Curentul Juridic – Juridical Current
2019, Vol. 76, No. 1, pp. 45-53

ARTIFICIAL INTELLIGENCE AND LAW: A REVIEW OF THE ROLE OF CORRECTNESS IN THE GENERAL DATA PROTECTION REGULATION FRAMEWORK

Sorina Mihaela BĂLAN [*]

ABSTRACT: *Interest in Artificial Intelligence (AI) research has increased rapidly in recent years, largely due to the many successes of modern machine learning techniques such as deep learning, the availability of large datasets and improvements in computing power. AI is becoming more and more applicable to healthcare and there is a growing list of tasks where the algorithms have matched or exceeded physician performance. Despite the successes, there remain significant concerns and challenges related to the opacity of the algorithm, trust and security of patient data. Despite these challenges, AI technologies will become more and more integrated, for example in emergency medicine in the next years. In 2017, there were many EU and UK legislative initiatives and proposals on the analysis and the impact of artificial intelligence on society, issues of responsibility, legal personality, ethical and legal issues, in the context of increasing volume processing higher data. Since March 2017, the Information Commissioner's Office (UK) has updated its database guide for the development of artificial intelligence and machine learning and to provide GDPR since 25 May 2018. The key challenge for artificial intelligence in personal data processing is to establish that such processing is correct, even with negative social consequences, which are not treated differently by GDPR. The question of the correctness of the regulatory framework is an important part to address the imbalance between big data organisations and personal data subjects, with a series of social and ethical effects to be assessed.*

KEYWORDS: *Artificial Intelligence (AI); General Data, Protection Regulation (GDPR-2016/679); Big Data analytics; Regulations; Collective rights.*
JEL CODE: *K 4*

1. ARTIFICIAL INTELLIGENCE AND THE LAW

The exponential evolution of computing power, data storage and increasing digitization of information have contributed to the current development in AI. AI technologies will have an impact in many areas in the near future, such as emergency medicine. But what is Artificial Intelligence? According to [1], it can be defined as "the theory and development of computer systems able to perform tasks normally requiring human intelligence”. Although there is recent progress [2], AI remains limited but can

[*] University of Dimitrie Cantemir, Târgu Mureş, ROMANIA.

transform society, such as applicability in energy, medicine, transport.

Machine learning is a sub-domain of AI that uses various methods to automatically detect from the data the models needed to predict or make decisions. Models start by chance, improve over time through a learning process using learning machines, rather than rule-based machines.

A type of machine learning is deep learning, which in according to [3] learns to represents complex and abstract concepts in terms of multiple simpler concepts by passing inputs through a large number of layers of interconnected non-linear processing units. There is progress in image recognition and speech recognition, natural language processing, speech synthesis [4-5].

The term "high data analysis" refers to forms of data processing using algorithms with datasets, which is difficult to analyse, either due to data volume or real-time data source processing, and the term "artificial intelligence" and "machine learning" are tools to unlock the datasets, in according to [6].

Since 2017, many legislative initiatives, proposals to examine and address the impact of artificial intelligence on society have emerged. These include:

- the European Commission's proposals for the EU to develop civil law rules on the use of robots and artificial intelligence [7];
- the UK Government's report on the growth of the Artificial Intelligence industry in the UK [8];
- news that the Estonian government is developing rules of liability for artificial intelligence [9];
- Granting Saudi Arabian citizenship to a robot [10];
- residence rights in Tokyo to a chatbot [11].

One of the AI challenges concerns its autonomy. Can it make independent decisions, interact with legal entities without informing its owner? [12].

If so, then, to what extent should the owner or operator answer for AI actions? Can it be part of the compulsory contracts of the operator or its owner? [13].

2. THE GDPR

What are the strategic, practical, organizational and technical implications of GDPR for companies using personal data? According to [14], the EU Data Protection framework to come into force in May 2018, consists of two instruments: the GDPR and the Directive on the protection of personal data processed to prevention, detection, investigation or prosecution of crimes. The general GDPR provisions include new definitions for pseudonymisation, sensitive personal data types, protection policies, and data breach violations. Pseudonymisation refers to the processing of personal data in such a way that the data can not be attributed to a particular subject of data without additional information; this requires keeping the separate additional information and subject to technical and organizational measures to ensure that they are not applied.

