered not only from an individual perspective, but also from the perspective of society as a whole. The use of AI systems can have a significant role in achieving a sustainable progress and in supporting the democratic process and social rights[13].

This comes, on the other side, with some challenges that is worth to deepen later in this analysis.

1.3. An oversight over society: the use of algorithms in the public realm and in the private realm

1.3.1. The public realm

The thriving possibilities and applications of algorithmic systems have brought the attention on the possible consequences of the development of models which are based on an increasingly intense and pervasive algorithmic governance[14] and policy-making. As increasing numbers of policymakers and administrators come to rely on artificial intelligence (AI) and algorithmic systems, a change in how public administrations works and how public goods and services are administered is to be forecasted.

[12] The absence of undesired bias corresponds to fairness. Algorithmic bias leads to discrimination and it may arise from training data, technical constraints, or societal or individual inclinations. However, it is not peculiar: humans have their degree of bias too. Castelluccia C., Le Métayer D., Understanding algorithmic decision-making: Opportunities and challenges, European Parliament, EPRS, STOA, 2019.
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf
[13] Burgess P., Algorithmic augmentation of democracy: considering whether technology can enhance the concepts of democracy and the rule of law through four hypotheticals, AI & Soc, 2021. https://doi.org/10.1007/s00146-021-01170-8
[14] Danaher J., The Threat of Algocracy: Reality, Resistance and Accommodation, Philos. Technol. 29, 245–268, 2016. https://doi.org/10.1007/s13347-015-0211-1

This reliance on data-based decision-making for public goals is enabled by the proliferation of digital instruments and repositories of governance applications[15] as well as by the reliance on Big Data and increasingly more complex forms of data analysis.

In the public sector, such systems are being used both to provide new services and to improve the existing ones. Energy, transportation, healthcare, education, the judicial system and security are some of the sectors involved. For instance, concerning the healthcare sector, in the EU context particular attention has been paid to the development and deployment of tracing and warning apps to monitor and break the chain of coronavirus infections. The European Commission intervened by issuing Recommendation 2020/518 [16]. While aiming at "a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data", the EC intervention had also to stress that any use of apps and data must respect data security and EU fundamental rights, such as privacy and data protection. The document paved the way for an EU-wide strategy on how to use data and technology in tackling the coronavirus outbreak.

In the field of social security, AI-powered fraud detection enables the identification of fraudulent patterns, allowing to track down large-scale corruption, to the benefit of social security.[17]

Likewise, AI technologies can be deployed for crime prediction and surveillance, supporting an efficient police patrol presence. Though, AI fairness in predictive policing is still debatable matter and tends not to favour minority groups. Also, mass surveillance enabled by facial recognition technologies is controversial on the ethical side, as may lead to racial profiling and violations of basic human rights and freedoms[18].

[15] The "global learning platform for government", APOLITICAL is an example of such tools. It is "co-designed and funded by Governments" and "equips public servants to do their jobs" through free access to courses, articles, events and connections. https://apolitical.co/home

[16] European Commission, Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID- 19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, 2020 OJ(EU) L 114/7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518&from=ENendation%202020/510

[17] Castelluccia C., Le Métayer D., Understanding algorithmic decision-making: Opportunities and challenges, European Parliament, EPRS, STOA, 2019.
https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf

[18]Kantarci A, AI Ethics in 2021: Top 9 Ethical Dilemmas of AI., AIMultiple, 2021. https://research.aimultiple.com/ai-ethics/#surveillance-practices-limiting-privacy

In addition, such smart technologies can enhance city management in general, allowing for the monitoring of energy consumption, the reduction and monitoring of traffic congestion, the improvement of pollution and waste management, as well as the enhancement of emergency systems management, through a more systematic handling.

AI, and specifically ML techniques, also contribute to society by producing new knowledge.

They also have a role in supporting administration decisions and the related transparency and accountability.

While, on the one hand, these technologies represent an enhancement opportunity for the functioning and development of the society, on the other hand, if compromised, they can cause considerable harm. Without considering that algorithmic systems could be purposely used to alter information and to injure the democratic integrity[19].

States and interest groups could be tempted to use these technologies to influence citizen behaviours. Distort information may be used to leverage social media targeted advertising, psychological profiling and the propagation of fake news[20].

Security vulnerabilities could be exploited by malicious actors causing major damages, given the increasingly central role of algorithmic technologies. As attacks too will become more automated and complex, it will be harder to put valid protective actions in place.

A large and growing number of applications for algorithms use is at stake in the public sector. Progress in this area can bring large benefits. Algorithm assisted decision-making may in some cases be more consistent and accurate than the human one.

The use of algorithms to make complex, high-impact decisions arise concerns about possible unfair outcomes and the risk of reinforcing existing biases.

Hence, there is the widespread idea that technological innovation must be paired with a high level of public accountability and monitoring over safe algorithm use. Greater transparency has been considered as a solution to the different problems posed by the algorithm usage in the public sector.

[19] Castelluccia C., Le Métayer D., 2019, supra, note 17, p. 22.
[20] Castelluccia C., Le Métayer D., 2019, supra, note 17, p. 36.

Transparent access to key information encompasses the data on which algorithms are trained and validated, their degree of bias, their attested effects on individuals, as well as on the society, and the role that humans cast throughout the decision-making processes.[21] It comes to be very valuable since transparency may help building public trust and pose the necessary supervision over decision-making processes.

This impacts the future role of such technologies in the society. Establishing trust in the use of algorithm decision-making will be crucial in easing the concerns about the dangers of the "government by algorithm", the idea that algorithms are increasingly displacing human decision-making in disruptive ways.

1.3.2. The private realm

The use of algorithms is of a paramount importance also in the private sphere. The expression the 'Fourth Industrial Revolution' portrays an impactful change.

New jobs will develop, while some of the existing ones are changing or are destined to disappear. This holds in particular for those tasks which are repetitive or that could significantly profit from the analysis of high volumes of data.[22]

The production, collection and storage of a huge mass of information together with the processing by increasingly complex algorithms characterize the market model of the digital age. The information, therefore, becomes the pivot around which goods and services are designed and developed.

Companies are enabled to tailor their services to the individual needs of users, to reorganize production processes more efficiently and to improve decision-making capacity. This can boost both the volume of profitable business opportunities and the level of competition within markets and industries.

[21] Reese S., Algorithmic transparency in the public sector, Reform and Imperial College London's The Forum Policy Hackathon, 2021. https://reform.uk/sites/default/files/2021-05/Hackathon%20Write%20Up%20Final.pdf
[22] Castelluccia C., Le Métayer D., 2019, supra, note 17, pp. 37-38.

AI solutions may also help overcome the lack of infrastructure and information asymmetries in emerging markets by supporting innovation in terms of new business models and state-of-the-art solutions tailored to address previously unserved and underserved communities.

In many cases the data and the algorithmic systems processing become a real production surplus: they create new profit opportunities and set up an overall redefinition of the balance of power.

Hower, this gives rise to potential conflicts between commercial opacity and democratic transparency. As a matter of fact, the trade secret protection, together with degrees of complexity, may grant business using algorithmic systems a layer of protection from legal and public surveillance. [23]

In addition, it must be taken into account that through the exercise of private autonomy the appropriation of such data as well as the functioning of the algorithm builds forms of exclusivity, making use of contractual conditions and commercial secrets.

It is the case of digital platforms whose acquisition of behavioural information for profit scopes is object of an intense debate on disparity in bargaining power between digital platforms and users, on asymmetrical distribution of information[24] and on market manipulation which occur in the data economy.

Knowledge about the way machine-learning applications embedded in products and services work is central for consumers to be in control of their life as consumers.

As these technologies may drive towards forms of data accumulation exploitative abuse, transparency may be crucial to grant consumers freedom of choice. Choice is not only relevant in terms of being able to choose amongst different products. For consumers to have a free choice also means that they are not being manipulated into taking certain decisions.

However, because of the black-box nature of many applications, it may be challenging to get access to clear, concise, meaningful and verifiable information granting consumers clarity and control at the right moment. This is also one of the requirements of the GDPR.

[23] Lu S., Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial intelligence 23(1), 2020.

[24] Ranchordas S., Online Reputation and the Regulation of Information Asymmetries in the Platform Economy, Critical Analysis of Law, 2018, Forthcoming, University of Groningen Faculty of Law Research Paper No. 2/2018. https://ssrn.com/abstract=3082403

As a matter of fact, the consumers are threatened also as individuals due to the fact that comprehensive data collection may culminate in a loss of privacy.

The increasingly more advanced data analytics tools make it possible to infer sensitive information, also from apparently non-personal data such as meta-data. If misused, such insights can have direct effects on core social values and principles including individual autonomy, equality and freedom of speech. [25] For instance, discrimination triggered by data analytics may lead to greater efficiencies, but, at the same time, bound an individual to pre-existing socio-economic factors that may be potentially harmful.

This poses challenges also on the applicability of the core principles (*e.g.*, the definition of personal data, awareness and consent) on which privacy protection relies.

1.4. The context: Big Data

Algorithms need large amount of data for their functioning.

The volume of data produced in the world follows a rapid growth and is expected to reach 175 zettabytes in 2025.[26]

This of course comes with some challenges and risks which call for an effective protection of data referred to individuals. Nonetheless, innovation is not to be considered incompatible with the retain of fundamental rights.

Big data can provide noteworthy benefits and efficiencies for society and individuals in areas such as healthcare, scientific research, the environment. They can also allow for new business models which rely on novel capabilities for the gathering, combination and use of information.

As a matter of fact, the exponential growth of information sets up for inferences that no human evaluation would be able to understand. [27] This determines both a quantitative and qualitative upgrade.

[25] OECD, Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, 2015. https://doi.org/10.1787/9789264229358-en.
[26] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, 2020. https://ec.europa.eu/info/sites/info/files/commissi on-white-paper-artificial-intelligencefeb2020_en.pdf
[27] Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L., The ethics of algorithms: Mapping the debate, Big Data & Society, 2016.

Machine learning and predictive algorithms are in fact able to analyse very large amounts of data and this marks a clear quantitative advantage over the feasible human work. Though this data could also be qualitatively heterogeneous, such advanced technologies are capable of identifying precious relationships, correlations, inferences and behavioural patterns that would escape the human mind.

However, data-driven decision making could also unexpectedly lead to false results. This may be caused by poor quality data, flaws due to the improper use of data and analytics, or to changes in the environment from which data are collected.

