The Regulation of Algorithms and Artificial Intelligence under the GDPR, Case Law and Proposed Legislation

Raffaele Zallone
Studio Legale Zallone
Milano, Italy
r.zallone@studiozallone.it

***Abstract*— Autonomous cars will be working (among other things) thanks to a wide use of A.I. The regulation of Artificial intelligence has been a matter of debate for some time and different theories have been developed on how to govern A.I. Yet, recently many steps forward the regulation of A.I. have been made. In this paper I shall analyze how the legal scenario of data governance in Europe has been changing and how the regulation of Algorithms (hence of A.I.) is moving forward I Europe. I shall briefly recall the GDPR provisions applicable to the regulation of algorithms, then examine recent case law where the legal aspects of algorithms regulation have been at the basis of the decisions issued. Finally, I shall briefly review the proposed European Regulation on A.I. to illustrate its potential impact on the industry.**

Keywords*— *Artificial Intelligence (AI), GDPR, algorithm regulation, European Regulation of AI

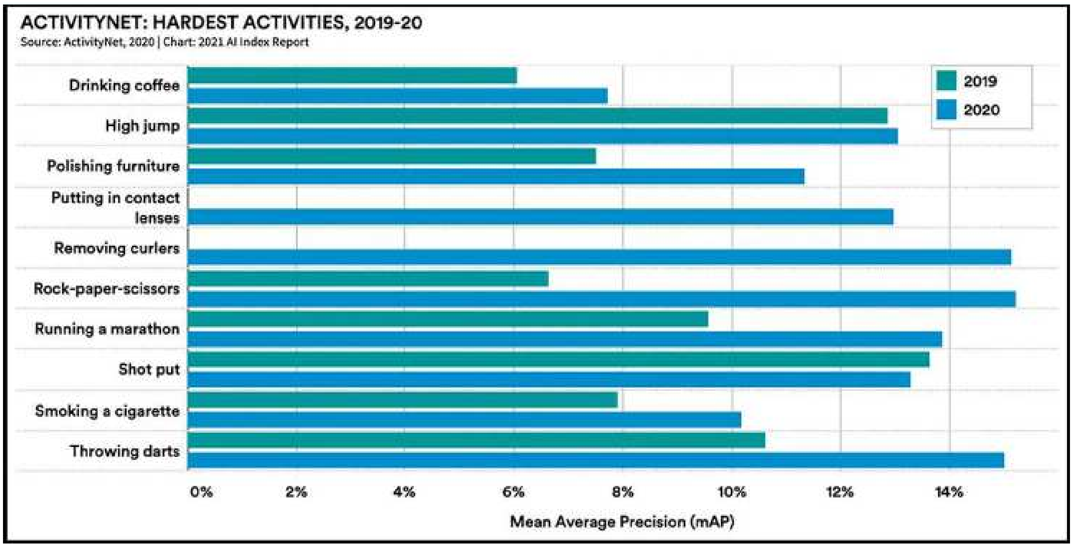
I. Introduction

Artificial Intelligence (AI) "has the potential to improve the welfare and well-being of people, to contribute to positive sustainable global economy activity, to increase innovation and productivity and to help respond to key global challenges". This statement can be found in the Organization for Economic Co-operation and Development (OECD) Recommendation on Artificial Intelligence.

This significant contribution of AI to society, economy and well-being in general is generally recognized. At the same time a growing number of commentators, lawyers and politicians acknowledge the fact that the increase in use of AI is not without risks. AI is being used not only in sophisticated, state of the art programs to better manage manufacturing or other industrial process. It is used in applications used daily by millions of people: it is used to evaluate candidates for a job, to rate passengers and drivers of a transportation system, to decide on loans and mortgages, to target consumers with advertisements [1-3]. In many fields, tasks that were done by humans are now delegated to AI algorithms, Figs. 1, 2, and 3.

