

REVIEW ARTICLE

Artificial Intelligence and Independent Authorities

Fereniki Panagopoulou

Associate Professor, Panteion University Ph.D. (Humboldt), M.P.H. (Harvard), LL.M., Ph.D. (National and Kapodistrian University of Athens), Greece.

Received: 24 September 2024 Accepted: 08 October 2024 Published: 23 October 2024

Corresponding Author: Fereniki Panagopoulou, Associate Professor, Panteion University Ph.D. (Humboldt), M.P.H. (Harvard), LL.M., Ph.D. (National and Kapodistrian University of Athens), Greece.

Abstract

In the context of the present paper, we will discuss question of which authority should supervise artificial intelligence in Greece. At the beginning we will analyse all the alternative possibilities and at the end we will recommend our proposal. It is recommended that the Greek DPA be transformed into a National Authority for Privacy, Information and Artificial Intelligence (NAPIAI). This option calls for a restructuring of the DPA, its potential merger with the Hellenic Authority for Communication Security and Privacy (ADAE), the reinforcement of its staff and its enrichment with personnel from several other disciplines, in addition to that of privacy protection.

Keywords: Independent Agencies, Algorithm, Public Administration, Greek Data Protection Authority, Information, Autonomy, Privacy.

1. Introduction

Artificial intelligence affects many aspects of public administration and justice. The functioning of independent authorities involves two strands, namely an administrative and a quasi-judicial one.

Inspired by the example of the Greek Data Protection Authority, which I had the honour of serving for eight years, one could conceive the following working hypothesis: A citizen files a complaint with an administrative service, the service registers it and, following that, the members of the authority, assisted by the thorough and detailed advice provided by its scientific staff, issue a decision on the matter. As a consequence of this, a question on the role of the algorithm in the context of such procedures naturally emerges.

To begin with, on the basis of automated procedures by means of the electronic submission of the complaint, this can be registered under a certain category. The algorithm can retrieve the relevant

legislation and the previous decisions/acts of the independent authority, and recommend a response to the complaint in question. Likewise, the Greek Supreme Council for Civil Personnel Selection (ASEP) can undertake the selection of personnel by automated means: for example, it can screen whether the required qualifications for a post are met by the candidates, classify them and proceed to the selection of the recruits.

In the context of the present paper, we will discuss question of which authority should supervise artificial intelligence.

2. The Question Regarding which Authority will Supervise Artificial Intelligence

2.1 Introduction

The question of which authority should supervise artificial intelligence is the subject of intense debate and reflection on an international level. What is called for is the existence of an effective authority that will (a)

Citation: Fereniki Panagopoulou. Artificial Intelligence and Independent Authorities. *Journal of Public Administration*. 2024; 6(1): 34 -38.

©The Author(s) 2024. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

sensibly balance the protection of autonomy, privacy and intellectual property with the advancement of innovation and research, the strengthening of the market, and the safeguarding of competition; (b) provide certification as to the quality and safety of artificial intelligence systems; (c) supervise and certify applications in which artificial intelligence systems are utilized; and (d) advise the legislator on matters relating to artificial intelligence.

2.2 Alternative Possibilities

The proposed models are the following:

2.2.1 Data Protection Authority (DPA)

At first glance, the easiest and most practical option would be for the Data Protection Authority (DPA) to assume the supervision of artificial intelligence. This option has several advantages: *Firstly*, Article 63(5) of the AI Regulation explicitly provides for the entrustment of market surveillance of artificial intelligence systems used for law enforcement purposes to data protection authorities. *Secondly*, artificial intelligence systems entail, to a large extent, the processing of personal data. Therefore, there is a strong link between the regulation of artificial intelligence systems and data protection. *Thirdly*, the DPA has a wealth of experience when it comes to dealing with artificial intelligence systems, such as biometric facial recognition systems and generative artificial intelligence systems (ChatGPT in particular). *Fourthly*, in the digital world, data protection constitutes a fundamental component of the protection of individual rights and freedoms. Indeed, data protection touches every aspect of modern legal life. *Fifthly*, the risks posed to health, safety and other rights are already taken into account by data protection authorities when assessing data protection impact assessment studies concerning high-risk processing operations. The fundamental rights impact assessment under the Regulation will most likely largely overlap with the DPIA of the General Data Protection Regulation. *Sixthly*, the DPA, as a national competent authority and, in the context of Directive 2016/680/EU, as a supervisory authority of national departments and member of the joint supervisory authorities of the Schengen Information System, the Customs Information System, the Visa Information System, Europol, and so on, already possesses the required knowledge and experience in the field of law enforcement. *Seventhly*, the DPA, as the competent authority under the General Data Protection Regulation, Directive 2016/680, Directive

2002/58 (ePrivacy), and the regulations governing the operation of the major information systems of the Union, already possesses - to a large extent - the necessary knowledge of existing standards and legal requirements. *Eighthly*, the European Data Protection Board, jointly with the European Data Protection Supervisor, adopted an opinion welcoming the selection of the European Data Protection Supervisor as the competent authority for the EU institutions and bodies, and proposing the designation of data protection authorities as the competent authorities for matters relating to artificial intelligence also in the Member States. Due to the special nature of the EU institutions and other EU organizations and bodies falling within the scope of the Regulation, it is deemed advisable to designate the European Data Protection Supervisor as the relevant competent authority for market surveillance. In Statement 3/2024 the EDPS invites Member States to consider the appointment of Data Protection Authorities as market surveillance authorities. *Ninthly*, it prevents questions on unconstitutionality due to the establishment of an authority that would take powers away from the DPA, which is an authority that has been constitutionally enshrined.

Still, there are some disadvantages associated with the option of the DPA. *Firstly*, artificial intelligence constitutes the 4th industrial revolution and cannot be placed under the wing of an authority that is already in existence and which was put in place for a different purpose, namely solely for the protection of personal data. *Secondly*, there is a possibility that the DPA may be biased in favour of data protection vis-à-vis the promotion of research and innovation. From this perspective, it may represent an impediment to artificial intelligence. *Thirdly*, the members of the DPA specialize in data protection and not in artificial intelligence. *Fourthly*, the DPA, as currently composed, is understaffed and will not be able to meet its newly expanded tasks.

2.2.2 Establishment of a National Artificial Intelligence Authority (NAIA)

Artificial intelligence constitutes the 4th industrial revolution and its special nature does not allow for its assignment to an authority that is already in existence. The protection of individuals is closely linked to the protection of their personal data resulting from the development of artificial intelligence; however, it is also linked to other goods, such as research, innovation, competition, systems security and intellectual property, in respect of which the DPA may

not possess the required expertise. For this reason, the possibility of establishing a dedicated supervisory authority for artificial intelligence should be explored. This authority would be composed of experts from the entire range of fields related to artificial intelligence.

This approach is supported by the reasoning that the new authority will focus its attention on all areas relating to artificial intelligence. This argument could be countered by the fact that the division of responsibilities between the supervisory authority and the DPA could lead to confusion over their respective competencies. This raises the issue of which cases will be dealt with by the DPA and which by the specialized supervisory authority. This confusion is further aggravated by the controversy created as to what constitutes artificial intelligence and is, thus, a matter falling under the responsibility of the new authority and what does not constitute artificial intelligence and is, therefore, a matter falling under the remit of the DPA. If both authorities are involved in a case, there is a risk of multiple sanctions for the same infringement and, hence, a violation of the *ne bis in idem* principle. If data protection powers are taken away from the DPA and assigned to the new authority, the new authority will have to fulfil the constitutional requirements of the DPA.