The risk of taking the wrong decisions opens the debate about who has to be held liable among decision makers, data and data analytic providers and who should be the controllers of such decision-making.

Added to this, the notion of "ownership" puts in place specific challenges when applied to data. Data typically is subject to different rights across different stakeholders who, according to their role, have also different power over the data themselves.

In case of personal data, this is indeed complex, since generally data subjects are granted with explicit control rights which cannot be restricted.

As pointed out by the OECD[28], one of the main challenges is to balance the tension between the need of a free flow of data across the global data ecosystem and the safeguard of individuals' and organisations' opposing interests. In particular, the interest in privacy protection on one hand, and the economic interests on the other hand.

This calls for a comprehensive dialogue and coordination between governments, business groups, the technically skilled community, as well as, citizens through their democratic participation.

[28] OECD 2015, supra, note 14.

1.5. Challenges: Bias and Opacity and Black Box

The usage of algorithms does not limit at granting a greater efficiency. It is important that the algorithmic process is correct, legitimate and effectively accurate. This, in particular in the field of algorithmic decision-making, is essential to respect the rights of subjects who are formal addresses or simply undergo the effects of such decisions.

Simply digitalising a process does not expunge it of fundamental biases and vulnerabilities. Algorithmic systems are often regarded as neutral, impartial tools based on objective calculations. Actually, they are designed by humans and feed on data provided by them.

The need for a sort of "accountability by design" is generally recognized, but because of the gap in the human reasoning that the algorithms fill, it is not that easy to achieve.

Therefore, the quality of the data sets used is crucial. They must be sufficiently large and representative so that they do not display pre-existing social and cultural constructs.

Intelligence is a "value-laden concept" with an historical role in patriarchy, racism and ideologies of superiority and inferiority.[29]

The discrimination can lay already in the programming phase, in data that lead to inequitable decisions[30]. According to the garbage in - garbage out (GIGO) logic, inaccurate or outdated data can only produce unreliable, biased decision-making results. This give rise to "cognitive biases" [31] which may also be directly related to the human ones.

In other circumstances, biases may be due to the process itself. This happens not because the system is "bad", but because it "learns" wrong behaviours that it then repeats[32].

[29] Cave S., The Problem with Intelligence, Its Value-Laden History and the Future of AI, Leverhulme Centre for the Future of Intelligence, University of Cambridge, 2020.

[30] Predictive policing algorithms are racist. They need to be dismantled, MIT Technology Review., 2020. https://www.technologyreview.com/2020/07/17/1 005396/predictive-policing-algorithms-racistdismantled-machine-learning-bias-criminaljustice/

[31] Malgieri G., Comandé G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law, Volume 7, Issue 4, 2017. pp. 243-265. https://doi.org/10.1093/idpl/ipx019

[32] Pellecchia E., Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation in Le nuove leggi civili commentate, 1209-1236, 2018. pp. 7-10.

In the case of "statistical biases"[33], the algorithm will reflect the possible unbalance of the dataset given as input, as it processes such data through a statistical analysis which enables it to find patterns and perform the task.

Therefore, as one may easily understand, it is fundamental to focus not only on the result of the algorithmic decision, but also on the methods and criteria laying under it. This brings particular attention to transparency and human surveillance which is especially relevant in the European legal framework[34].

However, to have a complete and clear understanding of the factors involved in algorithm design and configuration is not straightforward.

The decision-making capacity of learning algorithms may not allow for clear insights on the factors and processes influencing a particular choice. This may exacerbate the chasm between algorithms design and human understanding[35].

This is the theme of the so-called "black box" [36] containing the intricate machine learning architectures of AI.

ML algorithms have a certain degree of autonomy. They are not based on absolute programming, correlations and inferences replace causality. This means that the machine does not work solely on the basis of the parameters introduced in advance by the programmer, but has the autonomous ability to adopt decisions, to carry out assignments, to make predictions and to output accurate results starting from certain instructions.

Such algorithms, exactly as a black box, can only be described in their external behaviour and their internal functioning is unknown.

In this sense, algorithms can be so opaque that it may not indeed be known which parameter contributed to which aspect of the result delivered[37].

---

[33] Malgieri, Comandé 2017, supra, note 28.

[34] The EU adopts an anthropocentric approach to deal with AI technologies. European Parliament, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence (COM (2019)168).

[35] Mittelstadt et al. 2016, supra, note 17.

[36] On the theme of "black-box", a great contribution comes from Frank Pasquale who proposed a social theory on the intentional exploitation of this feature. Due to private companies tightly shielding it and unavailability to public, too much algorithmic decision-making remains a black box. The massive unbalance of powers this phenomenon carries has heavy consequences in shaping personal reputations, as well as new media audiences and financial strength. Frank Pasquale. Pasquale F., The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015.

[37] In particular, Jenna Burrell classifies the opacity as: (1) intentional business or state secrecy, (2) technical illiterate, in case only the ones equipped with the expert knowledge can understand the functioning of an algorithmic system, and

This concept contrasts with the so-called "white box" model, in which the operations of a given system are transparent and known. [38]

There are different types of algorithms. Their functionalities and abilities are not the same either. Some of them are not understandable because they have the ability to define and even modify the decision-making rules themselves.

Thus, a trade-off emerges: the degree of accuracy within the decision-making of algorithms occurs at the expense of transparency.

2. TRANSPARENCY

2.1. The notion

Algorithmic transparency is aimed at acquiring the ability to identify the source of the data flows exploited and created by AI systems, to portray and accurately replicate the mechanisms by which these models make specific decisions and learn to adapt to the context.[39]

It helps to detect the causes of misbehaviours by the model, allowing for corrective measures that avoid their replication.

Beyond the data and the system, transparency should be adopted also to the extent to which an AI system impacts and molds the organisational decision-making process and to the reasons behind the choice of using it[40].

(3) intrinsic which is the one concerned with black box systems. Burrell J., How the machine 'thinks': understanding opacity in machine learning algorithms. Big Data Soc 3:205395171562251, 2016. https://doi.org/10.1177/2053951715622512

[38] Loyola-González O., Black-Box vs. White-Box: Understanding Their Advantages and Weaknesses From a Practical Point of View, 2019. IEEE Access. 7. 154096-154113.

[39] Kossow N., Windwehr S., Jenkins M., Algorithmic transparency and accountability, Transparency International Anti-Corruption Helpdesk Answer, 2021.

[40] European Parliament, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence (COM(2019)168).

Moreover, users should be aware of the fact that they are interacting with an AI system, that should be therefore identifiable, and they should also know which people have the responsibility over it. [41]

Albert Meijer (2014) [42] distinguishes between three broad connotations of transparency and such distinction come to be useful both for the normative and social applications of transparency[43]:

- Transparency as an individual feature. Transparency intended as the inherently feature of systems, organizations, agents to be clear about their work, intentions and behaviours. This particular approach to transparency does not address the determination of the target to whom an actor should be transparent.
- Transparency as a relational notion. Transparency cannot be understood outside the relation between an agent and a recipient. This means that it is relevant how the agents' efforts in being clear are perceived and received by recipients.
- Transparency as a systemic notion. Transparency understood within an institutional context requires a clear understanding of the specific features of such context in order to figure its application and impact out.

Transparency is tied to explanations and explainability. These refers both to the *ex-ante* access to information about the proceeding and quality of a process and the *ex-post* access to the results and the way they came out. Legal scholars debate revolves around the kind of explanation data protection rules require.

Transparency is relevant also in relation to trust. Transparency can signal the ability of a technology to perform as expected and the fact that actors choose to disclose private information may be perceived as sign of integrity. This may have effects on the society as a whole through the adoption of collaborative behaviours enabling the digital progress boost.

[41] European Parliament, COM (2019)168, supra, note 39.
[42] Meijer A., Transparency, eds. M. Bovens, R. E. Goodin, & T. Schillemans, The Oxford handbook of public accountability (pp. 507–524), Oxford University Press, 2014.
[43] The following description of the distinction follows the work of Felzmann, H., Fosch-Villaronga, E., Lutz, C. et al., Towards Transparency by Design for Artificial Intelligence, Sci Eng Ethics 26**,** 3333–3361, 2020. https://doi.org/10.1007/s11948-020-00276-4

2.2. The relation with accountability

The idea of accountability is strictly related to the one of transparency. Mechanisms should be put in place to ensure the obligation to justify and ensure responsibility for AI systems and their outcomes, before and after their implementation.[44] This, from a technical perspective, is relevant to grant the correct allocation of responsibility in questions which involves algorithms and decision processes.[45]

As a matter of fact, the knowledge gained from the understanding of a system's logic, enabled by transparency, may serve as provision to hold that system accountable.

Transparency and accountability are strongly related but not synonymous. Accountability extends the notion of transparency as "transparent workings of a system" to "why this system was deemed 'good enough' at decision making".[46]

On the subject the Association for Computing Machinery [47] provided seven "Principles for Algorithmic Transparency and Accountability" which are key.

"1. Awareness: Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society.

2. Access and redress: Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affected by algorithmically informed decisions.

[44] Castelluccia C., Le Métayer D., 2019, supra, note 17.
[45] Comandé G., Responsabilità ed accountability nell'era dell'Intelligenza Artificiale in Giurisprudenza e Autorità Indipendenti nell'epoca del diritto liquido, eds. F. Di Ciommo, O. Troiano, La Tribuna, 2018. pp. 1001, 1013. Comandé Giovanni, Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità, Analisi Giuridica dell'Economia, 1. 169-188, 2019.
[46] Wieringa M., What to account for when accounting for algorithms: A systematic literature review on algorithmic accountability, in Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020. pp. 1–18.
[47] Association for Computing Machinery, Principles for Algorithmic Transparency and Accountability, 2017. https://www.acm.org/binaries/content/assets/pub lic-policy/2017_joint_statement_algorithms.pdf

3. Accountability: Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results.

4. Explanation: Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts.

5. Data Provenance: A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals.

6. Auditability: Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected.

7. Validation and Testing: Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public."

This sets out the ground for an increasingly stronger reliance on intelligent algorithmic systems. The seven requirements for a trustworthy AI, proposed by a High-level Expert Group[48], are helpful to that scope.

These are:

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and Data governance
4. Transparency
5. Diversity, non-discrimination and fairness
6. Societal and environmental well-being
7. Accountability

[48] European Commission, Ethics guidelines for trustworthy AI High-Level Expert Group on AI, 2019.