As one distinguished scholar has stated, it is well accepted that algorithms can present significant challenges to our legal system given that "the uncertainty and opacity of the work being done by algorithms and its impact is also increasingly problematic" [4]; in addition, "they are often hard to explain and changing over time". This has led to a very significant debate and has shed a high regulatory focus on algorithms; most recently, just as an example, the Council of Europe Legal Affairs Committee has approved a resolution urging for regulation on the use of AI in criminal cases and the European Commission has introduced a proposed regulation on AI [5].

Notwithstanding this general consensus, the debate is still on going on how to regulate AI and, on a practical side, what are the means that a Court has to decide if and when an AI algorithm is in violation of the law. Again, different theories and methods have been analyzed and proposed, but the debate continues.



ACTIVITYNET: HARDEST ACTIVITIES, 2019-20

Source: ActivityNet, 2020 | Chart: 2021 AI Index Report

Fig. 1. Activities recognized with AI systems. Source https://spectrum.ieee.org/the-state-of-ai-in-15-graphs/language-ai

978-88-87237-52-8 ©2021 AEIT

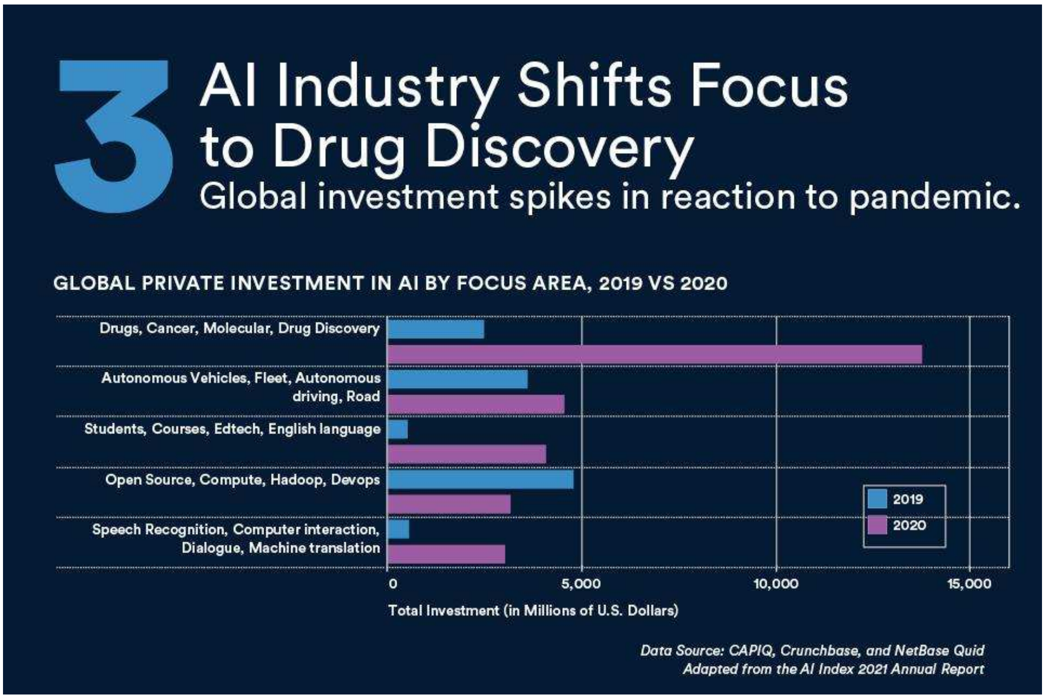


Fig. 2. AI Industry focus. Source https://hai.stanford.edu/news/state-ai-10-charts

