

Report on the meeting between European Ombudsman and European Commission representatives

Correspondence - 19/11/2021

**Case SI/3/2021/VS - Opened on 18/06/2021 - Decision on 17/06/2022 - Institutions
concerned** European Commission | European Data Protection Supervisor |

Case : SI/3/2021/VS

Case title: Artificial intelligence and the EU administration

Date: Wednesday, 29 September 2021

Remote meeting, Brussels

Present:

European Commission

- Head of Unit, DG CNECT A2
- Head of sector AI policy, DG CNECT A2
- Legal and Policy Officer, DG CNECT A2
- Legal and Policy Assistant, DG CNECT A2
- Legal Assistant, DG CNECT
- Head of Unit, DIGIT
- Team Leader-Data Scientist, DIGIT
- Programme Manager - EU policies, DIGIT
- Representative of DG JUST



- Representative of DG HOME
- Planning and policy steering, DG HR
- Senior Expert - Coordinator for inter-institutional Relations - relations with the European Ombudsman, SG
- Legal and Policy Officer, SG
- Administrative Agent, SG.DPO
- Adviser, SG

European Ombudsman

- Rosita Hickey, Director of Inquiries
- Peter Dyrberg, Inquiries and Process Expert
- Valentina Stoeva, Inquiries Officer
- Nicholas Hernanz, Inquiries Officer
- Olatz Fínez Marañón, Inquiries trainee

INTRODUCTION

Rosita Hickey, Director of Inquiries at the European Ombudsman, opened the meeting by welcoming the participants and thanking the European Commission for accepting the meeting invitation. The objective of the meeting was to discuss how the Commission envisages that the recently proposed harmonised rules on Artificial Intelligence (AI) might operate, specifically with regard to the EU administration and public administrations in general. She mentioned the relevance and interest of this topic to the European Ombudsman as well as to the European Network of Ombudsmen (ENO), particularly given that national Ombudsmen have dealt with complaints in this area. She added that the use of AI in public administrations is an issue that raises concerns regarding transparency and protection of fundamental rights.

Representatives of various DGs of the European Commission attended the meeting, including DG CNECT, DIGIT, DG JUST, DG HOME, SG, and HR.

Ms Hickey gave the floor to the Commission for a presentation on its [Proposal for an Artificial Intelligence Act \[Link\]](#) (AIA).

PRESENTATION ON THE PROPOSAL FOR AN ARTIFICIAL INTELLIGENCE ACT (AIA)

The European Commission adopted its proposal for the first ever comprehensive regulation on AI in April 2021. This was the result of several years of preparatory initiatives: the Commission



outlined its European AI Strategy in April 2018, presented a Coordinated Plan on AI (prepared with Member States) in December 2018 and, shortly after that, appointed the High-level Expert group on AI which developed the Ethics Guidelines for Trustworthy AI. The publication of the White paper on AI in February 2020 was followed by a public consultation where more than 1 200 responses were submitted by various stakeholders.

The proposal for an AI Act aims to lay down uniform rules for AI systems in the EU market. It puts forward rules applicable to the whole AI lifecycle including placing on the market, putting into service and using AI systems in the Union. It has two main objectives:

1. to address risks to safety and fundamental rights
2. to create a single market for trustworthy AI in the EU

The proposal for the AI Act aims to provide an innovation-friendly and a proportionate risk-based framework that seeks to avoid overregulation while providing legal certainty to providers and users and stimulating trust in the market. It would also create a level playing field for key actors across the AI value chain independent of their origin (from the EU or third countries).

Regarding the scope of application, the regulation would be applicable to:

- Public and private providers, independent of their origin, placing on the market or putting into service AI systems in the Union;
- Users of AI systems who are located within the Union;
- Other providers and users, where the output produced by the AI system is used in the Union.

EU institutions, bodies, offices and agencies are also covered by the regulation when they are acting as providers or users of AI systems. The regulation would, however, not apply to national security (excluded in principle from the scope of EU law), AI for exclusively military purposes (for dual-use AI systems, the regulation would apply), and public authorities and international organisations in third countries acting under agreements for law enforcement or judicial cooperation with the EU or a Member State.