Building on that, the Commission introduced six types of requirements for high-risk AI applications in its White Paper on AI[49]:

1. ensuring quality of training data;
2. data and record-keeping of the programming of AI systems;
3. information to be provided in a proactive manner to various stakeholders (transparency and explainability);
4. granting robustness and accuracy;
5. carrying human oversight;
6. and other specific requirements for certain particular AI applications, such as those used for purposes of remote biometric identification.

These specifications are further reinforced by the role transparency is given in the safeguard of human rights. It is a step towards the safe and fair use of AI[50]: systems which do not allow for human assessment [51]are not in line with the protection of human rights which is of outmost importance for the EU standards.

Transparency is thus considered crucial. This of course requires continuous and regular documentation, monitoring and assessment both from the technical viewpoint, by supervisioning the algorithmic systems at every stage of their life, and from the legal perspective, in particular in data protection rules, consumer protection rules and even business to business rules.

[49] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, 2020. https://ec.europa.eu/info/sites/info/files/commissi on-white-paper-artificial-intelligencefeb2020_en.pdf

[50] According to the Council of Europe, transparency is part of the 4th step towards the protection of human rughts in the cintext of AI and "Systems that cannot be subjected to appropriate standards of transparency and accountability should not be used." Council Of Europe Commissioner For Human Rights, Recommendation – Unboxing Artificial Intelligence: 10 steps to protect Human Rights, Strasbourg: Council of Europe, 2019. https://rm.coe.int/unboxingartificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

[51] Pasquale F., Le nuove leggi della Robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale, Luiss University Press, 2020.

2.3. Challenges

Algorithmic transparency aims at understanding both the general process behind the functioning of algorithmic systems and the path through which an algorithmic system comes out with an individual result. In relation to this, depending on whom a system is intended to be transparent for, different degrees of transparency may be required. The technical properties of such systems have also to be taken into account.

On legal grounds, transparency as a way to overcome information asymmetries must deal with the fact that public disclosure of information serves to balance powers to the extent that the state of transparency grants everyone with the relevant rather than complete information.

Transparency may expose sensitive and private data. In particular, when dealing with machine learning algorithms using personal data for the training step. A full transparency may therefore result problematic for the privacy right.

Moreover, some issues may arise for businesses in cases in which being more transparent would threat their advantage on the market.

Also, it must be considered that information does not only need to be disclosed: it has to be received and understood by the audience it is addressed to.

Administering algorithms is intrinsically a balancing task. On the one hand, private individuals and entities subjected to an algorithmic-made decision, have the right to get to know its modus operandi. On the other hand, algorithms may be a source of competitive advantage for businesses, and any disclosure may go against the interest of the company.

On technical grounds, there are often limitations to a systematic approach.
Looking over the inner workings of a system does not necessarily lead to understanding and controlling it. Artificial intelligence systems are increasingly complex, the instructions could be unsupervised by programmers and therefore hardly understandable.
Transparency is required to challenge al the possible biases and opacities.

This must be integrated with a cognitive and human perspective with social considerations.

The lack of algorithms' oversight is socially unacceptable.[52]

However, this is not an easy matter neither from a legal nor from a technical point of view: the protection of individuals' and businesses' rights and interests may collide with the transparency request.[53]

This sets the ground for further analysis. A path can be detected within the European Union regulatory framework and it is worth to investigate it through some case studies, that will be treated in Chapter 4, for the sake of clarity and completeness.

2.3.1. Some recent decisions within the Italian case-law

Despite the huge reliance of the current society on algorithms, the exercise of balance between legal, economic and technical interests with regard to transparency has still a long way to go.

In particular, when such transparency is the core of judiciary claims, the Courts decisions contribute to build up a path towards future expertise.

The following analysis focuses on two recent cases within the Italian legislation which are leading the way in the national debate over of algorithmic transparency.

2.3.1.1 Deliveroo Italia srl. Case, Bologna Court[54]

Machine-learning algorithms are central to the Deliveroo's business model. It relies on "Frank", a ML-based algorithm which uses great amounts of data to provide

[52] On this matter, the work of Frank Pasquale, Le nuove leggi della Robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale, Luiss University Press, 2020, is particular interesting. He proposes a framework of collaboration between humans and AI technologies, against a disrupted scenario where human beings are substituted.

[53] Lo Sapio G., La trasparenza sul banco di prova dei modelli algoritmici, Osservatorio sulla trasparenza 21 aprile 2021, Federalismi.it, 2021. https://www.segretaricomunalivighenzi.it/archivio/anno-2021/aprile/doc-lo-sapio.pdf

[54] Tribunale di Bologna, 31.12.2020

"real-time operational monitoring", to make predictions and decisions about drivers in real-time, to handle orders according to these decisions.[55]

In the Deliveroo case, however, the Bologna Court held that precisely this algorithm had discriminatory outcomes.

In particular, "Frank" was entitled to distribute work slots using a priority system derived from a digital platform downloaded on smartphones. This system was based on a "score" awarded by the riders which would have been negatively affected if a rider failed to cancel a shift pre-booked through the app at least 24 hours before its start.

This led to huge differences in the amount of work available. Riders with the highest score were first to be offered access to sessions and could quickly "fill up" available slots. This at the expenses of riders with lower scores who had fewer job opportunities in the future.

The applicants alleged that the system was indirectly discriminatory because of the way in which riders were given priority, since there could be good reasons, such as illness or serious emergencies, why riders did not participate or needed to cancel in peak times.

The court recognized that the system was not able to sensibly differentiate between riders. It lacked an individual assessment mechanism allowing for a fairer score calculation.

Lack of transparency was a key element in the Deliveroo case: neither the algorithm allowed for a clear and comprehensive understating of its functioning, nor Deliveroo did provide insights on the mechanisms and criteria adopted.

This was, exactly, the underlying reason of the Court decision to held "Frank" discriminatory.

[55] Outside Insight. How Deliveroo uses machine learning to power food delivery. (2018, November 26). https://outsideinsight.com/insights/how-deliveroo-uses-machine-learning-to-power-food-delivery/

A system capable of intelligently differentiate between the reason for cancellation or inability to work would have prevented discrimination from arising.

The case is indicative of the growing attention of the judicial system to tackle black-box algorithms. This, indeed, will require increasingly more consideration as algorithmic applications will be ever more embedded in different sectors of the society and, therefore, will pose questions on matters such as individuals' rights and labour protections as in this particular scenario.

It, accordingly, marks a step towards a legal framework where individuals' protection and technological innovation go hand in hand, with the former guiding, rather than hindering, the latter.[56]

2.3.1.2 MIUR case, TAR Lazio

The two cases, T.A.R. Lazio Roma Sez. III bis, Sent., 21/03/2017, n. 3742 and T.A.R. Lazio Roma Sez. III bis, Sent., 22/03/2017, n. 3769, the Italian Administrative Court of Lazio (TAR Lazio) ruled over the request by a number of Italian trade unions against the Ministry of University and Education ("MIUR") of getting access to the algorithm used by MIUR to manage the territorial mobility procedures of the teaching staff.

In the Administrative Court's opinion, if an algorithm is used to handle an administrative process which may have an impact on the rights or legitimate interests of individuals, it is to be regarded as part of the administrative proceeding itself, which is subject to the right to access of interested parties and as such it must be transparent and accessible.

[56] Amoruso G. M., Nicotra M., Deliveroo, l'algoritmo che discrimina: perché è importante la sentenza del tribunale bolognese, Agenda Digitale, 2021. https://www.agendadigitale.eu/sicurezza/privacy/deliveroo-lalgoritmo-che-discrimina-perche-e-importante-la-sentenza-del-tribunale-bolognese/

The Court also ruled over what effectively constitutes transparency. Attempts by the MIUR to soothe the objecting teachers by submitting them the software house's brief, were not considered enough.

It was clarified that the source code of the algorithm enjoys the nature of electronic administrative document and as such only full access to it could grant interest parties a comprehensive understanding of the algorithm's underlying functioning.

The ruling of TAR Lazio shed light on some relevant legal implications of the widespread use of AI algorithms in decision-making processes, and paved the way for an ever-increasing use of artificial intelligence in Italy's public administration.

On the side of full knowledge, the principle of transparency has a prominent importance, both for the public administration holder of the power for the exercise of which the use of the algorithm tool is envisaged and for the subjects affected.

On the subject of transparency, it has been clarified that the mechanism through which the robotic decision is made concrete (i.e., the algorithm) must be "knowable".

This is in order to be able to verify that the criteria, conditions and results of the algorithmic procedure comply with the requirements and purposes established by the law or by the administration itself.

Furthermore, also the prerogatives of those who create and economically exploit the algorithm are stake and, in these cases, the priority is to safeguard the industrial secret and intellectual property.

In this perspective, the Court ensured that the information to be provided does not goes beyond what is needed to fulfil the interests of the applicants.

This may not be easy to achieve because of opacity other than the economic interests at stake.

The opacity would be attributable to the difficulty of making the algorithmic functioning easily known both to the recipients of the provision, and to the judges, so as to make the connections between the data and the results achieved comprehensible, ensuring the transparency of the administrative action.

That is why the regulatory action is a balancing task which requires careful assessment of both legal and technical challenges.

3. THE NEED FOR TRANSPARENCY. LEGAL AND TECHNICAL ISSUES: SOME CASE STUDIES [57]

As the technology advances and the use of algorithms for decision-making is exponentially growing, the legal regulation calls for "algorithmic transparency" and, in particular, for the disclosure of the logic behind the algorithm that adopts a certain decision. Algorithmic transparency embraces different transparency degrees from the uncovering of a source code to the explanation of its functioning.

Legally speaking, transparency is an important requirement within the process of algorithmic decision-making to the extent that it is necessary to ensure the respect of fundamental rights of people, or, in general, to enhance the predictability and accountability of the whole process.

Technically speaking, different decisions might require different degrees of algorithmic functioning explanation.

3.1. GDPR, AI and Transparency

Personal data processing through the use of opaque algorithms could give rise to information asymmetries between data subjects and data controllers which may be harmful for individuals involved. [58] This poses obstacles in understanding the reasons behind algorithmic systems' discriminatory outcomes.

The EU data protection law[59] acknowledges the tangible harms which could result from automated data processing and profiling activities.