2.2.3 Establishment of a National Authority for Privacy, Information and Artificial Intelligence (NAPIAI)

Another suggestion would be to form a new authority composed of three departments: Privacy, Information and Artificial Intelligence. If this were to be done, there would be no confusion in terms of competencies, as anything related to artificial intelligence would fall under the NAPIAI. The department of Artificial Intelligence will be responsible for the promotion of research and innovation, the protection of competition and intellectual property, the supervision of technology, the certification of artificial intelligence applications, and the provision of expert advice to the legislator. The establishment of a dedicated Artificial Intelligence department will ensure that there is no bias in favour of personal data. At the same time, the provision for the protection of access to information is of crucial importance.

¹Cf. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in Germany and the Information Commissioner's Office in the United Kingdom. See Fereniki Panagopoulou-Koutnatzi, The constitutionally defended protection in the case of release decision-making by the Hellenic Data Protection Authority (HDPa) for data provision, *Administrative Trial Journal* 2017, p. 337 et seq. (340-341).

²Cf. Spyros Vlachopoulos in: Leonidas Kotsalis (ed), *Personal Data, Analysis-Comments-Application*, Nomiki Vivliothiki Publications, Athens, 2016, p. 111 et seq. (124 - 125); and Spyros Vlachopoulos, *Transparency of state actions and protection of personal data. The boundaries between disclosure and secrecy in the executive powers*, Ant. Sakkoulas Publications, Athens-Komotini, 2007, p. 74 et seq.

³See Fereniki Panagopoulou-Koutnatzi, *General Data Protection Regulation: a critical ethico-constitutional assessment one year after its implementation*, *Administrative Law Gazette* 2019, p. 226 (230).

The current trend in European legislation, which is aligned with the equal treatment of individual rights, is the establishment of a single administrative authority for both the protection of personal data, as well as the freedom of information.¹ Therefore, priority should not be reserved solely for the protection of personal data when other conflicting constitutionally protected legal rights, such as freedom of information, are at stake.² This position is in perfect harmony with the GDPR, which emphatically states in recital 4 that “the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.” At the same time, the freedom of expression and information is also enshrined in Article 85 of the GDPR, which strikes a balance between the right to protection of personal data and the right to freedom of expression and information, including processing for journalistic purposes.

In consequence of the above, priority should not be solely given to the protection of personal data when other conflicting constitutionally protected legal rights, such as freedom of information, are at stake. If this were not the case, there would be a reasonable risk that greater weight would be placed on the protection of personal data under an independent constitutional principle than on access to information, which would, in effect, be left ‘orphaned’. The result would be that the controller would prefer - and reasonably so - not to provide the data, as no sanction would be imposed for doing so, rather than providing it.³

All the members of the Authority will be appointed based on the requirements of Article 101A of the Greek Constitution. The introduction of transitional

provisions for the completion of the members' term of office in the existing authorities that may be subject to change is deemed necessary.

2.2.4 Establishment of a new Authority that will be Composed of Members of the DPA, the National Bioethics and Technoethics Committee, Representatives from the fields of Innovation and Research, the Market, and so on.

This model allows for the representation of all stakeholders, removing the legal obstacle posed by the *ne bis in idem* principle,⁴ as all independent authorities will be represented. Nevertheless, Greek practice has shown that this approach may not be workable. It is also stressed that if data protection competencies are taken away from the DPA and assigned to the new authority, the new authority will have to fulfil the constitutional requirements of the DPA.

2.2.5 E. Establishment of a Dedicated Directorate under the wing of a new Authority

A directorate dedicated to artificial intelligence could be integrated into the existing structure of the DPA. This directorate would be composed of full-time permanent members who specialize in personal data, as well as some new members from the fields of innovation and research. This model already exists in Member States such as France⁵ and the Netherlands.⁶ This directorate may be given further flexibility for synergies with academia, research centres and businesses in the field of artificial intelligence, as well as for supporting start-ups. Following more than five years of experience in implementing the GDPR (and at EU level, at that), the DPAs are now ripe and ready to promptly identify and address issues that a new authority would have to deal with, thus achieving the fastest, most efficient and optimal solution in terms of cost/benefit for the national legislator.