The proposal defines AI systems based on the definition provided in the OECD Council Recommendation on AI [1] and takes into account two cumulative elements:

- Functional definition: AI is a software where the human provides a set of objectives (not explicitly the rules to reach those objectives) that generates outputs such as content, predictions, recommendations, or decisions influencing the environments it interacts with; list of techniques and approaches for development of the software (Annex I) grouped under learning, reasoning and modelling approaches. This list can be updated by the Commission over time to take account of technological and market developments.

The proposal for the AI Act uses a risk-based approach, meaning that regulatory intervention is needed only when necessary depending on the level of risk to safety and fundamental rights that an AI system is likely to pose. The proposal classifies AI systems in four categories:



- unacceptable risk (four prohibited AI practices: harmful subliminal manipulation; exploitation of vulnerabilities of certain people; social scoring by public authorities; and real-time remote biometric identification for law enforcement purposes in publicly accessible spaces subject to certain strictly defined exceptions),
- high risk AI systems (permitted but subject to compliance with requirements),
- AI posing certain transparency-related risks (permitted subject to information obligations), and
- AI posing minimal or no risk (permitted without additional restrictions but possible compliance with voluntary codes of conduct).

The high-risk category, which encompasses the core part of the legislative proposal, includes two main categories of AI systems:

1. AI systems intended to be used as safety components of certain regulated products (Annex 2)
2. Certain stand-alone AI systems intended to be used in pre-defined areas (specific use cases listed in Annex 3), including certain systems inter alia in the following areas (most relevant for Ombudsmen):
 - remote biometric identification and categorisation;
 - employment and workers management, access to self-employment;
 - access to and enjoyment of essential private services and public services and benefits;
 - law enforcement;
 - migration, asylum and border control management;
 - administration of justice and democratic processes.

The proposal for an AI Act sets out in detail the requirements for high risk AI systems, namely:

- use of high-quality training, validation and testing data and data governance procedures,
- establishing documentation for the system and design logging features,
- ensuring appropriate degree of transparency and providing users with information,
- enabling human oversight,
- ensuring robustness, accuracy and cybersecurity.

In order to ensure compliance with these requirements, the bulk of the obligations is placed on the provider, with lighter user obligations aiming to ensure that the AI systems are safe and compliant with fundamental rights throughout their lifecycle.

1. Provider obligations:

- undergo ex ante conformity assessment to demonstrate compliance with AI requirements before the system can be placed on the EU market/put into service (self-assessment for AI systems listed in Annex III of the Commission proposal, except for remote biometric identification systems) and potential re-assessment of the system (in case of significant modifications);
- establish and implement quality management system in its organisation;
- draw up and keep up-to-date technical documentation;
- keep logs to monitor the operation of the high-risk AI system (when empowered by law or the user);



- register stand-alone AI systems in a public EU database;
- affix CE marking and sign a declaration of conformity;
- conduct post-market monitoring and take corrective action;
- report to market surveillance authorities serious incidents and malfunction that can pose risks to fundamental rights;
- collaborate with market surveillance authorities.

2. User obligations:

- operate AI systems in accordance with instructions of use;
- ensure human oversight when using AI systems (essential for public authorities);
- monitor operation for possible risks;
- inform the provider or distributor about any serious incident or any malfunctioning;
- use the information given by the provider for the data protection impact assessment (where applicable);
- existing legal obligations for users continue to apply.

In order to address, in particular, opacity and ensure transparency towards the wider public, the proposed AIA includes provisions on:

1. transparency and traceability of high-risk AI systems (Articles 11-13)
2. access rights for competent supervisory authorities (Article 64)
3. transparency towards affected people (people must be informed when they are using certain AI systems, including when not classified as high-risk) (Article 52)
4. public oversight: EU-wide publicly accessible database of stand-alone high-risk AI (Article 60).

As regards how the proposal addresses discrimination risks and risks to other fundamental rights, the Commission explained that the proposal for an AI Act would facilitate the implementation of the existing EU and national equality laws and thus minimise risk in cases where 'high-risk AI systems' may be involved. To this end, it provides for requirements and relevant obligations to ensure:

1. implementation of risk management systems
2. high quality of datasets
3. human oversight
4. accuracy and robustness
5. measures to enable tracing and proof of breaches to fundamental rights.