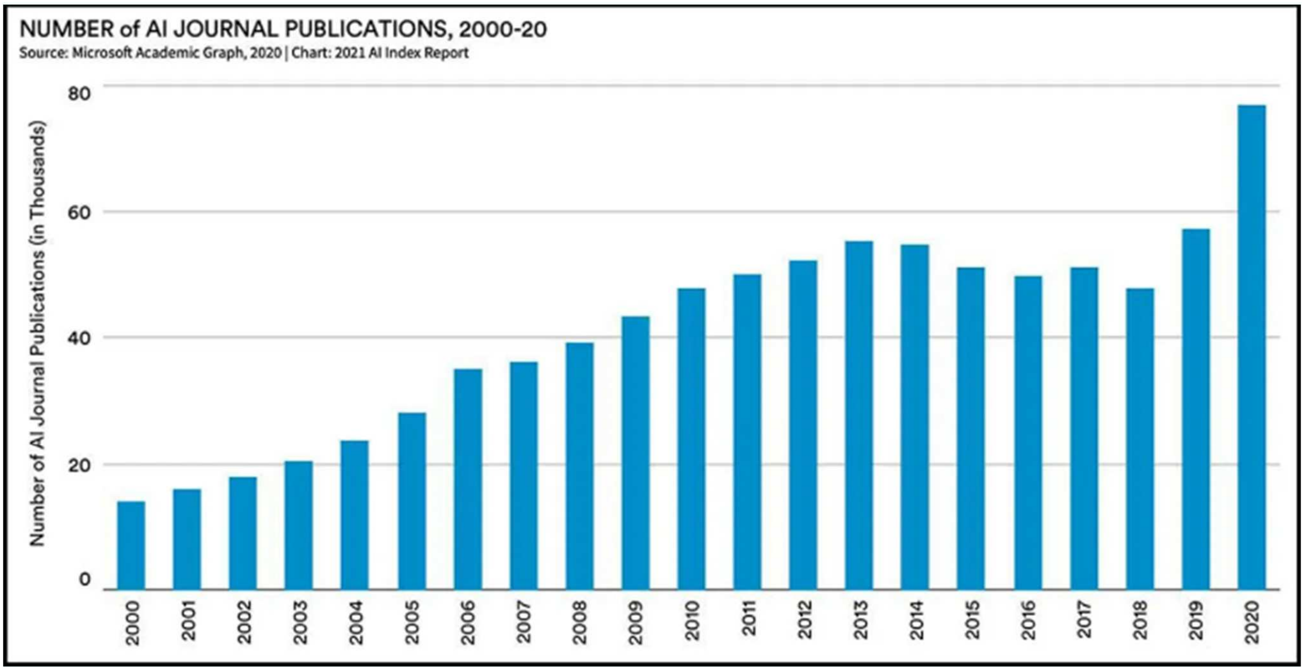


Fig. 3. Number of AI journal publications in 2000-2020 terms. Source https://spectrum.ieee.org/the-state-of-ai-in-15-graphs/language-ai

II. The Regulation of Algorithms

A. The law

The debate over regulation of algorithms, which has started in the US at first, as a consequence of the continuous introduction of new and sophisticated AI Systems, has more recently spread in Europe as well.

As already stated, the rationale under the drive to regulate algorithmic decision-making is that algorithms are developed by humans, who follow traditional mental schemes, paths and models, so that the decision to use or to not to use certain data or to give different score value to the information collected is normally motivated by the underlying business goals that the programs is meant to achieve. In other words, the algorithm may be based on the same old historical and traditional bias and ways of thinking that have created several, significant distortion in our society, hence the need to regulate the way these programs.

Europe has had a tradition of data governance since the implementation of its Directive on the protection of personal data of 1995; as we all know, since 2018 the Directive has been now replaced by the GDPR. Critics of data protection legislation have commonly objected that the regulation of privacy has been a way for Europe to try and fight the technological power and supremacy of the US. This objection does not take into account history, for many reasons: first of all, critics seem to forget that article 12 of the Universal declaration of Human Rights of 1948 forbids "arbitrary interference with privacy" [6]. In addition, data protection legislation has been introduced in Europe since the 70's, that is to say way before the US supremacy in the digital world had emerged. The data protection legislation of Hessen, in Germany, was implemented in October of 1970, and the German federal law on data protection was approved in 1977; in the meantime, other countries, like Sweden, France, Denmark, Norway and Belgium had followed suit and the Strasbourg Convention was signed in January 1981 [7].

Through the years critics have also tried to downplay the importance of the protection of personal data, pretending it to be only bureaucracy without real results; once again this critic is groundless, since protection of personal data, what is generally known and referred to as privacy laws, are the only available tool to mitigate the spread of uncontrolled use of personal data with its impact for our rights and freedoms. The latest legislation on data protection, known as the GDPR, has introduced significant provisions that go in the direction of regulating algorithms though a mix system of accountability and transparency.