Genetic, biometric and health data are mentioned as data types. If genetic data refers to the characteristics of the individual, that are inherited or acquired during prenatal development, the biometric refer to the physical, physiological or behavioral characteristics of the individual and allow a unique identification (facial images, dactyloscopic data). Violation of personal data is a security breach that leads to the destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data, transmitted, stored or otherwise processed.

GDPR requires personal data to be processed transparently, under the responsibility and liability of the operator, in relation to the data subject, in addition to the legal and fair processing provided in DIR95. The GDPR states that the operator is not obliged to maintain, obtain or process additional information to identify the data subject, if the scope data for which data is processed does not require identification by the operator. If DIR95 provided for the unambiguous agreement of the data subject, the GDPR requires the agreement of a data subject to be freely given and to be a specific, informed and explicit indication of his wishes. The data subject has the right to withdraw his / her consent at any time, but the withdrawal does not affect the lawfulness of the processing on the basis of the consent prior to its withdrawal.

GDPR sets out the conditions for child data processing in relation to information society services offered directly to children. The processing of a child's personal data is legal if the child is at least 16 years old. If the child is younger, processing is legal only if it is authorized by the child's parent or curator, but there must be a verifiable consent.

GDPR guarantees the right of the data subject to obtain rectification, erasure and restriction of the processing of his personal data, similar to DIR95 (Articles 16-18), and specifies this right by establishing new conditions for the right to erasure (the right to be forgotten). The person concerned has the right to obtain from the operator to deletion of his or her personal data by withdrawing the consent on which the processing is based, and there are no other processing grounds.

Also, GDPR specifies the conditi ons for restricting data processing and introduces the right of the data subject to data portability. The data subject has the right to transmit personal data directly to another operator who, in turn, is required to ensure that the right to portability of data will not adversely affect the rights and freedoms of others and will not prejudice the right to be forgotten.

The GDPR provides the right of the data subject to oppose to the processing of his data for specified purposes at any time for reasons related to his / her particular situation. This processing is related to the public interest, the exercise of public authority or the legitimate interests of the operator and guarantees the data subject the right to object to the processing of personal data for direct marketing purposes, similar to DIR95, but where the data subject objects, his personal data can no longer be processed for these purposes. The GDPR obliges the operator to provide the data subject with automated means to oppose the processing of his data for information society services.

The GDPR specifies the right of the data subject not to be the subject of automated individualized decisions based solely on automatic data processing and intended to assess personal aspects of the data subject, such as workplace performance, creditworthiness, reliability and conduct (Article 15). GDPR adds the right of the person concerned not to be subject to a profiling measure that can be used as a basis for decision-making, whether automated or not.

The general obligations (Article 24, controller's responsibility) require the controller to implement adequate technical and organizational measures to ensure data protection and accountability for such measures. The GDPR introduces two new obligations: that of controllers and processors to keep track of the processing activities under their responsibility and to cooperate with the supervisory authority (replacing the obligation of

DIR95 to notify the supervisory authority) (Article 30) and the obligation of the controller and processors to designate a representative in the EU if they are established elsewhere (Article 27).

The controller must adopt data protection policies and implement appropriate technical and organizational measures to ensure that the processing of personal data is performed in accordance with the GDPR. Technical measures include, for example, pseudonymization or encryption (Article 32), and organizational ones include keeping a record of processing activities (Articles 30-31) and performing an impact assessment of data protection (Article 35).

GDPR obliges the controller to implement mechanisms to ensure the effectiveness of the implemented measures. Approved codes of conduct (Article 40) or approved certification schemes (Article 42) may be used for this purpose. The GDPR obliges each controller, processor and operator representative to keep a record of processing activities under his responsibility (Article 30), instead of requesting notification of processing operations to the supervisory authority, which is the appropriate DIR95 obligation.