As to the governance structure of the Act, it is based on a system covering national and EU



level. The national level would play a key role for enforcement through national market surveillance authorities. The EU level would coordinate implementation and exchange information through an EU AI Board (the Commission would act as the Board's Secretariat). The European Data Protection Supervisor (EDPS) would be the market surveillance authority for the EU institutions, offices, bodies and agencies. There would also be a Commission expert group for technical and scientific advice where all relevant stakeholders are represented (civil society, academics, businesses etc.).

The tasks of the European AI board would be to:

- facilitate consistent application of the legal framework by Member States;
- contribute to market monitoring;
- collect and share best practices;
- contribute to standards / AI policy;
- provide advice on AI issues.

The proposal for the AI Act includes new mechanisms for cooperation and powers for public authorities responsible for fundamental rights supervision (e.g. equality bodies, data protection authorities, Ombudsmen offices, etc.):

- to request access to any documentation maintained under this Regulation when that is necessary to perform their duties under their mandate;
- to request joint testing of high-risk AI systems to be organised by the market surveillance authorities;
- to be informed when market surveillance authorities suspect that an AI system presents a risk to fundamental rights;
- to be informed by market surveillance authorities about reported malfunctioning of high-risk AI systems which constitutes a breach of fundamental rights obligations under Union or national legislation.

The Commission gave an overview of the next steps. The proposal is now being negotiated by the Council and the European Parliament. Once adopted, there would be a two-year transition period, after which the AIA should become directly applicable in its entirety and obligatory for operators following a two year transitional period after its entry into force. In parallel, harmonised standards developed by the European standardisation organisations (CEN/CENELEC, ETSI) should be ready and support operators in the practical implementation of the new requirements and conformity assessment procedures.

QUESTIONS AND ANSWERS

The European Ombudsman (EO) team raised a question concerning the tasks of public authorities in fundamental rights supervision. The representatives of the Commission answered that the Member States (MSs) are free to designate the relevant market surveillance authorities who may also be authorities exercising fundamental rights supervision (the Commission specifically mentioned data protection authorities). In addition, national public authorities or bodies which supervise or enforce the respect of obligations under Union law protecting fundamental rights could request access to any documentation created or maintained under the



AI Act which would allow them to fully execute their tasks. There would also be new opportunities for joint testing of AI systems and exchange of information with market surveillance authorities.

Each MS would have to identify the supervisory authorities for fundamental rights and make the list of authorities publicly available. They should also be notified to the Commission and all other Member States.

I. The work of Ombudsmen institutions and other oversight bodies

1. Within the Ombuds institutions community, issues related to the use of AI can pose challenges to their investigative capacity and negatively impact citizens' ability to complain (e.g. citizens are not aware that AI is being used and therefore cannot outline this aspect in their complaint). It is also considered that in the face of the challenges posed by the use of AI, different oversight bodies should be prepared to cooperate and that rules should be revised to facilitate this joint work. [2] Has this experience/these challenges fed into the Commission's thinking to date in any way?

The Commission representatives agreed that there were valid concerns regarding the use of AI and its possible negative impact on the ability of citizens to complain. The Commission said that it was one of the underlying reasons for this Act. The regulation should fully empower citizens to make use of their rights.

Under the AIA, Ombudsman Offices could be identified by Member States as national bodies supervising fundamental rights protection and thus take advantage of the access rights to documentation, and new mechanisms for cooperation with market surveillance authorities. The Commission welcomes any further suggestions about the implementation of the regulation. The regulation includes various kinds of transparency provisions e.g. toward the people who are confronted with certain AI systems so that they know when they are interacting with an AI system. These transparency obligations are complementary to the ones in existing legislation, e.g. in consumer protection or data protection legislation at EU and national levels.

2. Could the Commission provide some examples of AI-powered tools currently used or being planned by national public administrations that will impact citizens and may lead to an increase of complaints received?