Recommendation

In the context of the present submission, it is recommended that the Greek DPA be transformed into a National Authority for Privacy, Information and Artificial Intelligence (NAPIAI). This option calls for a restructuring of the DPA, its potential merger with the Hellenic Authority for Communication Security

and Privacy (ADAE), the reinforcement of its staff and its enrichment with personnel from several other disciplines, in addition to that of privacy protection.

3. Conclusion

On the basis of the above, the following concluding thoughts may be drawn.

Artificial intelligence cannot be left to run without being monitored. For this purpose, it is recommended that the DPA be transformed into a National Authority for Privacy, Information and Artificial Intelligence (NAPIAI). This Authority will have full supervisory powers over all issues related to artificial intelligence, without being limited to the narrow framework of data protection.

Authors' Contribution

I would like to extend my warm thanks to Vasileios Zorkadis, Stefanos Vitoratos, Alexandros Nousias, Georgia Panagopoulou, and Androniki Tzomaka for their contribution to the discourse on the matter of the supervisory authority.

4. References

1. Fereniki Panagopoulou-Koutnatzi, The constitutionally defended protection in the case of release decision-making by the Hellenic Data Protection Authority (HDP) for data provision, *Administrative Trial Journal* 2017, p. 337 et seq. (340-341).
2. Spyros Vlachopoulos in Leonidas Kotsalis (ed), *Personal Data, Analysis-Comments-Application*, Nomiki Vivliothiki Publications, Athens, 2016, p. 111 et seq. (124 - 125).
3. Spyros Vlachopoulos, *Transparency of state actions and protection of personal data. The boundaries between disclosure and secrecy in the executive powers*, Ant. Sakkoulas Publications, Athens-Komotini, 2007, p. 74 et seq.
4. Fereniki Panagopoulou-Koutnatzi, *General Data Protection Regulation: a critical ethico-constitutional assessment one year after its implementation*, *Administrative Law Gazette* 2019, p. 226 (230).
5. Fereniki Panagopoulou-Koutnatzi, *Interpretation of Article 19 of the Constitution*, in Syntagma Watch, available at: <https://www.syntagmawatch.gr/>

⁴See Fereniki Panagopoulou-Koutnatzi, *Interpretation of Article 19 of the Constitution*, in Syntagma Watch, available at: <https://www.syntagmawatch.gr/my-constitution/arthro-19/>, Athens 2022, p. 51. See M. Moustakas, *The ne bis in idem principle and Greek administrative law*, *Theory and Practice of Administrative Law Journal*, 6/2015, p. 134, 174; and Panagiotis Voyatzis, *Ne bis in idem and presumption of innocence from criminal to administrative proceedings: compatibility issues between the ECtHR and the Council of State*, *Theory and Practice of Administrative Law Journal*, 6/2015, p. 533 et seq.

⁵<https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases>.

⁶<https://digitalpolicyalert.org/change/4226-order-on-data-protection-authoritys-supervisory-role-over-ai-algorithms>.

- my-constitution/arthro-19/, Athens 2022, p. 51. 6. Meletios Moustakas, The ne bis in idem principle and Greek administrative law, *Theory and Practice of Administrative Law Journal*, 6/2015, p. 134, 174.
6. Panagiotis Voyatzis, Ne bis in idem and presumption of innocence from criminal to administrative proceedings: compatibility issues between the ECtHR and the Council of State, *Theory and Practice of Administrative Law Journal*, 6/2015, p. 533 et seq.
7. “The CNIL creates an Artificial Intelligence Department and begins to work on learning databases”, French Data Protection Authority website, 2023, available at: <https://www.cnil.fr/en/cnil-creates-artificial-intelligence-department-and-begins-work-learning-databases>
8. “Netherlands: Order on Data Protection Authority’s Supervisory role over AI algorithms”, Digital Policy Alert website, 2023, available at: <https://digitalpolicyalert.org/change/4226-order-on-data-protection-authoritys-supervisory-role-over-ai-algorithms>.