The GDPR has introduced a general principle of accountability, which shifts on data controllers the responsibility for the risks and benefits associated with particular uses of personal data. In accordance with this accountability principle, controllers (*i.e.,* the organization carrying out the processing of personal date), are fully responsible for whatever part of the processing they use and rely on to operate their business.

They have to "to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized" [8].

Also, the GDPR continues stating that "Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions". Such decision can be taken only if the data subject has given expressed consent, or if it is required by law or it is necessary to perform a contract between the data subject and the controller [9].

The GDPR forbids decisions based on automated processing "which produces legal effects": examples of processing that can produce legal effects are "automatic refusal of an online credit application or e-recruiting practices without any human intervention", but also "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" [10].

Accountability alone is not enough: therefore, the GDPR establishes also a strict duty of transparency: consent, for example, must be informed, and such information must be "in a concise, transparent, intelligible and easily accessible form, using clear and plain language".

The information requirement has two sides to it: on one hand the obligation on the controller to inform the data subject at the time the personal data are collected, but also the GDPR established a system of individual rights, which again point to transparency of the processing: the right of access, which means the right to obtain a copy of the data being processed; the right of rectification, *i.e.* to have errors and mistaken corrected, and the right to be forgotten, which has spurred a heated many debate, but which actually existed before the GDPR and was finally strongly established in the landmark decision of the European Court of Justice against Google [11].

B. *The Court Cases*

The Courts have already had to express themselves on the matter of the principles outlined above, *i.e.,* accountability and transparency. The first case relates to a public competition for teachers. The Italian Ministry of Education run a public competition to assign teaching jobs, and the outcome of the competition was evaluated through a program. Several claimants challenged the results of the competition, claiming the lack of transparency of the algorithm used to determine the winners.

In its decision of December 13, 2019 the Council of State has stated that the law on similar matters is based on three principles: a) everyone has the right to know the existence of an automated decision-making process and to receive "significant information on the logic being used; b) the principle of non-exclusivity of the algorithmic decision, according to section 22 of the GDPR which establishes that the individuals involved have the right to require human intervention: finally c) the principle of non-discrimination.

In the case submitted for decision, the claimants had not received the relevant information, and the Court has described the level of information required: information on the decision-making mechanism, of the priorities assigned in the evaluation procedure and which data have been used to come to the decision.

Two more cases have been decided more recently, related to two different food delivery platforms. In both cases the riders working for the platform had complained about the way the platform had chosen to assign the deliveries, in both cases discriminating those workers who had complained about the platform, required better pay and insurance, in essence, claiming better work conditions. One of the cases has been decided by the Court of Bologna, the other by the Italian Privacy authority.

In both cases the platform has been found violating the rights of the workers, in that the algorithm that decided the assignment of the deliveries was not transparent. In both cases the platform used an algorithm to evaluate the availability and reliability of the riders, plus another set of information, like the geographic position, but no information had been given or were available as to the logic that led the platform to assign the deliveries to certain riders and not to others. The Data Protection Authority found also other violations of the GDPR [12].