There is an uptake in some national administrations using AI, including techniques that are more sophisticated. Given the general sensitivity of relevant use cases, they often become publicly known after some time has elapsed from implementation. Given the scarcity of publicly available information, it is also not always absolutely certain whether the algorithm is really an AI system or traditional software where the outputs produced are the direct result of rules explicitly pre-defined by humans.

With these two caveats, the Commission provided three illustrative examples of use of AI powered tools by public administrations.

The Netherlands



In 2014, the Dutch Ministry of Social Affairs and Employment developed a risk calculation model called *Systeem Risico Indicatie* (SyRI) to predict an individual's likelihood of engaging in benefits and tax fraud, and violations of labor laws. SyRI used artificial intelligence to search various government databases containing personal data. Concerns were raised by human rights organisations that the system was disproportionately targeting low-income neighbourhoods. A Dutch court banned the system in February 2020 because the government had not been transparent enough about how the algorithms worked [3] .

Spain

In 2017, the Spanish Ministry for Green Energy Transition ran an AI-powered software called BOSCO that reviews applications for a social bonus granted by the Spanish government to poor households for their electricity bills. Due to a malfunction of BOSCO, over half a million applicants saw their request for a social bonus rejected even though they fulfilled the requirements for receiving financial aid. The Spanish administration refused to share the software source code, arguing that it would be an infringement of intellectual property rights, even if it was of public use. As a result, the glitches could not be found. In the end, a Spanish court ruled that the code should be made public. [4]

Belgium

In 2018, in Flanders, several cities started organising school registration via a central online system that uses an algorithm to decide in which school a child can be registered. In order to avoid social segregation in different schools, the city of Leuven implemented a set of variables in the algorithm: on the basis of the answers given by parents to a series of questions relating to the education level of the mother and whether or not the student receives a grant, students were divided into 'indicator students' (defined as having fewer life chances) and 'non-indicator students'. Another variable was distance from home to school. The system left out a high number of students and the algorithm showed flaws as it was randomly placing students in schools far away from their homes.

II. Transparency

1. What are the envisaged transparency obligations under the proposed AI Act and how would those apply to the EU institutions when acting as a provider or user of an AI system? What is the difference between the transparency obligations under the Proposal and the GDPR obligation to inform users of the logic involved in automated decision-making (profiling) tools?

One of the main objectives of the AIA is to address the opacity of AI systems in their inner working and towards users and people affected by those systems as well as competent supervisory authorities. For more details, see above in the presentation the relevant transparency requirements.

In relation to the interaction with the GDPR, the proposed AIA does not limit the rights that the GDPR grants in its Article 22, which are fully applicable. People should be informed when solely automated decision-making systems with legal and similarly significant effects are used. These



rights will be facilitated by the proposed AI Act. By ensuring that the functioning of AI systems is traceable and transparent 'by design', the AIA would facilitate compliance with data protection obligations for explanation, human intervention and redress rights of affected people according to existing mechanisms, including data protection law.

2. Is it possible to give an indication of the types of processes and activities that the Commission, as an administration, currently uses AI for and what the Commission's plans are in this regard?

The Commission explained that with regard to internal AI uses, it is still in the exploratory stage. The Commission is looking into AI that could help policy-making processes or the general functioning of the Commission. E-translation is one field of interest and use. For example, there is a translation tool on the platform of the Conference on the Future of Europe [5]. Users are informed about the fact that they are using AI. Virtual assistants (chat bots) might also be used for both internal and external interactions in the future. For instance, Eurostat is considering this in relation to statistical information. Another area that is being considered is advanced analytics supported by AI, e.g. to analyse feedback on policies provided by citizens on the "Have Your Say" Portal (as an example, the Commission said that it had received 4 million replies to its public consultation on 'summer time'). In line with its upcoming obligations under the proposed AI Act, the Commission has already started work to develop a Code of Conduct and Guidelines for the development and use of AI in the Commission.

Other plans include a tool for web-scraping, which would allow the Commission to gather information from the web on how EU policies are applied. Web-scraping of online marketplaces, as well as the use of camera recognition software, could also in the future help to detect and prevent dangerous products entering the EU.