The GDPR establishes data security if it forces both the controller and the data controller to implement the appropriate security processing measures. The GDPR clarifies the obligations of the processor (Article 32) and introduces the obligation both to the controller and the operator to provide notifications of personal data breaches (Articles 33-34).

Following a confidentiality risk assessment, the controller and the processor must take the necessary steps to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any form of illegal processing, in particular any unauthorized disclosure, dissemination or access or modification of personal data.

As regards the personal data breach notification based on Article 4 (2) of Directive 2002/58 / EC on electronic privacy, the GDPR provides that the operator and the operator must meet the following requirements:

- in the case of a personal data breach, the operator must notify the supervisory authority without undue delay and, if possible, no later than 72 hours after its finding, unless the notification has to be accompanied by the reasons for the delay.
- the data controller has the obligation to alert and inform without undue delay after having notified the personal data breach, documented with relevant facts, the effects of the violation and the steps taken to remedy it.

GDPR introduces the new obligation for controllers to perform a data protection impact assessment prior to high-risk personal data processing operations (Article 35). The impact assessment on data protection should include at least the following:

- a general description of the processing operations envisaged and the purpose of the processing, an assessment of the needs and proportionality of the processing operations in relation to the purposes;
- an assessment of the risk for the data subject's rights and risk mitigation measures (ie safeguards, security measures and mechanisms to ensure personal data protection and demonstrate compliance with GDPR).

An impact assessment on data protection is not necessarily required if it has already been carried out as part of a general impact assessment required by law (for example, in the case of data processing by public authorities having a legal basis in the EU or legislation a Member State).

GDPR gives the person concerned the right to lodge a complaint with a supervisory authority and the right to an effective remedy against an operator. GDPRs are specified in bodies, organizations or associations that can file a complaint on behalf of the data subjects, aiming to protect the rights and interests of these individuals.

The GDPR specifies the Member States' obligations to adopt measures implementing Directives similar to DIR95 and to lay down penalties for their breach. The supervisory authorities of the Member States have the right to formulate rules for administrative fines imposed on the operator, the agent or the processor as sanctions for infringements. For example, violation of GDPR principles (such as the data minimization principle) is subject to a fine of up to € 20 million or 4% of the total annual turnover worlwide in the case of an enterprise.

3. CONDITIONS FOR PROCESSING PERSONAL DATA

The one of the challenges in the process of processing personal data is based on the necessary consent, as specified by the GDPR: "freely given, specific, informed and unambiguous indication of the data subject's wishes". ICO studies show that people are reluctant to read privacy notice and suggest that these notices could be provide in video or cartoons format, to encourage people to read. Many people simply provide their personal data because it is the price of using that service. That can this considered to be freely given?

Organizations need to develop their technical capability to meet the data subject's requests to withdrawal consent (if consent is used as the basis for processing). This would be a challenge for monitoring and verifying the data needed for any machine-learning algorithm to make sure that the dataset has not been skewed because of a withdrawl of certain data. According to [16], none of the challenges are resolve, posed by the requirement of affirmative action freely granted for consent or the possibility of withdrawal of consent are addressed.

Data processing must be "necessary in the legitimate interests of the controller or a third party's, legitimate interests, except where these legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child [17]. Organizations should develop their own value framework to test the proposed processing without the operator's certainty that processing would comply with GDPR, for which it would be advisable to create an internal ethics committee.

Like consent, the justification of legitimate interests has more difficulties. Given its links with the principle of fair and legal processing, examining the balance of interests between the operator and the data subject, the justification of the legitimate interests seems to require an assessment of what is fair in the circumstances.

The correctness of processing depends on the effects on people, their expectations of how the data will be used and the level of transparency. For this, controllers will need to properly define and analyze the groups and data available at the outset for the data protection impact assessments (DIPA). There are a number of risks in terms of using mechanical learning and artificial intelligence to create profiles.

A challenge for artificial intelligence is the responsibility and record keeping for organizations whose processing activity is more risky. As technology progresses, it becomes increasingly difficult to understand how the employee works. Increased accountability, improved governance and risk assessment are a step in the right direction.

