

CHAPTER 5

EUROPEAN UNION

*Barbara Marchetti**

I. Is there a national act containing a legal definition of Automated Administrative Decisions?

No, there isn't. The use of AI (Artificial Intelligence) by Union agencies and institutions is regulated by Regulation (EU) No. 2024/1689, the European Artificial Intelligence Regulation. While it does not define what an automated administrative decision is, Article 3 describes artificial intelligence as “a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”.

The regulation, grounded in Article 114 of the TFEU, sets out harmonised rules on the placing on the market, putting into service, and use of AI systems within the Union. It establishes prohibitions on certain AI practices, specific requirements for high-risk AI systems, obligations for their operators, harmonised transparency rules for certain AI systems, and provisions for the placing on the market of general-purpose AI models.

In broad terms, AI is therefore regulated by the European Union as a potentially risky product, adopting an approach proportional to the level of risk involved.

Although it primarily deals with products, a systematic reading of the text makes it clear that it governs the development, marketing, and use of AI systems by both private entities and public bodies, including Union institutions and public bodies.

This is clear from numerous provisions in the regulation, beginning with the identification of prohibited practices in Article 5 (some of which refer to law-enforcement activities under the purview of public authorities), and the list of sectors in Annex III referenced in Article 6 on high-risk systems, which covers activities, functions, and tasks typically within the public sphere. Examples include access to

* Full Professor of Administrative Law, Faculty of Law, University of Trento.

essential public services such as education and healthcare, access to employment and personnel evaluation procedures, and justice and democratic electoral processes, as well as border control, policing functions, AI systems used for critical infrastructure, and non-prohibited biometric identification or categorisation systems.

Furthermore, the regulation imposes specific obligations for public deployers (Article 26 and 27), notably requiring an impact assessment on fundamental rights. It also establishes a framework for sanctions for violations, with different treatments for private and public entities¹.

Although this is not a regulation specifically dedicated to European administration or the use of AI in the public sphere, nor a framework for automated administrative decision-making, it imposes obligations on European administrations that develop and use AI systems in carrying out their duties.

II. Is there a general legal basis (either at the constitutional level or in the Administrative Procedure Act) for the use of algorithmic automation and/or artificial intelligence (AI) by public authorities (government, agencies, local authorities, and specialised bodies)? If no such legal basis exists, are there any legislative provisions that permit public authorities to experiment with algorithmic automation or AI?

For the European Union institutions and bodies, the AI Act serves as the legal basis for the use of AI in the performance of their tasks. As a legislative act of the Union, issued following the ordinary legislative procedure, the regulation must be compatible with the Treaties and the Charter of Fundamental Rights of the European Union, and it also serves as a benchmark for the legitimacy of secondary acts, decisions, and guidelines adopted by the EU administration in this area.

While it does not expressly concern the exercise of public powers through algorithms, it establishes minimum rules and safeguards for

¹ On the applicability of the AI Act to EU Institutions and Agencies, see also European Ombudsman, *Closing note on Strategic initiative concerning the impact of artificial intelligence on the EU Administration and public administrations in the EU* (SI/3/2021 VS) para. 16 ff, available at <https://www.ombudsman.europa.eu/en/opening-summary/en/144117>. A list of AI applications deployed by public authorities in EU Member States and at the EU level can be found at <https://app.powerbi.com/view?r=eyJrjoiZWRmMjlkMTIzMjFmMS00YjRmLWlzMmQtZjdkOTA1ODg2YjBkliwidCI6ImlyNGM4YjA2LTUyMmMtNDZmZS05MDgwLTcwOTI2ZjhhZGRiMSIsImMiOjh9>.

administrations that develop or use AI systems, with direct implications on their relationships with citizens.

In cases where AI systems have a bearing on the adoption of individual decisions, the safeguards established in reg. 2024/1689 must align with the guarantees provided by Article 41 of the Charter of Fundamental Rights of the EU and the case law of the Court of Justice.

In general terms, the EU Commission and the EU Agencies could adopt regulations or guidelines to establish further rules or usage directives. For instance, the Commission has adopted certain guidelines to regulate the use of generative AI by its staff.

The AI Act also provides the legal basis for the exercise of the new competences attributed to the bodies created to ensure the enforcement of the regulation, particularly the AI Office (established by a Commission decision in January 2024²), the Artificial Intelligence Board, the Advisory Forum, and the Independent Expert Group, as regulated by Articles 64, 65, 66, 67, and 68, respectively.