The Commission is also considering AI in the field of human resources management. This is still in the very early stages. The interest is in using AI in recruitment processes (e.g. AI would allow the matching of job descriptions to CVs of applicants). This project is still in the research phase. There is an awareness of the biases that could arise from using AI in these types of scenarios. The European Personnel Selection Office (EPSO) is also investigating how AI could be used in its work and processes.

3. How is the citizens' perspective and participation ensured under the AI Act?

The main guarantee in this regard is that the proposed AI Act requires providers to inform citizens when they are dealing with AI (Article 52 of the AIA) and citizens can also access the publicly available information for all high-risk AI systems placed or put into service in the EU market (Article 60 of the AIA). Also, if and when citizens are users of high-risk AI systems, the provider has to provide them with more detailed information about the capabilities and limitations of the system, including information on all possible risks.

Furthermore, when citizens feel that their rights have been violated by an AI system, they can complain to the market surveillance authorities and/or the authorities they already know, such as data protection authorities, consumer protection authorities, anti-discrimination authorities,



ombudsmen, etc. These authorities can then request access to all relevant information for the high-risk AI system. The advantage for the citizen is that they do not need to address new and unknown authorities and that there is an integrated approach to their concerns, whilst competent authorities can analyse the AI, if needed even including the source code.

As part of the governance system at EU level, the Commission also plans to establish an expert group which would include *inter alia* civil society organisations representing citizens and their interests.

III. Good administration

1. The EU administration as user of AI. Is it possible to give an indication of the types of obligations that are envisaged for users and their link with principles of good administration?

Accuracy, traceability, accountability, effective human oversight, data protection, etc. are all principles that bind the EU administration and whose implementation the proposed AI Act aims to facilitate in practice.

The EU administration can be both a provider and a user of AI systems.

If EU institutions, bodies, offices and agencies are developing the systems in-house (not 'buying them off the shelf as a finalised product' from the market), the EU administration will be considered 'provider' when putting those systems into service for its own use. It would accordingly have to comply with the requirements in title III, chapter II (risk management, data quality, traceability, transparency, human oversight etc.) and undergo conformity assessment procedures based on internal checks (no involvement of third parties except for biometrics). Relevant procedural obligations are also applicable such as obligations to have in place a quality management system and a system for post-market monitoring, keep documentation and logs, report malfunctioning leading to breaches of fundamental rights obligations, etc.

If a public authority is not developing the system in-house, but buying it 'off the shelf', it would be just a user exercising authority over the use of the AI system, and it would have to comply with all ensuing obligations (e.g. in relation to prohibited practices in Article 5 of the proposal, transparency obligations towards affected persons under Article 52). For high-risk AI systems, there are also new horizontal obligations for users:

- follow the instructions for use and exercise effective human oversight (particularly important for public authorities to ensure accountability and legality of their actions)
- ensure that input data is relevant in view of the intended purpose of the high-risk AI system
- monitor the operation and, when the use may result in the AI system presenting a risk to fundamental rights, inform the provider or distributor and suspend the use of the system
- keep the logs automatically generated by that high-risk AI system
- use the information given by the provider to comply with their obligation to carry out a data protection impact assessment under GDPR/Law Enforcement Directive (LED), where applicable.



All these obligations will help public authorities (regardless of whether they are developing the system in-house or buying it from the market) to comply with their existing obligations under public administrative law and principles of good administration. The obligations should help ensure accountability of how they use high-risk AI systems, reason their AI-based administrative decisions with more transparent and explainable systems, and use only tested and validated systems for bias, accuracy and security that are subjected to meaningful human oversight and ongoing monitoring for risks to fundamental rights. These obligations and requirements would also help supervisory authorities detect, investigate and punish breaches of fundamental rights obligations when high-risk AI systems are used by public authorities and other users.

2. Is the Commission aware of any AI-powered tools being used by the Commission or by other EU agencies or bodies, for example in the field of HR/staff matters, EPSO/recruitment, or border monitoring (Frontex, EASO, eu-LISA) which could lead to more complaints in the future?