[57] These case studies with specific reference to the legal challenges of the interface between transparency rules *vis-à-vis* trade secrets protection are also explained by Silvia Scalzini in Trade Secrets And Data-Driven Innovation In The Eu, in Comandé, G. (ed.), Encyclopedia of Law for Data Scientists, EdwarElgar, 2021, forthcoming. Here the perspective is integrated also by technical considerations and challenges to the fulfilment of the goal of achieving a sufficient level of algorithmic transparency.
[58] Dalgıç Ö., Algorithms Meet Transparency: Why There is a GDPR Right To Explanation?, Turkish Law Blog, 2020. https://turkishlawblog.com/read/article/221/algorithms-meet-transparency-why-there-is-a-gdpr-right-to-explanationg
[59] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 OJ L 119/1.

Transparency is a central principle in the GDPR, as it promotes the strengthening of lawful and fair processing of personal data, accountability, and rights of individuals whose personal data are "collected, used, consulted or otherwise processed".[60]

The transparency obligations begin at the data collection stage and apply throughout the processing.

The principle of transparency of data processing requires that the information to the data subject is "concise, easily accessible and easy to understand"[61] and also that the data subject is informed "of the existence of the processing operation and its purposes".[62]

Under Article 5, "lawfulness, fairness and transparency" are fundamental requirement in the data processing. For the accountability principle laid out in Article 5.2, the data controller "must be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject."

Even if not explicitly defined in the GDPR, transparency consists in specific practical requirements on data controllers and processors as drawn in Articles 12-14.

Article 12 outlines general rules on transparency, which apply to the provision of information (Articles 13-14) and communications with data subjects concerning their rights (Articles 15-22).

According to these rules information to data subjects must be concise, transparent, intelligible, easily accessible and must use clear and unambiguous language and terminology. Such information must be provided to data subjects by different means, being them written, electronic or oral upon request and it shall not be conditional upon payment, it must be provided "free of charge".

Among these rules, Article 22 regulates automated decision-making, including profiling. According to it "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning

[60] Recital 39, GDPR
[61] Recital 58, GDPR
[62] Recital 60, GDPR

him or her or similarly significantly affects him or her". However, the right shall not apply if solely in case:

(a) if the decision "is necessary for entering into, or performance of, a contract between the data subject and a data controller";

(b) "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 subject's rights and freedoms and legitimate interests"; or

(c) "is based on the data subject's explicit consent"

Paragraph 3 of the article additionally states that in the circumstances (a) and (c) the data controller is obliged to "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."

Such suitable measures shall ensure a certain level of algorithmic transparency and, to this scope, they must encompass specific information and explanation to the data subject (Recital 71).

Article 22 states that the data subject has a right not to be subject to a decision based exclusively on automated processing.

According to the GDPR, profiling means processing of personal data in a way to use it to "evaluate certain personal aspects relating to a natural person", such as for example "to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (Article 4).

Profiling is a type of processing mostly leading to automated decisions.

On the one hand, Article 22 reflects somehow a scepticism towards misleading decisions and biases of automated systems when no human intervention supervise them. On the other hand, it guarantees the data subject certain rights, given that they cannot influence such automated decisions.

Therefore, a careful assessment is needed since there could be cases in which such decisions affect people because of data that can indirectly relate to them.

Indeed, within this scope, data subjects are entitled to obtain meaningful information about logics, significance and consequences of automated decision making as stated by Articles 13(2)f, 14(2)g and 15(1) h.

However, the broad nature of Articles 13-15 and 22 of GDPR and the technical limitations arise issues about their scope and applicability. In particular, the question is on whether these provisions provide a "right to explanation" for data subjects. [63]

Another perspective is given by Article 25 of the GDPR which places the rule for a data protection by design, and so for the implementation of the notion of transparency already at the early stages of the design of algorithmic systems.

In this case, the legal rule is integrated into the planning of the phenomenon to be regulated, it technically conforms its object from the inside by imposing design constraints that make the application legally compatible with fundamental principles and rights.

3.1.1. Legal Challenges

The GDPR somehow establishes a certain level of algorithmic transparency.[64]

It may be contested that Article 22 has a limited applicability since it only applies to "decisions based solely on automated processing". This could mean that a sort of a "right of explanation" for the data subject, together with the safeguards of Article 22(3), may not be applied whenever there is even a minimal human intervention. [65]

[63] Article 22 does not mention a "right to explanation". Yet, Article 22(3) encompasses the data controllers implementation of safeguarding measures if automated decision-making process meets requirements of Article 22(2). More explicitly, Recital 71 could be interpreted as a base for the "right to explanation" as it introduces the "right to obtain an explanation concerning algorithmic data processing" as a safeguard. The limitation is that in EU legislation, recitals do not establish legally binding rights, they simply provide guidance and help national legislations to interpret the provisions.

[64] Malgieri, Comandé 2017, supra, note 28.

[65] Wachter S., Mittelstadt B., Floridi L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 2017, p.92.

However, it is not clear if such "explanation" should be exclusively about the functioning of an algorithmic system or it should comprehend specific algorithm feature that affected the decision. [66]

Moreover, these articles cover different fields. According to Article 13(2)(f) and 14(2)(g) data controllers are obliged in a proactive manner to notify data subjects before the automated decision activity starts. Article 15(1)(h), instead, introduces an ex-post explanation by granting the right to access automated processing activities details at any time. [67]

Such issues prove that the simple existence of a requirement of algorithmic transparency does not ensure its smooth practical implementation. This is due to technical issues, as well as other legal obstacles which may impair an effective understanding of the reason behind an algorithmic decision. Valuable and confidential information such as trade secrets can stand in the way of algorithmic transparency.

3.1.1.1. Trade Secrets

As stipulated by the Trade Secrets Directive[68],a trade secret is information which meets three requirements (Article 2(1)):

i. It is secret;
ii. it has commercial value due to its secrecy;
iii. and it is subject to reasonable steps by the information holder to keep it secret.

If a piece of information meets these requirements, it has to be considered a trade secret. Article 4, which regulates the unlawful acquisition, use and disclosure of trade secrets, with a very extensive expression, refers to "any

[66] Malgieri G., Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations, Computer law & security review, 2019.
[67] Edwards L., Veale M., Slave To The Algorithm? Why A 'Right To An Explanation' Is Probably Not The Remedy You Are Looking For, Duke Law & Technology Rev, 2017. p.52. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855.
[68] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced".

Recital 1 explains that the "valuable know-how and business information, that is undisclosed and intended to remain confidential, is referred to as a trade secret". Trade Secrets come into play very commonly when dealing with the creation and know-how of businesses (Recital 3).

According to these, algorithms may be classified as trade secrets to the extent that they are pieces of information, in particular, instructions, aiming at performing a production-related task.

Therefore, algorithms can fall within the definition, and so can be protected as trade secrets, as long as they satisfy the above-mentioned requirements.

However, as one may understand also from Recital 14, to protect the meaning, and so the task algorithms pursue, is pointless, since generally they are already known.

Such algorithms may represent a source of significant competitive advantage for their owners. This is why they want to be granted with the protection of the intrinsic structure of instructions and of the syntax which is where the economic value effectively lays.[69]

The relevance of trade secrets and the resulting tension with data subject's rights to access and information protection is also encompassed by the GDPR.

Article 23 of the GDPR limits these rights to the protection of "the rights and freedoms of others"**.** While, Recital 63 explicitly states that the right to access should not "adversely affect" the trade secrets of the controller.

[69] Maggiolino M., Eu Trade Secrets Law and Algorithm Transparency, in L. C. Ubertazzi, AIDA, XXVII, Giuffrè Francis Lefebvre, Milano, 2018. p. 202.

The Trade Secrets Directive lays down suspension of a trade secret "for the purpose of protecting a legitimate interest recognised by Union or national law" (Article 5).

On the one hand, such legitimate interest may have the potential of explaining an algorithmic decision to a data subject. On the other hand, a trade secret should not affect data subjects' rights, in particular, as specified by Recital 35, the right of access to the "personal data being processed". [70]

Therefore, on legal grounds, it is challenging to comprehensively find a balance.

In this setting, the principle of proportionality may help.[71]

Indeed, the extent to which a trade secret (i.e., the underlying functioning of the algorithm) has to be disclosed may depend on the scope of the explanation.

To make an example, if an algorithm protected by a trade secret is to be disclosed to the competent judicial authorities, this has to be ensured as long as there is no further disclosure of the trade secret to anyone not involved in the legal proceedings. This may fall within the scope of Article 9 of Trade Secret Directive in "legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret".

It may be, moreover, possible to detect a path for the regulation of black-box systems which are subject to trade secrets. According to Article 3(1)(b), if a product or object has "been made available to the public" and the disclosure of the trade secret is the result of "observation, study, disassembly or testing", the acquisition of the trade secret is considered to be lawful.
This means that further analysis based on black-box testing, *i.e.* an automated explanation of the algorithmic inner functioning, or on the use of reverse engineering may be allowed by the law in order to obtain explanations.[72]

[70] Brkan M., Bonnet G., Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas, European Journal of Risk Regulation, 11(1), 18-50, 2020. p.41. doi:10.1017/err.2020.10
[71] Scalzini S., Trade Secrets And Data-Driven Innovation In The Eu, in Comandé, G. (ed.), Encyclopedia of Law for Data Scientists, EdwarElgar, 2021, forthcoming.
[72]Brkan M., Bonnet G., 2020, supra, note 70, p.41.

3.1.2. Technical Challenges

The right to explanation in the context of data protection could be central in granting transparency and its impact.

Hence, once the right to explainability is recognized, the problem could take on further articulations. It is to be understood what must be explained, what level of analyticity it must be expected, how to solve the dilemma between explainability and the black box, which characterizes the artificial intelligence applications of machine learning and deep learning.

On legal grounds, GDPR applicability may be limited in cases where algorithmic decisions involve non-personal or anonymized data. However, anonymisation of data is not sufficient as long as the data subject remains identifiable. The use of big data, which benefits from increasing importance, greatly facilitates re-identification of data subjects. The classification of them into specific categories (man/woman, low/high income) enables collective decisions pertaining not only individuals, but also the groups they belong to.

In order to comply with the GDPR it is not sufficient to inform data subjects that the decisions are based on a decision policy determined before knowing the inputs and that the outputs can be reproduced as the policy is the same for every decision.