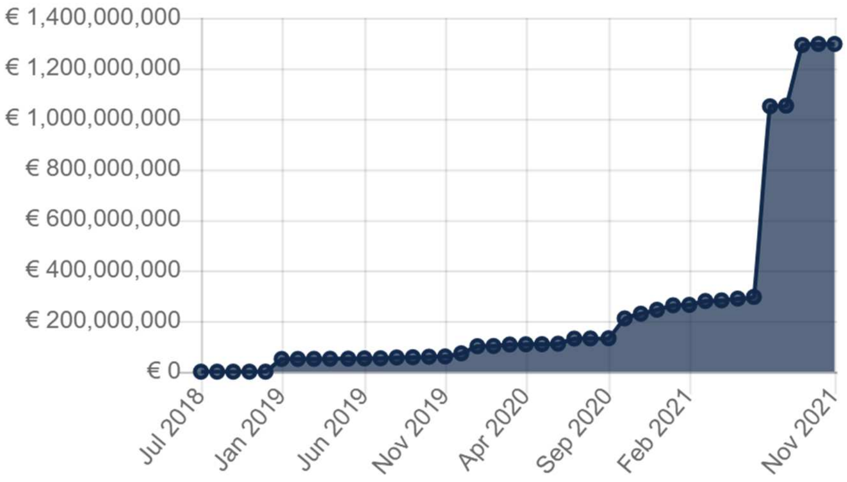


Fig. 4. GDPR: fines imposed versus time; source: source https://www.enforcementtracker.com/?insights.

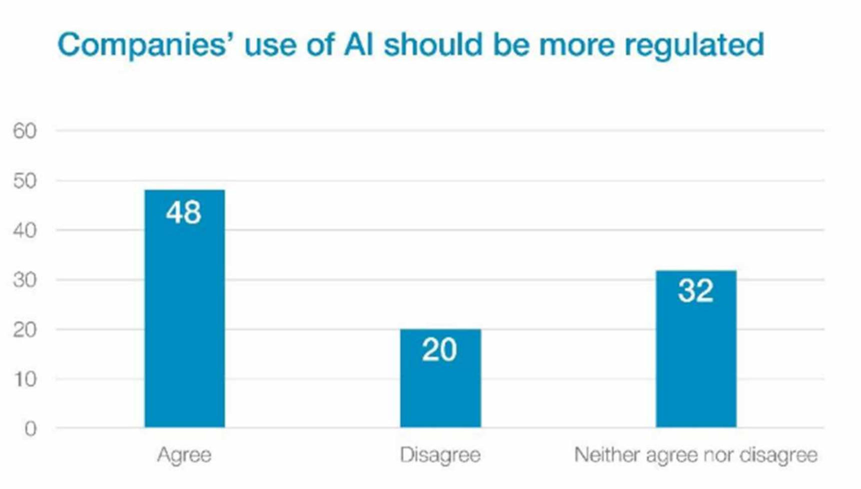


Fig. 5. Consensus about the regulation of the use of AI by companies. Source https://www.aibotics.tech/post/artificial-intelligence-these-3-charts-show-what-people-really-think

III. THE PROPOSED REGULATION OF AI

As has been said before, the EU has been moving swiftly in the field of data governance, therefore the proposed regulation has followed the path already marked from existing data protection and cybersecurity provisions, like the GDPR and the NIS Directive, and has once again put the emphasis on principles like transparency, data retention, security and protection of data, and data breach notification duties.

The definition of AI is the following:

"*artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".

The definition, as everyone can see, is very broad and will most likely be applicable to products and technologies that some may not consider to be AI.

The techniques mentioned in section 3 are:

"(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods".

In any event, the consensus is that this definition will be applicable to a wide range of applications exploiting digital technologies aimed at developing new, innovative products. And it is fair to say that, although the Regulation is far from being approved and implemented, it cannot be ignored by anyone who is presently developing or planning to develop new products in the near future.

The proposed Regulation is, as one can imagine, very complex (180 pages, plus three Annexes) and a summary of it would require quite some time, so I will try to concentrate on a few of the relevant provisions:

1. The Regulation lists a number of “prohibited AI practices”, in short, (a) practices, systems and techniques aiming at “distorting a person’s behavior” whose consequence may be harm to that person or to another person, plus (b) the use by public authorities of systems for the classification of the trustworthiness of a person; and (c) real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement”. This last practice may be allowed, only in special situation and upon certain conditions.

2. The proposal lists quite a number of systems and products which are defined as “high risk AI systems”. The full list of these systems is listed in annex II to the Regulation. The development and placing on the market of such high risk AI Products is subject to a series of requirements, covering risk management systems, data governance, technical documentation, record keeping, transparency of information to users, human oversight, accuracy, robustness and cybersecurity, Fig. 6.

3. In order to avoid forum shopping or non-compliance by non-EU-based manufacturers, the same obligations are placed on third parties like importers, distributors, etc.