There is currently no AI deployed within the Commission's HR services. They are currently in an exploratory/research phase. However, there are some preliminary informal discussions regarding the potential use of AI in recruitment processes. EPSO is also investigating how AI could be used in the framework of selection procedures.

For AI used by EU agencies in the field of home affairs, see reply below.

3. Is there any plan to use AI-powered chatbots or automated voice-controlled assistants at the level of EU institutions, bodies or agencies in order to increase the efficiency of dealing with requests from citizens (e.g. Europe Direct)?

There are two ongoing projects involving the Commission's Directorate General for Communications (DG COMM). The first one is about interaction with citizens on social media. AI will provide backstage support to social media staff. The second project, with Europe Direct, is about setting up a knowledge repository behind the information that staff members need in order to reply to citizens, in particular linking and retrieving information that could be relevant. AI could be used in question classification.

The Commission also said that Frontex, EASO and eu-LISA operate under their own regulations and can use certain AI tools allowed by their mandate. The agencies are subject to strict supervisory systems in relation to data protection. EASO, for example, uses an [early warning and preparedness system \[Link\]](#). Frontex undertakes [risk profiling \[Link\]](#), for example of vessels. eu-LISA is the agency responsible for the home affairs databases. It is planning to boost the performance of the databases through AI, in particular for travellers using the Schengen Information System through increased accuracy for biometrics. eu-LISA is strictly limited to maintaining the databases, it has no direct interaction with individuals, unlike MS authorities at the borders. The Commission explained that smart border gates are using AI to verify the identity of a person. There are plans to use deep learning capabilities on biometric data for border checks. This is not new; it has been used since the entry into force of the Visa Information System in 2011. The Commission said that it did not receive any complaints on the



use of the system. AI technologies significantly contribute to improving the data accuracy of the systems. The Commission has concluded that AI tools are helping to improve fundamental rights in these situations.

IV. Fundamental rights

1. The right to good administration is a fundamental right. What ex ante and ex post controls of respect for fundamental rights are envisaged under the AI Act? What is the relation between the ex ante and the ex post control?

The AI Act envisages a combination of ex ante (before a high-risk AI system is placed on the market/put into service) and ex post enforcement.

Ex ante conformity assessment procedures are mandatory for high-risk AI systems in line with the procedures already established under the existing New-Legislative Framework (NLF) product safety legislation. The provider should demonstrate compliance with the requirements for high-risk AI listed in Articles 9 to 16 of the AIA. The ex-ante assessment (through internal checks or with the involvement of a third-party) is split according to the type of risks and level of interplay with existing EU legislation on product safety - Annex II subject to third party conformity assessment and Annex III subject to self-assessment (with the exception of remote biometric identification (RBI) systems). For systems in Annex III, the provider should also register stand-alone high-risk AI systems in an EU database that would be managed by the Commission, which will enhance transparency. Furthermore, in any of these cases, recurring re-assessments of the conformity would be needed in case of substantial modifications to the AI systems.

An ex-post system for market surveillance will be established by national competent authorities designated by the Member States. Their task would be to control the market ex post and investigate compliance with the obligations and requirements for all high-risk AI systems already placed on the market. The prohibitions under Article 5 and the transparency obligations under Article 52 will also be enforced ex post. Market surveillance authorities would have all powers under Regulation (EU) 2019/1020 on market surveillance [6] , including - among others - powers to: follow up on complaints for risks and non-compliance; make on-site and remote inspections and audits of the AI systems; request documentation, technical specifications and other relevant information from all operators across the value chain; request remedial actions from all concerned operators to eliminate the risks, or where the non-compliance or the risk persists, prohibit or order its withdrawal/recall from the market/immediate suspension of use; impose sanctions for non-compliance with the obligations.

2. How does the proposal ensure that there is no discrimination bias or algorithmic discrimination, in particular on the grounds of gender and ethnicity?