GDPR requires a particular kind of transparency: the data subject has to understand reasons behind the decision. This poses issues in case of automated decision-making based on algorithms since numerous complications arise when it comes to the explanation of the reasons underlying a decision.

Typically, behind automated-decision making there are ML algorithms, prone to very fast learning while processing data. In such cases, to guarantee transparency is a very complex task.

The amount of technical obstacles standing in a way of explaining algorithmic-based autonomous decisions depends on the complexity of an algorithm.

When dealing with interpretable algorithms, achieving transparency is easier. In these cases, it is possible to implement a "white-box" approach relying on the analysis of the source code which make it straightforward for the users to see and understand it.

However, some issues may arise whenever the code is subject to a trade secret. As pointed out previously[73], "observing, studying, disassembling or testing" of a product which has been made public may not violate the trade secret.[74] Yet, it is not possible to assume that such reverse engineering necessarily leads to satisfactory results [75] and in cases of more complex, AI-based algorithm the "white-box" approach would not even be feasible.

On the contrary, black-box methods (local explanation and counter-factual faithfulness or explanations) do not rely on the analysis of the code.

It is very challenging to ensure transparency and, so, to get explanations of elaborate algorithmic system which may also have a high degree of autonomy.

Among the black-box methods, one solution, which is also suitable in terms of GDPR requirements, consist in local explanations. By sampling possible inputs, a simpler local model is computed and it is used to determine the correlations between input and output, as well as to derive the main factors of the original decision-making process. The main idea is that even if an algorithm is very complex and overall difficult to explain, it may be possible to provide reliable and understandable local explanations.[76]

For example, one current black-box algorithm which explains the predictions of a classifier is LIME (Local Interpretable Model-agnostic Explanations).[77]

Another solution under the "black-box" approach, concerns counterfactual explanations[78]. This method evaluates how a change in a particular factor influences the output.

It may be employed, for instance, to assess the fairness of a decision, based on the consequences that the factors within a specific input have on it. In this way it would be possible to provide explanations, without full disclosure of the internal logic of the

[73] See "Trade Secret" section 3.1.1.1, p.25.
[74] Article 3 (1) (b), Trade Secret Directive
[75]Brkan M., Bonnet G., 2020, supra, note 70, pp.45-50.
[76] Castelluccia C., Le Métayer D., 2019, supra, note 17, p.48.
[77] To go further, C3.ai, LIME: Local Interpretable Model-Agnostic Explanations, C3 AI, 2020. https://c3.ai/glossary/data-science/lime-local-interpretable-model-agnostic-explanations/
[78] Wachter S., Mittelstadt B., Russel C., Counterfactual explanations without opening the black box, automated decisions and the GDPR, Harvard Journal of Law & Technology, 2018.

algorithm. In this sense, there would be less risk of exposing sensitive data and infringing rights.

Also cryptographic tools may allow to prove the properties of the decision-making process of an algorithm, without revealing details of the decisional policy [79]. This could be a fair compromise between the rights of the ones challenging the reliability of the automatically generated outcome and the interests of the algorithm's owner who, in this way, does not have to disclose the source code.

For this reason, these types of explanations may be useful in terms of compliance with the GDPR requirements.

3.2. Transparency within the Platform to Business (P2B) Regulation

Another example of the need of algorithmic transparency is within the business-to-business relationships, especially due to the "increased dependence of such business users, particularly micro, small and medium-sized enterprises (SMEs), on those services in order for them to reach consumers".[80]

In order to enhance transparency in the P2B relationships, the Regulation (EU) 2019/1150 [81] sets up a co-regulatory system, where the *regulatory* part includes "a set of legally binding transparency obligations on platforms, an obligation to set up internal redress mechanisms, as well as provisions to allow for collective redress for associations representing businesses." The *self-regulatory* part, instead, consists of "a non-binding call to industry [to platforms] to establish an independent mediation body for complaints." [82]

[79] Kroll J.A., Huey J., Barocas S., Felten E.W., Reidenberg J.R., Robinson D.G., Yu H., "Accountable Algorithms", in University of Pennsylvania Law Review, Vol. 165/2017. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review
[80] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, 2019 OJ L 186. Recital 2.
[81] EC, Regulation 2019/1150, supra, note 79.
[82] European Commission, Executive summary of the Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, SWD(2018) 139 final, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0139&from=EN

Articles 1 and 2 sets the ground for the application of the P2B regulation: it shall apply to online intermediation service providers (platforms) and online search engines. These include e-commerce marketplaces (*e.g.*, Amazon Marketplace, eBay), social media services (*e.g.*, Facebook, Instagram), online software application services (*e.g.*, Google Play, Apple App Store, Microsoft Store) and those digital services through which users can input questions and perform searches of websites (*e.g.*, Google search, Bing).

A peculiarity of the P2B regulation is that it is not consumer-focused: it applies to "online intermediation services and online search engines provided, or offered to be provided, to business users and corporate website users, respectively, that have their place of establishment or residence in the Union and that, through those online intermediation services or online search engines, offer goods or services to consumers located in the Union, irrespective of the place of establishment or residence of the providers of those services and irrespective of the law otherwise applicable" (Article 1).

Turning to the legally binding disclosure obligations, to increase the transparency of platforms' practices, clear and transparent terms and conditions must be easily available. They must include relevant information to the business users, including eventual contractual changes (granting them a minimum grace period of 15 days), in "plain and intelligible language" (Article 3).

On this path, Article 4 requires platforms to state reasons for restricting, suspending or terminating trader users' services with 30 days of prior notice.

As stated in Article 7, disclosure duties encompass also discrimination practices such as platforms favouring their business or related commercial partners.

Moreover, according to Article 9 platforms shall describe rules on access to both personal and non-personal data which business and corporate website users provide to them or which are directly generated by the platform's services.

Transparency, in this setting, encompasses the tension between data protection rights and online platforms which are mainly interested in having access to great amount of data with the aim of offering increasingly better and prolific services, as well as innovating.

In light of this, transparency has a dual role. On the one hand, it grants that business users retain relevant information about "the scope, nature and conditions of their access to and use of certain categories of data", including any sharing of such data with thirds parties and the possibility to opt-out (Recitals 33, 34). On the other hand, it may "contribute to increased data sharing and enhance, as a key source of innovation and growth, the aims to create a common European data space" (Recital 35).

As far as forward-looking, this notion of transparency is not straightforward to address.[83]

Other specific algorithmic transparency obligations are addressed to online intermediation services and online general search engines, to tackle the economic dependency induced by potentially harmful ranking practices[46] , which according to Article 2(8) and Recital 24 consist of "relative prominence given to the goods or services offered through online intermediation services and search engines, as presented, organized, or communicated by the providers", as a result of the use of algorithmic sequencing, rating or review mechanisms, visual highlights, or other saliency tools or combinations of these".

Indeed, a very relevant rule concerns the ranking practices and is treated by Article 5. In order to avoid unclear ranking rules for search results, Articles 5(1) and (2) require that providers give information about the main parameters affecting the way in which goods and services are ranked.

Ranking "can essentially be thought of as a form of data-driven, algorithmic decision-making" [84], which "has an important impact on consumer choice and, consequently, on the commercial success of the users"[85]. Therefore, Article 5 is aimed at improving predictability for users, by requiring not only to disclose the main parameters of the ranking but also the reasons for the relative importance of those main parameters as opposed to others. In addition, pursuant to Article 5(5), the users should obtain an 'adequate understanding' of whether, how and to what extent "(a) the characteristics of the goods and services offered to consumers through the online intermediation services or the online search engine; (b) the relevance of those

[83] However, Regulation does not prescribe a minimum level of data access or ban any unfair practices relating to data access. As such, it does not tackle the interaction of data access with data protection in strategic behaviour that can undermine the level of data innovation to the detriment of both businesses and consumers. Graef I., Gellert R., Husovec M, Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation, DP 2018-028 TILEC Discussion Paper, 2018.
[84] European Commission, Commission Notice Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council 2020/C 424/01, para 1.2.
[85] EC, Guidelines on 2019/1150, supra, note 83, para 1.2.

characteristics for those consumers; (c) as regards online search engines, the design characteristics of the website used by corporate website users".

Such obligations can be viewed as expanding the "explicability duties" (Articles 13 and 14, GDPR) from P2C (Platforms-to-Consumers) to P2B(Platforms-to-Businesses) relationships.

According to these rules, the logic of algorithmic decisions taken by the platforms should meet transparency and therefore should be made accountable to the businesses.

This Regulation attempts also at creating a level playing field between businesses. Platforms are required to disclose to the businesses the main parameters of the ranking systems they use. These include "algorithmic sequencing, rating or review mechanisms, visual highlights, or other saliency tools" [86]. At the same time, it recognises the eventual protection of algorithms by the Trade Secrets Directive (Article 1(5), P2B Regulation).

At the end of 2020, the European Commission published Guidelines[87] on ranking transparency under the P2B Regulation.
These are not binding but are aimed at fleshing out the transparency requirements under the P2BR and provide suggestions on best practices.

3.2.1. Legal Challenges

The P2BR aims at addressing a perceived imbalance in the relationship between online platforms and the businesses which provide goods and services on them. The same holds for online search engines and the websites which appear on their listings, with a particular attention to ranking.[88]

Online search engines (OSEs) and operators of online intermediation services (OISs), are required to provide information about the main parameters used. This may represent a potential compliance burden.

[86] Recital 24, P2B Regulation.
[87] EC, Guidelines on 2019/1150, supra, note 83.
[88] Heywood D., Platform to Business Regulation to apply from 12 July 2020, Taylor Wessing, 2020. https://www.taylorwessing.com/en/insights-and-events/insights/2019/07/eu-online-platforms-regulation-to-apply-from-12-july-2020

The underlying logic is that there is no 'one size fits all' solution. Providers need to identify on a case by case and service by service basis which are those "main parameters" that have to be disclosed.

There is the need to carefully assess also how to disclose the appropriate level of information. It is important to consider both the explanation itself which must be provided in clear and intelligible language and how to make it available in an accessible and technologically neutral way in compliance with the legislation.

One of the challenges for providers is understanding how much information to disclose. It has to be "meaningful", so to provide “real added-value to the users concerned”, and it should "take account of the nature, technical ability and needs of the 'average' users of a given service which may vary considerably between different types of services". [89]

Giving too little information would not be meaningful but providing too much information, overwhelming “users with too lengthy or complicated descriptions, or descriptions of parameters other than the main ones” may result in a compliance failure as well. [90]

This limitation to disclosure should also lower the risk of enabling a “deception of consumers or consumer harm through the manipulation of search results” as referred to in Article 5(6).