4. The proposed Regulation calls for heavy fines which, depending on the violation, can go up to 30 million Euros or 6% of the worldwide turnover of the year preceding the violation, whichever is higher.

IV. The Consequence in the Automotive Field

The first question to ask is: are autonomous vehicles considered High Risk AI? The answer is positive, since Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers asses that, as expressly mentioned in Annex II to the proposed regulation.

The consequence of being a high-risk AI is, first of all, to be subject to all the requirements listed in Title III, Chapter 2 of the proposed regulation, *i.e.*:

a) risk management systems, must be established, implemented, documented and maintained, consisting of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. The risk management system comprises identification and analysis of potential risks; evaluation of additional potential risks estimation and evaluation of such risks that may emerge from the use of the system; adoption of risk management system.

b) data governance: High Risk AI systems that use the training of models with data shall be developed on the basis of training, validation and testing data sets that meet defined quality criteria.

c) technical documentation must be prepared and drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in the regulation.

d) record keeping, *i.e.,* the automatic recording of events (‘logs’), to ensure a level of traceability of the AI system’s functioning throughout its lifecycle.

e) transparency of information to users. *i.e.,* High Risk AI must give users instructions for their use that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users.

f) human oversight: High Risk AI must allow to be effectively overseen by natural persons.

g) accuracy, robustness, and cybersecurity: high risk AI must achieve an “appropriate” level of accuracy, robustness and cybersecurity, which must be declared in the instruction for use.

In practice, the risk management system and record keeping mean that high risk AI systems must be continuously monitored, so that the potential risks not known at the moment of the launch on the market and that have emerged only during the use of the system can be addressed and, hopefully, eliminated. Therefore, all vehicles must have a record keeping mechanism that must communicate with the manufacturer of the system. On its side, the manufacturer must monitor and analyze the data arriving from the vehicles, to detect new potential risks that were not known before and address them.

These obligations must be somehow harmonized with the data minimization and data retention requirement of the GDPR. What I mean is that the manufacturer must clearly declare in its information to the user the kind of processing that it shall do with the data coming from the system and the duration of the retention period. With respect to these provisions there is a question that needs to be answered: will the manufacturer be responsible to perform these obligations for ever and ever? Each product has a given, pre-defined life-cycle, that in the case of a vehicle can be 4 to 6 years or more, depending on use and general conditions. If the product is used beyond the life-cycle, will the manufacturer be obliged to continue monitoring as long as the product is used (used vehicles, second-hand and third-hand are the norm in certain less-developed countries)?

The second question to answer is: as it always happens, each software has several releases; each new release adds new features or improves the ones already existing: shall the manufacturer obliged to supply the new features or will they be installed only upon request? As I have indicated above, transparency is considered already to-day as a specific obligation of the manufacturer or the user of an AI system. The transparency requirement already exists in the GDPR and the new proposed regulation goes into the same direction. In fact, the language used is similar. The GDPR calls for the information to the user to be: “*in a concise, transparent, intelligible and easily accessible form, using clear and plain langu*age” [13], while the proposed regulation requires that the user be given: “*concise, complete, correct and clear information that is relevant, accessible and comprehensible to users*.” [14].

It may seem a trivial point, but describing an AI system in a concise form, easily understandable, using clear and plain language can be a semantic nightmare. Manufacturers will have to make sure that they do not use legalese jargon and that all the information be accessible. Under the GDPR, the information can be given in layers, *i.e.,* users can be given an initial set of basic information, with all the information being easily accessible, for example on a website. Obviously, the information will have to be in the language where the product is sold, so that local would not need to be fluent in English or in the language of the manufacturer.

On the cybersecurity, the proposal follows the same logic of the GDPR: it does not indicate exactly what measure to take, but it also states that the systems must be resilient and the measures must be "appropriate". This means that:

a) it is up to the manufacturer to ensure the right level of security, given he is the only one who has exact knowledge of the specifics of its system; and
b) that the manufacturer is accountable for potential security failure, if it does not prove the adequacy of the measures implemented: the burden of proof will be on the manufacturer.