The proposed AI Act includes various requirements for high-risk AI systems regarding **data quality and data governance procedures** (design choices and assumptions, labelling, data



gaps assessment, bias examination, etc.). Data sets with which the system is developed and tested should be representative, relevant, complete and accurate and include appropriate statistical properties of the persons on which the system is intended to be used (Article 10 of the Act). The provider should also establish a **system for risk management**, including obligatory prior testing to address the risk of discrimination in view of the intended purpose of the system. This will counteract bias and discrimination. Standards to verify data sets will be laid down to support providers in demonstrating compliance with these new requirements.

In addition, **traceability and documentation** would be required to enable to trace back the AI systems results. The **requirements for accuracy** will require testing and validation of the system that it performs reliably across different demographic groups and transparency for the metrics used. Finally, the requirements for **transparency and human oversight** help users of high-risk AI systems identify risk of discrimination and take appropriate measures to address them. This human oversight should address any limitations of the system and also avoid 'bias automation' when the person relies automatically on the system's output. Users will also have to continuously monitor the system and report any malfunctioning that may cause breaches of fundamental rights obligations, including discrimination.

These requirements will be assessed throughout the entire life cycle of the high-risk AI systems.

V. European Artificial Intelligence Board

The current proposal is to create a Board comprising representatives from MSs, the EDPS and chaired by the Commission to:

- facilitate the harmonised implementation of the regulation;*
- provide guidance to the Commission;*
- contribute to the effective cooperation of the national supervisory authorities*

Could the Commission provide more details on the set up, objectives and envisaged functioning of this new body?

The objective of the European AI Board is to complement implementation at national level by serving as an EU advisory body and platform for exchange between Member States. To that end, it would be responsible for a number of tasks, including collecting and sharing best practices among MSs and contributing with opinions, recommendations, advice or guidance on matters related to the implementation of the Regulation.

The Commission would act as a chair and secretariat of the Board, be responsible for convening meetings and preparing the agenda as well as providing administrative and analytical support. With regard to the composition of the Board, it would comprise high-level representatives of each MS national supervisory authority, the EDPS and a Commission



representative as a chair.

The composition of the Board should allow for meaningful exchanges between and with the national authorities who observe the functioning and implications of the use of AI systems in their daily work. The members of the Board will provide insights into how AI may affect citizens and how to respond on the regulatory level. Citizens should benefit from the exchange of best practices, guidance and recommendations. This would ensure that in Europe the best possible, harmonised approach is being applied.

The internal functioning would be decided upon by the Board itself, as it would develop and adopt its rules of procedures. These would also contain operational aspects related to the execution of its tasks. The Board is free to design its internal structure and may also set up sub-groups for specific topics and questions.

As a complementary action (and currently not foreseen in the Regulation), the Commission intends to introduce an independent expert group in the implementation process. The expert group would be composed of experts who are recruited and remunerated by the Commission in order to provide additional expertise to the Board and the Commission, where required.

CONCLUSION

The EO representatives thanked the Commission representatives for the information shared, including the power point presentation that will be made available to ENO.

Brussels, 29 September 2021

Rosita Hickey Valentina Stoeva

Director of Inquiries Inquiries Officer

[1] <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>

[2] Ombudsmen reports:

<https://www.nationaleombudsman.nl/nieuws/onderzoeken/the-citizen-is-not-a-dataset> [Link]

<https://www.defenseurdesdroits.fr/sites/default/files/atoms/files/synth-algos-en-num-16.07.20.pdf>
[Link]

<https://bcombudsperson.ca/guide/getting-ahead-of-the-curve/> [Link]

[3]

<https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court>
[Link]



Full judgment text in English:

<https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:1878> [Link]

[4] The case is mentioned in the following article (in Spanish):

<https://derechocal.es/opinion/control-judicial-de-los-algoritmos-robots-administracion-y-estado-de-derecho> [Link]. See also this article: "Being ruled through secret source code or algorithms should never be allowed in a democratic country under the rule of law" | Civio [Link]

Before reaching the courts, the matter was presented before the Consejo de Transparencia y Buen Gobierno- CTBG (Council of transparency and good governance). Its decision on the matter was published in February 2019:

https://www.consejodetransparencia.es/ct_Home/Actividad/recursos_jurisprudencia/Recursos_AGE/2019/128_parti [Link]

[5] <https://futureu.europa.eu/?locale=en>

[6] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011.