Another challenge is trade secrets protection, as such information is an asset that may be protected by trade secrets, and even if the margins left by the disclosure duties are thin, platforms might not want to share the way to convey it to their clients.

A principle of proportionality, therefore, should be applied to information disclosure[91].

Business and corporate website users must be able to get an "adequate understanding" of the ranking mechanisms as stated by Article 5(5). The description given should at least be “based on actual data on the relevance of the ranking parameters used” (Recital 27). The European Commission, through the Guidelines on ranking transparency,

[89] EC, Guidelines on 2019/1150, supra, note 83, para 1.3
[90] EC, Guidelines on 2019/1150, supra, note 83, para 1.3.3
[91] Scalzini S., Trade Secrets And Data-Driven Innovation In The Eu, in Comandé, G. (ed.), Encyclopedia of Law for Data Scientists, EdwarElgar, 2021, forthcoming.

interprets the ‘main parameters’ as “what drove the design of the algorithm in the first place” (Para 41).

Moreover, providers cannot withdraw the disclosure of the main parameters “based on the sole argument that it has never revealed any of its parameters in the past or that the information in question is commercially sensitive.” (Para 82).

So, providers need to consider what information will be most useful to them. There is no requirement to disclose exactly how algorithms are used but merely stating that they are used will be insufficient.

For all parameters disclosed the level of detail "should go beyond a simple enumeration of main parameters and provide at least a secondary layer of explanatory information".[92]

3.2.2 Technical Challenges

The main challenge is to find an efficient way to disclose the appropriate level of information, both in terms of explanation provided that must be in plain and intelligible language, and in terms of technical feasibility which has to grant an accessible and not confusing legal compliance. In line with the P2B Regulation, this is particularly relevant when dealing with ranking practices.

The “Guidelines on Ranking Transparency” [93] recognize that there is no “one size fits all” solution.
Therefore, providers have to assess on a case by case and service by service basis, which are the main parameters the use. Accordingly, they have to be disclosed and, also, contextualized in line with the degree of their importance.

The Guidelines set out a useful path for a systematic and feasible approach to transparency. The criteria to take into account are the original reasons for developing the

[92] EC, Guidelines on 2019/1150, supra, note 54, para 6.2.
[93] EC, Guidelines on 2019/1150, supra, note 54.

algorithm in line with "what the provider considers to be the top type of result on its service[94]" and what fulfils the best interests of the consumers.

It is also suggested that a good strategy would be to analyse the more unexpected elements [95] that may influence the ranking and the information that would be most useful for users to know.

Likewise, the Guidelines refer to a series of considerations when specific criteria or adjustment mechanisms apply to the ranking such as, for example, personalisation, consumer search behaviour and intent, the user's history, default settings, sorting & filtering mechanisms, cross-platform presence, external factors such as star ratings or industry awards, randomisation, the effect of machine learning, measures taken to avoid third-party bad-faith manipulation of ranking results, user reviews, or providers' measures against illegal content.

General written explanations may, therefore, not be sufficient to grant users with clear and comprehensive information. It would be appropriate to adopt a more specific approach based on systems which are tailored directly on the services provided by the platforms. In this way it would be easier to meet the needs of users with different interests and demands.

As suggested by the European Commission[96], to do so in a feasible manner and to assure the compliance with Articles 3 and 5 of P2BR, platforms may put in place tools to get feedbacks directly from their users who would, therefore, assess by themselves if the information given is useful and detailed enough. Depending on the type of service offered, it may be done in a fully-automated way or in a semi-automated manner, with the aid of human intervention. This may represent a good strategy as it would result in a both cost and performance efficiency.

[94] EC, Guidelines on 2019/1150, supra, note 54, para 3.2.
[95] As stated by the Guidelines, para 3.2: "these could also be factors that a user may assume are irrelevant as they are unrelated to the quality of the good or service they offer through the service".
[96] EC, Guidelines on 2019/1150, supra, note 83, para 6.5

Also, the way explanations are given may be optimized.

The Regulation requires OISs to provide information in their terms and conditions in a clear and intelligible manner. In practice, services can choose how best to communicate the information to users, but it must be done in a way that is not inconsistent or spread out over different tools and media. This is necessary to grant transparency as meant by the law. [97]

The Guidelines suggest that OISs may "take steps that direct business users to the exact location of the description and/or include it in Q&A sections, tutorials, guidelines, pop-up windows, video messages or in other forms" or may "consider establishing a single touchpoint (for example in a user 'dashboard') that could reference or index all the relevant informational tools available to explain ranking transparency" which is even a more straightforward solution as reduces the risk of non-compliance.

Likewise, OESs have to provide the information in a way that is easily accessible on their webpage. Good solutions are represented by a link to more detailed information, as well as icons, tabs or banners[98].

The Regulation did not lay down very detailed requirements[99]. Yet, the Guidelines, even if non-binding, turn out to be helpful in providing insights on best practices which allow for a more pragmatic transparency assessment.

However, the P2B set of rules will be soon expanded by the "Digital Services Act Package" which will aim at harmonizing responsibilities for online platforms and information service providers while reinforcing oversight over platforms' content policies and, for this, is expected to boost transparency.

[97] EC, Regulation 2019/1150, supra, note 79.
[98] European Commission, Commission Notice Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council 2020/C 424/01. Section 7.2.
[99] Busch Christoph, The P2B Regulation (EU) 2019/1150: Towards a 'Procedural Turn' in EU Platform Regulation?, Journal of European Consumer and Market Law 133, 2020. https://ssrn.com/abstract=3686103

4. TOWARDS MORE COMPREHENSIVE AND SPECIFIC SET OF RULES

4.1. The Proposals for the Digital Services Act and the Digital Markets Act

The European Commission aims at providing a new legal framework for digital services capable of strengthening the digital single market while granting the protection of the Union values and of the fundamental rights that are increasingly influenced by the governance of private subjects in the information society. Algorithmic transparency is at the core of such a framework given the fact that online services currently rely on wide data collection practices to power their algorithmic systems which may be opaque and, therefore, inaccessible for public interest scrutiny.

This was further accentuated by the COVID19 crisis: algorithmically-driven technologies govern the present media and communications infrastructure.

Aware of the risks and challenges posed by the digital age, the European Commission launched a public consultation in June 2020 to seek opinions and to collect data from individuals, businesses, online platforms, academics, civil society and all stakeholders in order to jointly define the rules governing digital services in the EU.

On December 15, 2020 it proposed the so-called "digital package". It consists of two legislative initiatives within the European Digital Strategy *Shaping Europe's Digital Future*: the Digital Services Act (DSA) and the Digital Markets Act (DMA).

The main objectives of the digital package are: (i) “to create a safer digital space in which the fundamental rights of all users of digital services are protected" and (ii) "to establish a level playing field to foster innovation, growth and competitiveness, both in the European Single Market and globally". [100]

[100] The Digital Services Act package. European Commission 3 mar. 2021.

Basically, they aim at filling the gaps of the current regulatory framework which has proved inadequate to deal with the use of opaque systems and the related issues.

According to the Digital Markets Act (DMA)[101], the ones classified as "gatekeepers" [102] will have to proactively implement certain actions to ensure transparency.

They are explicitly required to be transparent about the rankings systems under Article 6. Since such systems have direct impact on consumers, it is important that they are provided on a non-discriminatory basis.

The Commission is moreover empowered with the authority to "request access to data bases and algorithms of undertakings and request explanations on those by a simple request or by a decision" (Article 19).

The approach of the Regulation consists on the setup of fines (Article 26) or periodic penalty payments (Article 27) as tools to force undertakings, in particular gate-keepers, to comply and, consequently ensuring transparency under quest[103].

This is in line with the purpose of the DMA to place, according to an *ex-ante* approach, a series of obligations and prohibitions on the ones classified as gatekeepers in order to ensure the openness of the digital services at stake.

However, it still remains to assess if such provisions may be felt as a burden in the evolving field of businesses using algorithmic systems and, therefore, if they are effectively capable of ensuring transparency so to consequently benefit innovation and competition.

The Digital Services Act (DSA)[104], instead, defines clear responsibilities and accountability for providers of intermediary services, and in particular online platforms, such as social media and marketplaces."

[101] European Commission, Proposal for a Regulation Of The European Parliament And Of The Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final, 2020.
[102] According to Article 3, DMA: "A provider of core platform services shall be designated as gatekeeper if: (a) it has a significant impact on the internal market; (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future."
[103] Under Article 19, DMA the information requested by the Commission must be disclosed.
[104] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final, 2020.

As a matter of fact, it recognises the impact that very large online platforms[105] have on the economy and on the society. For this reason, it will bring some adjustments aimed at increasing the levels of transparency and accountability on how the platforms' providers "moderate content, on advertising and on algorithmic processes". [106]

In particular, the proposed measures establish "due-diligence" and transparency obligations applicable to all digital service providers in the European Single Market, including those that are established outside the EU, with particular reference to the procedures of "notice and takedown" of illegal contents and the possibility of challenging the decisions of platforms content moderation activities.

This to grant users' online safety across the European Union and to protect their fundamental rights.

Algorithms are specifically encompassed by the "recommender systems". Article 2 (o) defines them as "fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed".

If such systems are employed, as often happens on the main e-commerce sites, the parameters used and any options for the recipients of the service to modify or influence these parameters must be clearly indicated in the terms and conditions of the platform. Additionally, for the sake of transparency, all intermediation service providers will be required to include in their terms and conditions any restrictions or limitations they impose in relation to the use of their services. In particular, information on algorithmic decision-making should be included (Article 12).

[105] The Digital Services Act identifies "very large online platforms" as the ones reaching more than 45 million average monthly users. They process a huge amount of data and information and they may have great influence on the market and on users' choices. Moreover, they may represent a systemic risk in terms of dissemination of illegal content. In light of this, the proposal sets a higher standard of transparency and accountability on advertising, algorithmic processes and on how the providers of these platforms moderate content.
[106] European Commission, Digital Services Act – Questions and Answers. Brussels, 15 December 2020. file:///C:/Users/Utente/Downloads/Digital_Services_Act__Questions_and_Answers.pdf

Furthermore, consumers should be provided with the right to opt out of profiling-based content recommendations. (Article 29)[107].