Finally, the last point I had like to make is related to the human oversight, *i.e.,* the obligation that the system be "effectively" overseen by a natural person, when in use. This obligation has many facets to it, in that the measures to allow human oversight must be built in at the time of manufacturing. In addition, the measures implemented shall enable the individual to whom the oversight is assigned to:

a) understand the capacity and operation of the system, so that anomalies can be addressed asap;
b) be able to interpret the outputs of the system;
c) be able to decide to override the output of the system or interrupt its operation with a simple "stop" button.

V. Pro's and Con's of the Proposed Legislation

I have tried to highlight some of the potential consequences of the new proposed regulation, but the question that is often asked is: is it necessary to have a new regulation on something so complex and difficult to understand? As a lawyer, obviously my answer is positive, and I shall try to explain why.

It is clear that A.I. systems will be challenged in court, for whatever reason and in whatever matter. The point is therefore the following: with no regulation, case law may reach different conclusions on the same matter. In other words, the risk to have different outcome to cases debating the same subject is high. The judges would have to decide on their own, and the decision may be arbitrary and not founded on clear and logic grounds. On the other hand, having a common legal basis, the decisions must be taken according to the same law, and we would not have different results in different jurisdiction. This would avoid the so-called "forum shopping", i.e. the establishment of corporations in countries where the judiciary is more lenient than in others.

On the negative side is the risk of increasing bureaucracy, as may happen when regulatory bodies are established. An additional risk is the slowing down of the development process, due to the high level of controls that have to be put in place. Finally, one point which is specific for the automotive filed is the one related to human intervention. According to the present wording of section 14, the operator using the A.I. system must have a deep knowledge of the technology, be able to understand and interpret the outputs of the system to spot anomalies and malfunctioning, and determine that it is appropriate to either override the decision of the system, or to stop it. Training the users to this level of understanding, skill and knowledge will be a real challenge and may have a severe impact on the industry.

Conclusions

The proposed regulation for AI is not final and far from being approved; yet it poses significant challenges for the automotive industry that will need to be addressed by the industry. Regardless of the fact that the regulation is still not final, it is a clear indication of the direction the European legislator has taken, and any changes most likely shall not substantially modify this course. The requirement for transparency is becoming increasingly Two more cases have been decided more recently, and they both relate to a food delivery platform. The riders working for the platform had complained about the way The same outcome standard has been applied in a very recent case in Italy. The court of Bologna has issued an injunction against a food delivery company, forbidding the use of their scheduling program, used to assign to each worker a time and geographical zone. The effect of the program, according to the court, was a discrimination against certain categories of workers, thus foreclosing them access to more favorable geographical and time zones.

References

[1] R. Zallone, "The privacy paradox or how I learned to have rights that never quite seem to work," AAAI Spring Symposium - Technical Report, 2010, SS-10-05, pp. 199–202.

[2] R. Zallone, "Connected Cars under the GDPR," 2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE), 2019, pp. 1-6.

[3] R. Zallone, "Artificial Intelligence vs Autonomous Cars vs General Data Protection Regulation," 2020 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE), 2020, pp. 1-6.

[4] Brent Daniel Mittelstadt, Patrick Allo, Maria Rosaria Taddeo, Sandra Wachter and Luciano Floridi, "The Ethics of Algorithms: mapping the debate," Big Data & Society July–December 2016, pp.1–21.

[5] Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

[6] https://www.ohchr.org/en/udhr/pages/Language.aspx?LangID=itn.

[7] Convention 108 of the Council of Europe, https://rm.coe.int/1680078c45.

[8] GDPR, Recital 71.

[9] GDPR, Section 22.

[10] GDPR, Recital 75.

[11] Google Spain, Google Inc vs AEPD, Mario Costeja Gonzàles, Judgement of the Court (Grand Chamber) of May 13th , 2014 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=IT.

[12] Tribunal of Bologna, decision of Dec. 31, 2020; Garante Privacy,Aggust 2nd 2021, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994.

[13] GDPR, Article 12.1.

[14] Proposed A.I. Regulation, Article 13.2.