The Autonomy of Artificial Intelligence (IA) means that models of governance will have to be taken into account in detail. It is necessary to introduce ethics and data protection in the design phase, in the training and implementation phases. There is a risk that AI will process data in violation of the GDPR restrictions, such as an algorithm that analyzes secondary data, could place people in groups that could be discriminatory and would become unjust, without a legal basis.

4. AI AND THE CORRECTNESS OF THE ALGORITHM

The challenge for data processing and analysis is to demonstrate that it is done fairly, and the introduction of AI changes sharply the requirement of fairness, a change in the balance of power between individuals and data controllers. The magnitude and spread of extensive data analysis of all types of social functions, the complexity of processing, and the level of data control exerted by large data companies raise concerns around artificial intelligence [18].

According to [19], many of the Asilomar principles which were developed to provide artificial intelligence bring benefits to humanity, are relevant to data protection: "Personal privacy: people should have the right to access, manage, and control the generated data , given the strength of the AI systems for the analysis and use of this data.”. Another principle that goes beyond the limits of GDPR is: "Human values: AI systems must be designed and operated in such a way as to be compatible with the ideals of human dignity, rights, liberties and cultural diversity.” and "The power conferred by the control of advanced AI systems should respect and improve, rather than undermine the social and civic processes on which society's health depends". These principles indicate a social and ethical dimension of the implementation of AI, which is not addressed directly by GDPR.

According to [20-21], there are collective interests in creating profiles about particular groups (whether or not they are used to make a decision about a particular person), and these interests that assume relevance are of an over-individual nature and a collective dimension that is not adequately addressed by the existing data protection legal framework.

The interests that can be shared by an entire group without conflicts between the views of its members are called agregative, and the conflicts between the opinions of its members are known as non-aggregative interests, the best way to describe the collective dimension of data protection. There are collective privacy and data protection priorities that are relevant to the general interest, and the rationale for collective data protection focuses on potential damage to groups caused by exhaustive and invasive data processing (the COMPAS recidivism algorithm). The COMPAS algorithm produced different and discriminatory results for black people compared to white people. A ProPublica study found that COMPAS predicts black defendants will have higher risks of recidivism than they actually do, while white defendants are predicted to have lower rates than they actually do. It was not enough for people to challenge the decision of the COMPAS algorithm in each instance, but it had to be challenged on the basis of injustice for blacks as a group.

For now, the only people with visibility in COMPAS are its programmers, who are less trained than judges to provide justice. Judges have legal training, are bound by ethical oath, and have to take into account not only their decisions but also their reasoning in public opinion. Programmers do not have all these safeguards. Computers can be intelligent, but they are not wise. Everything they know, we have learned and taught our partisans. „*They do not want to teach them without transparency and corrective action by people*.” [22],

Data protection authorities should have a more proactive approach to reviewing or even licensing artificial intelligence processing personal data, potentially involving other stakeholders as part of a review that would take into account social, ethical and others, the collective impact of a particular form of data processing [20],

The advent of artificial intelligence and machine learning, which are the tools to unlock the value of important data, have led to ethical questions when analyzing data protection. There are many competing views on how ethical data processing should be regulated. Increased accountability and transparency requirements of GDPR pose technical challenges for AI developers.

Is data protection compatible with the analysis of big data, given that the rights of data-processing organizations are opposed to the rights of individuals to prevent certain processing? Regulations and initiatives should encourage a "management" approach where organizations that apply artificial intelligence or large data analysis are responsible and recognize both the social impact of their data processing activities and the trust they have in terms of individual, collective rights and freedoms.

Any future legislation on artificial intelligence in a broad sense must provide for adequate levels of transparency and governance. GDPR does not recognize the collective aggregate interests that appear in building a profile.

According to [21], before the profile is actually applied to make a decision or to initiate an action against a person, the members of this group have an interest in being grouped or not. This profile may affect the individual's identity and the information or challenges they are presented with. The behavior of other members of the group may affect the person. Here, GDPR is deficient in this respect as it does not adequately protect collective interests that need to be addressed in future AI legislation.