Indeed, very large online platforms[108] will therefore be obliged to develop appropriate management tools to mitigate the systemic risks associated with their activities.

In the case of very large online platforms, Recital 64 specifies that the Digital Services Coordinator of establishment or the Commission, as well as vetted researchers have the power of accessing data in order to supervise and ensure the compliance with the rules set out by the DSA.

This is further reinforced by Article 54(3) stating that during on-site inspections the Commission may require explanations on "organisation, functioning, IT system, algorithms, data-handling and business conducts" and by Article 57(1) which points out that for monitoring purposes, the Commission may require the platform "to provide access to, and explanations relating to, its databases and algorithms.".

However, in order to balance the different interests that may be at stake, through Article 31(6), platforms are given the right to refuse such access based on trade secrecy concerns.

This shows that although the DSA intend to address algorithmic transparency in a comprehensive manner, some distinction is needed for a correct enforcement. According to the cases on the line, different level of disclosure, being it full, limited or restricted only to the main parameters, shall be called for. [109]

In light of the above, one may understand how the Digital Services Act fits into the current European scenario, especially in the context of EU's digital transformation process.

[107] As specified by DSA, this provision falls within the meaning of Article 4 (4) of Regulation (EU) 2016/679 where/ according to which "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;".
[108] As defined by Article 25, DSA.
[109] Huseinzade N., Algorithm Transparency: How to Eat the Cake and Have It Too, European Law Blog, 2021. https://europeanlawblog.eu/2021/01/27/algorithm-transparency-how-to-eat-the-cake-and-have-it-too/

Even if the proposal is only at an early legislative stage, it affirms the ambition and commitment of the EU to pursue and promote its own model of digitization and innovation. This model clearly embraces the compliance with the values of the Union, the protection of democracy and the fundamental rights of the citizens.

In particular, an approach such as the one of the Digital Services Act could certainly have the potential to redress the lack of equity, transparency and accountability that is an extremely important challenge to be faced when dealing with the use of artificial intelligence systems by private (and public) actors.

4.2. The proposal for an Artificial Intelligence Act

The variety of AI applications, its multiformity, dynamism, as well as its margin of unpredictability, make it difficult to lay down a legislative framework capable of balancing all the elements and interests at stake.

The Artificial Intelligence Act [110] represents a one-of-its-kind and a huge innovation in the field of legislative initiatives, since it directly aims at a general regulation of artificial intelligence technologies. Through it, the European Commission wants to promote a joint European action ensuring the proper functioning of the internal market, to boost development and investment, and adequately governing the risks and benefits of AI.

According to the Commission, the proposed regulatory framework consists of a proportionate system, centred on a risk-based approach that does not create unnecessary restrictions on trade. In this setting, the legislative intervention would be envisaged only in situations in which there is a justified need or where such need could be reasonably forecasted in the near future. At the same time, the legal framework intends to include flexible mechanisms that would allow dynamic adaptation, depending on the evolution of technology.[111]

[110] Proposal for a Regulation laying down harmonised rules on artificial intelligence
[111] Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts, p.3.

This is why the proposal is built on a differentiation between AI systems posing (i) an unacceptable risk, (ii) a high risk, and (iii) low or minimal risk.

In particular, within this framework, the transparency of the activities of the AI systems must be ensured in order to enable users to understand and control how specific outputs are produced.

The Commission puts in place a soft law regime for systems with low or minimal risk with the purpose of fostering the voluntary application of transparency principles which are in the domain only of high-risk.

As a matter of fact, under high-risk circumstances there are stricter transparency requirements.

Article 13 prescribes a sort of "transparency by design" especially for high-risk AI systems, stating that such systems must be designed and developed in a way that they can ensure a sufficiently transparent operation, allowing users to correctly interpret the results and use them appropriately.

There must be also specific instructions for their use. These must specify the characteristics, capabilities and performance limits of the system, including the purpose, the level of accuracy and robustness. The instructions must also contain any known or knowable circumstance relating to the use of AI systems, as well as to their possible abuse and the risks they could pose for health and human rights in general. Additionally, the expected life cycle for that system and any measures necessary for maintenance and to ensure proper operation must be declared.

However, as clarified by Title IV of the Act, certain AI systems which are neither prohibited, nor necessarily high-risk are subject to a number of transparency obligations as well. These obligations include that:

1. Providers must ensure that AI systems intended to interact with natural persons inform the natural persons that they are interacting with an AI system. The only exception is whenever this is obvious or in relation to the investigation of crimes.
2. Natural persons who are subject to an emotion recognition system or a biometric categorization system must be informed thereof by the users of such systems.

3. Users of AI systems generating so-called "deep fakes" must declare that the content has been artificially created or manipulated. In this case, there may be exceptions when such processes are necessary to detect, prevent, investigate and prosecute criminal offences or are necessary for the exercise of the right to freedom of expression and the right to freedom of the arts, subject to appropriate safeguards.

The Artificial Intelligence Act recognizes the need to maintain a regulatory framework consistent with current European legislation and applicable to sectors where high-risk AI systems are already being used or will be used in the near future. At the same time, it attempts to address in a more comprehensive and systematic way the matters innovation arises, with particular regard to algorithmic transparency.

The approach adopted by the EU, indeed, stems from the awareness that, on legal grounds, there is the need to foresee and accompany scientific and technological progress in its evolution.

In in its attempt to horizontally regulate such an evolving and multifaceted sector, the European Commission has to find a balance between an articulated system to protect the rights of individuals and social groups and the related rules whose rigour may hinder the development and investment on some AI systems in the European continent.

This poses challenges in terms of transparency.

That is the reason why the Artificial Intelligence Act relies on a framework of proportionality (Para 2.4) which imposes regulatory burdens only in specific circumstances.[112]

The adoption of both soft and hard laws is the other feature implemented to grant a definitive algorithmic transparency.

To date, the transversality of the areas in which the AI systems finds application, the technical uncertainty about their development and their impact will undoubtedly be the heart of evolutions and debates. Accordingly, the proposal must still go through the EU's legislative process and will likely be subject to amendments.

[112] Specific circumstances shall be understood as those situations where AI systems are likely to pose high risk. This in accordance with the Artificial Intelligence Act risk-based approach, as also explained previously in the text.

CONCLUSION

The complicated solution to the problem of algorithmic transparency is legal as much as technical. In such a context, it is not possible to rely only on the traditional means of human reasoning; instead, a solid basis for the validation of technological processes is needed.

The thesis analysed two case studies where legal and technical challenges stand in the way of the need for algorithmic transparency respectively for personal data protection goals and for pro-competitive and market fairness goals and try to propose interdisciplinary solutions.

As a matter of fact, transparency measures overcome different legal requirements, such as the privacy rights of individuals involved in automated-processes (in particular according to GDPR) and the interests of companies to keep commercially sensitive parts of their algorithm secret, which could well constitute a trade secret worthy of legal protection (in particular according to the provisions of TS Directive).

Moreover, it is not possible to assume that algorithmic transparency always results in tangible benefits for users. Even if the intrinsic mechanisms of an algorithm were made public, because of its technical complexity, (some) users could find such specifications ambiguous and, therefore, not very usable.

The technological progress may, therefore, be useful in aiding and supporting the legal methods.

As also recognized in the European Union context, a good solution may be the combination of ex-ante [113] creation of models that allow human understanding, thanks also to reverse engineering techniques, and of ex-post standards to technically validate the outputs (eventually through independent audits).

In some cases, in particular when dealing with autonomous, opaque algorithms, it would useful to seek the aid of technology through solutions such as local, counterfactual explanations or cryptographic tools that may allow for transparency while safeguarding the rights of both the data subject and the algorithm's owner.

[113] Felzmann, H., Fosch-Villaronga, E., Lutz, C. et al., Towards Transparency by Design for Artificial Intelligence, Sci Eng Ethics 26**,** 3333–3361, 2020. https://doi.org/10.1007/s11948-020-00276-4

Thus, there is no point in chasing a transparency based on the standardization of the algorithms processes, as it would be incompatible with the technological progress and would have implications also on business and individuals.

It is far more useful to engage on a debate which revolves around how to implement it without, however, stopping innovation and competition between companies, so to, ultimately, favour the society as a whole.

Furthermore, a "multistakeholders" [114] approach should be encouraged.

A collaborative action between regulatory and competition authorities, civil society, businesses and the academic and scientific world may pave the way for finding a fair balance between algorithmic transparency and the economic interest of tech firms who have to legally protect, use and improve their algorithms. Such algorithms which are strictly functional to their business activities, may be characterized by the processing of huge amounts of data, also personal ones, but have to be ultimately aimed at providing web users with increasingly efficient and functional digital services.

This certainly lays the foundations for balanced regulatory proposals[115] capable of proportionally define the shapes that algorithmic transparency must concretely take and of redressing the distortions which stem from the exploitation of these technologies.

[114] Lucic A., Srikumar M., Bhatt U., Xiang A., Taly A., Liao V., Rijke M., A Multistakeholder Approach Towards Evaluating AI Transparency Mechanisms, arXiv preprint arXiv:2103.14976, 2021.
[115] To date, in the European context, these are the DSA and the Artificial Intelligence Act, as explained in Chapter 4.

REFERENCES

Amoruso G. M., Nicotra M., Deliveroo, l'algoritmo che discrimina: perché è importante la sentenza del tribunale bolognese, Agenda Digitale, 2021. https://www.agendadigitale.eu/sicurezza/privacy/deliveroo-lalgoritmo-che-discrimina-perche-e-importante-la-sentenza-del-tribunale-bolognese/

Association for Computing Machinery, Principles for Algorithmic Transparency and Accountability, 2017. https://www.acm.org/binaries/content/assets/pub lic-policy/2017_joint_statement_algorithms.pdf

Bamberger K.A., Lobel O., Platform Market Power, Berkeley Technology Law Journal 1051 (2017), San Diego Legal Studies Paper No. 17-311, 2017, https://ssrn.com/abstract=3074717

Bonafè M., Trevisi C., Intelligenza artificiale, l'algoritmo "trasparente": un rebus ancora da sciogliere, Agenda Digitale, 2019. https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-lalgoritmo-trasparente-un-rebus-ancora-da-sciogliere/#Diritto_alla_trasparenza_degli_algoritmi

Brkan M., Bonnet G., Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas, European Journal of Risk Regulation, 11(1), 18-50, 2020. doi:10.1017/err.2020.10

Burgess P., Algorithmic augmentation of democracy: considering whether technology can enhance the concepts of democracy and the rule of law through four hypotheticals, AI & Soc, 2021. https://doi.org/10.1007/s00146-021-01170-8

Burrell J., How the machine 'thinks': understanding opacity in machine learning algorithms. Big Data Soc 3:205395171562251, 2016. https://doi.org/10.1177/2053951715622512

Busch C., The P2B Regulation (EU) 2019/1150: Towards a 'Procedural Turn' in EU Platform Regulation?, Journal of European Consumer and Market Law 133, 2020. https://ssrn.com/abstract=3686103

C3.ai, LIME: Local Interpretable Model-Agnostic Explanations, C3 AI, 2020. https://c3.ai/glossary/data-science/lime-local-interpretable-model-agnostic-explanations/

Castelluccia C., Le Métayer D., Understanding algorithmic decision-making: Opportunities and challenges, European Parliament, EPRS, STOA, 2019.

https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf

Cave S., The Problem with Intelligence, Its Value-Laden History and the Future of AI, Leverhulme Centre for the Future of Intelligence, University of Cambridge, 2020.

Comandé G., Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità, Analisi Giuridica dell'Economia, 1. 169-188, 2019.

Comandé G., Responsabilità ed accountability nell'era dell'Intelligenza Artificiale in Giurisprudenza e Autorità Indipendenti nell'epoca del diritto liquido, eds. F. Di Ciommo, O. Troiano, La Tribuna, 2018. pp. 1001, 1013.

Council Of Europe Commissioner For Human Rights, Recommendation – Unboxing Artificial Intelligence: 10 steps to protect Human Rights, Strasbourg: Council of Europe, 2019. https://rm.coe.int/unboxingartificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

Dalgıç Ö., Algorithms Meet Transparency: Why There is a GDPR Right To Explanation?, Turkish Law Blog, 2020. https://turkishlawblog.com/read/article/221/algorithms-meet-transparency-why-there-is-a-gdpr-right-to-explanationg

Danaher J., The Threat of Algocracy: Reality, Resistance and Accommodation, Philos. Technol. 29, 245–268, 2016. https://doi.org/10.1007/s13347-015-0211-1

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. https://doi.org/10.1017/err.2020.10

Edwards L., Veale M., Slave To The Algorithm? Why A 'Right To An Explanation' Is Probably Not The Remedy You Are Looking For, Duke Law & Technology Rev, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855.

EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 OJ L 119/1.

European Commission, Commission Notice Guidelines on ranking transparency pursuant to Regulation (EU) 2019/1150 of the European Parliament and of the Council 2020/C 424/01.

European Commission, Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, 2020 OJ(EU) L 114/7. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020H0518&from=ENendation%202020/510

European Commission, Digital Services Act – Questions and Answers. Brussels, 15 December 2020 file:///C:/Users/Utente/Downloads/Digital_Services_Act__Questions_and_Answers.pdf

European Commission, Ethics guidelines for trustworthy AI High-Level Expert Group on AI, 2019.

European Commission, Executive summary of the Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, SWD(2018) 139 final, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0139&from=EN

European Commission, Proposal for a Regulation Of The European Parliament And Of The Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final, 2020.

European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, 2020. https://ec.europa.eu/info/sites/info/files/commissi on-white-paper-artificial-intelligencefeb2020_en.pdf

European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM/2020/825 final, 2020.

European Parliament, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence (COM(2019)168), https://ec.europa.eu/transparency/regdoc/rep/1/2019/EN/COM-2019-168-F1-EN-MAIN-PART-1.PDF

Felzmann, H., Fosch-Villaronga, E., Lutz, C. et al. , Towards Transparency by Design for Artificial Intelligence, Sci Eng Ethics 26**,** 3333–3361, 2020. https://doi.org/10.1007/s11948-020-00276-4

Graef I., Gellert R., Husovec M, Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation, DP 2018-028 TILEC Discussion Paper, 2018.

Heywood D., Platform to Business Regulation to apply from 12 July 2020, Taylor Wessing, 2020. https://www.taylorwessing.com/en/insights-and-events/insights/2019/07/eu-online-platforms-regulation-to-apply-from-12-july-2020

Huseinzade N., Algorithm Transparency: How to Eat the Cake and Have It Too, European Law Blog, 2021. https://europeanlawblog.eu/2021/01/27/algorithm-transparency-how-to-eat-the-cake-and-have-it-too/

Italiano G. F., Le sfide interdisciplinari dell'intelligenza artificiale, in "Analisi Giuridica dell'Economia, Studi e discussioni sul diritto dell'impresa" eds. A. Nuzzo and G. Olivieri, 1/2019, pp. 9-20.

Kantarci A, AI Ethics in 2021: Top 9 Ethical Dilemmas of AI., AIMultiple, 2021. https://research.aimultiple.com/ai-ethics/#surveillance-practices-limiting-privacy

Kossow N., Windwehr S., Jenkins M., Algorithmic transparency and accountability, Transparency International Anti-Corruption Helpdesk Answer, 2021.

Kroll J.A., Huey J., Barocas S., Felten E.W., Reidenberg J.R., Robinson D.G., Yu H., "Accountable Algorithms", in University of Pennsylvania Law Review, Vol. 165/2017. https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review

Lo Sapio G., La trasparenza sul banco di prova dei modelli algoritmici, Osservatorio sulla trasparenza 21 aprile 2021, Federalismi.it, 2021.
https://www.segretaricomunalivighenzi.it/archivio/anno-2021/aprile/doc-lo-sapio.pdf

Loyola-González O., Black-Box vs. White-Box: Understanding Their Advantages and Weaknesses From a Practical Point of View, 2019. IEEE Access. 7. 154096-154113.

Lu S., Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial intelligence 23(1), 2020.

Lucic A., Srikumar M., Bhatt U., Xiang A., Taly A., Liao V., Rijke M., A Multistakeholder Approach Towards Evaluating AI Transparency Mechanisms, arXiv preprint arXiv:2103.14976, 2021.

Maggiolino M., Eu Trade Secrets Law and Algorithm Transparency, in L. C. Ubertazzi, AIDA, XXVII, Giuffrè Francis Lefebvre, Milano, 2018. p. 202.

Malgieri G., Automated decision-making in the EU Member States: The right to explanation and other "suitable safeguards" in the national legislations, Computer law & security review, 2019.

Malgieri G., Comandé G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, International Data Privacy Law, Volume 7, Issue 4, 2017. pp. 243–265. https://doi.org/10.1093/idpl/ipx019

Meijer A., Transparency, eds. M. Bovens, R. E. Goodin, & T. Schillemans, The Oxford handbook of public accountability (pp. 507–524), Oxford University Press, 2014.

Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L., The ethics of algorithms: Mapping the debate, Big Data & Society, 2016

OECD, Data-Driven Innovation: Big Data for Growth and Well-Being, OECD Publishing, 2015. https://doi.org/10.1787/9789264229358-en.

Olhede S.C., Wolfe P.J., The growing ubiquity of algorithms in society: implications, impacts and innovations, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 2018, 376.2128: 20170364.

Parkins D., The world's most valuable resource is no longer oil, but data, The Economist, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

Pasquale F., Le nuove leggi della Robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale, Luiss University Press, 2020.
Pasquale F., The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, 2015.

Pedreschi D., Giannotti F., Guidotti R., Monreale A., Pappalardo L., Ruggieri S., Turini F., Open the Black Box Data-Driven Explanation of Black Box Decision Systems, in ArXiv Preprint, N. 1/2018.

Pellecchia E., Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation in Le nuove leggi civili commentate, 1209-1236, 2018.
Ranchordas S., Online Reputation and the Regulation of Information Asymmetries in the Platform Economy, Critical Analysis of Law, 2018, Forthcoming, University of Groningen Faculty of Law Research Paper No. 2/2018. https://ssrn.com/abstract=3082403

Reese S., Algorithmic transparency in the public sector, Reform and Imperial College London's The Forum Policy Hackathon, 2021. https://reform.uk/sites/default/files/2021-05/Hackathon%20Write%20Up%20Final.pdf

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, 2019 OJ L 186.

Scalzini S., Alcune questioni a proposito di Algoritmi, Dati, Etica e Ricerca, in Rivista Italiana di Medicina Legale e del Diritto in campo sanitario 1/2019, Focus. Tutela dei dati personali concernenti la salute e attività di ricerca: considerazioni interdisciplinari nella prospettiva etico-giuridica, 2019. pp.169-178.

Scalzini S., Trade Secrets And Data-Driven Innovation In The Eu, in Comandé, G. (ed.), Encyclopedia of Law for Data Scientists, EdwarElgar, 2021, forthcoming.

Scassa T., Data Ownership, CIGI Papers No. 187, Ottawa Faculty of Law Working Paper No. 2018-26, 2018. https://ssrn.com/abstract=3251542 or http://dx.doi.org/10.2139/ssrn.3251542

Stone P., Brooks R., Brynjolfsson E., Calo R., Etzioni O., Hager G., Hirschberg J., Kalyanakrishnan S., Kamar E., Kraus S., Leyton-Brown K., Parkes D., Press W., Saxenian A., Shah J., Tambe M., Teller A., Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel, Stanford University, 2016. http://ai100.stanford.edu/2016-report.

Strusani D., Houngbonon, G. V., The Role of Artificial Intelligence in Supporting Development in Emerging Markets, 2019.

T.A.R. Lazio Roma Sez. III bis, Sent., 21/03/2017, n. 3742 and T.A.R. Lazio Roma Sez. III bis, Sent., 22/03/2017, n. 3769.

Wachter S., Mittelstadt B., Floridi L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 2017, pp. 76,96

Wachter S., Mittelstadt B., Russel C., Counterfactual explanations without opening the black box, automated decisions and the GDPR, Harvard Journal of Law & Technology, 2018.

Wieringa M., What to account for when accounting for algorithms: A systematic literature review on algorithmic accountability, in Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020. pp. 1–18.

Zuddas P., Brevi note sulla trasparenza algoritmica, Amministrazione in cammino, LUISS, 2020.https://www.amministrazioneincammino.luiss.it/wp-content/uploads/2020/06/ZUDDAS.pdf