Is data protection compatible with the analysis of big data, given that the rights of data-processing organizations oppose the rights of individuals to prevent certain processing?

Regulations and initiatives should encourage a "management" approach where organizations that apply artificial intelligence or large data analysis are responsible and recognize both the social impact of their data processing activities and the trust they have in terms of individual, collective rights and freedoms.

5. CONCLUSION

The key question for artificial intelligence is whether it is "correct". A deeper understanding of "fairness" and ethical approaches in an algorithmic world is needed to provide individuals with effective rights against unfair and socially harmful applications of artificial intelligence, and also to clarify organizations with the point of fairness. Legislation limiting human responsibility for artificial intelligence, granting legal personality to artificial intelligence or other legislative measures to encourage innovation in artificial intelligence can prove to be beneficial.

REFERENCES

Oxford. Artificial Intelligence. English Oxford Living Dictionaries. Available form : https://en.oxforddictionaries.com/definition/artifical_intelligence.

Lynch, S., Andrew, Ng., (2017), Why is the new electricity. Stanford news, Available from: https://news.stanford.edu/thedish/2017/03/14/andrew-ng-why-ai-is-the-new-electricty/.

Lecun, Y., Bengio, Y., Hinton, G., (2015), Deep learning, Nature, 521, pp. 436-444.

Russakovsky, O, Deng, J, Su, H., et al., (2015), ImageNet Large Scale Visual Recognition Challenge, Int. J. Comput. Vis, 115, pp. 211-252.

Jonathan Shen, Ruoming Pang, Ron J. Weiss, et. al., (2017), Natural TTS Synthesis by Conditioning WaveNet on Mel Spectrogram Predictions, http://arxiv.org/abs/1712.05884.

Following the approach of the Information Commissioner's Office in its paper ‘Big data, artificial intelligence, machine learning and data protection (20170904 Version: 2.2)’, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>; Information Commissioner's Office (2017), paras 6–11.

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

https://www.gov.uk/government/publications/growing-the-artificial-intelligence-industry-in-the-uk

https://e-estonia.com/artificial-intelligence-is-the-next-step-for-e-governance-state-adviser-reveals/.

https://www.washingtonpost.com/news/innovations/wp/2017/10/29/saudi-arabia-which-denies-women-equal-rights-makes-a-robot-a-citizen/.

https://futurism.com/artificial-intelligence-officially-granted-residency/.

Holder, C., Khurana, V., Harrison, F., Jacobs, L., (2016), Robotics and law: Key legal and regulatory implications of the robotics age (Part I of II), Comput Law Secur Rev, 32 (3), pp. 383-402.

Chopra, S., White, L., (2004), *Artificial Agents – Personhood in Law and Philosophy*, Proceedings of the 16th European Conference on Artificial Intelligence, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.91.5904&rep=rep1&type=pdf.

European Commission, (2016), European Commission, 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 the Directive 95/46/EC (General Data Protection Regulation), Official Journal L119, 04/05/2016.

Blackmer, W., S., (2016), GDPR: Getting Ready for the New EU General Data Protection Regulation, 22, Information Law Group, InfoLawGroup LLP.

See fn 22 regarding analysis of Article 22, http://privacylawblog.fieldfisher.com/2017/let-s-sort-out-this-profiling-and-consent-debate-once-and-for-all/

GDPR Article 6(1)(f).

Mantelero, A., (2014), The future of consumer data protection in the E.U. Re-thinking the “notice and consent” paradigm in the new era of predictive analytics, Comput Law Secur Rev, 30 (6), pp. 643-660.

https://futureoflife.org/ai-principles/>, The Council of Europe's Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data.

Mantelero, A., (2016), Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer law & security review 32, pp. 238–255.

Mittelstadt, B., (2017), From Individual to Group Privacy in Big Data Analytics, Philos. Technol. 30, pp. 475–494.

www.northpointeinc.com/.../compas/Practitioners-Guide-COMPAS-Core-_ 031915.pdf