Lastly, the regulation sets out specific provisions on the sanctions applicable to EU institutions and administrative bodies in the event of breaches of its obligations.

III. Do public authorities rely on algorithmic automation/AI in their daily operations? If yes, to what extent? Which areas are most affected by automation (e.g., security, policing, immigration, transport, tax management, welfare, health and employment services, education, justice, or digital identity)?

European institutions, agencies, and other bodies make extensive use of AI systems.

For example, in the banking sector, the ECB uses AI applications to query supervisory data, incorporating chatbot functionalities for supervisory technologies and methodology. Specifically, in text analysis, Athena translates and analyses the content of supervisory documents, cross-referencing information from other sources (e.g., public media), thus allowing supervisors to deepen their understanding of banks and their risks. Additionally, Heimdall supports experts in processing information to assess the suitability and propriety of members of the management body. Another initiative is related to price-setting and inflation dynamics: by applying web scraping and machine learning, the

² See Commission decision C-2024/1459 establishing the Artificial Intelligence Office.

ECB gathers a vast amount of real-time data on individual product prices, improving the accuracy of its analyses³.

XAIDA is a Horizon 2020-funded project designed to characterise, detect, and attribute extreme events using an innovative data-driven, impact-based approach through new AI technologies. Similarly, SAFERS, also funded under Horizon, is based on an integrated platform that information from multiple sources and processes it using AI algorithms to generate useful insights, such as risk maps, early detection of active fires, and fire propagation predictions, to name but a few⁴.

The EUIPO employs AI-based image recognition technology to search for similar-looking trademarks and designs. By analysing colours, shapes, and textures, eSearch plus delivers more complete and better-ranked results. It also automatically identifies and suggests the likely Vienna codes for trademark images and the likely Locarno classes for design images⁵.

EIOPA has launched several initiatives to upgrade its Business Intelligence and data analytics framework, including collecting and analysing EMIR data via the TRACE system. EIOPA has also implemented a code-sharing platform with NCAs to exchange knowledge and experiences among supervisors (particularly regarding machine learning). It is working alongside the EBA on a Digital Regulatory Reporting (DRR) project to develop a robust solution for continuous reporting framework development, including Data Point Model (DPM) releases, validation rules lifecycle, and XBRL taxonomy packages.

The European Food Safety Authority (EFSA) is developing projects to incorporate AI methods in the evidence management phase of its internal risk assessment process. By 2027, the primary goal is to improve the accessibility and scope of the evidence while strengthening

³<https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html>; <https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/ecb-supervisory-boost-gen-ai/>.

⁴ XAIDA project: AI for the detection and attribution of extreme events: <https://climate-adapt.eea.europa.eu/en/metadata/projects/extreme-events-artificial-intelligence-for-detection-and-attribution>; SAFERS project: structured approaches for forest fire emergencies in resilient societies: <https://climate-adapt.eea.europa.eu/en/metadata/projects/structured-approaches-for-forest-fire-emergencies-in-resilient-societies>.

⁵ eSearch plus (machine learning-image recognition for trademark registration): <https://euiipo.europa.eu/eSearch/>.

the reliability of the risk assessment process through human-centric AI closely integrated with human expertise⁶.

AI is also extensively used in border control. Frontex, for instance, employs numerous applications for various purposes. Currently, the EBCG's border controls heavily rely on border guards. While they are supported by new technologies that automate certain aspects of border control, the automation level remains relatively low, typically requiring human-in-the-loop operators.

Broadly speaking, it is clear that the European administration mainly employs AI for data processing and analytics. The growing availability of large datasets is used to support the initial development of sector-specific plans, strategies, and policies. Data analysis is also a key to carrying out supervisory activities effectively. On the other hand, AI is far less commonly used to make direct individual decisions or determine their content.

When this does occur, EU law requires human involvement (*human in the loop* – HITL⁷) as set out in Article 22 of the General Data Protection Regulation (GDPR) and Article 14 of the Artificial Intelligence Act. This is explicitly stated, for example, in the case of trademark registrations by EUIPO, where an official can review the AI system's automatic result in the light of the parties' arguments; and in eu-LISA's information system, where Frontex must ensure that no errors have occurred when the system automatically denies travel authorisation into EU territory⁸.

⁶ AI for extracting and integrating data obtained through New Approach Methodologies for chemical risk: <https://efsa.onlinelibrary.wiley.com/doi/epdf/10.2903/sp.efsa.2024.EN-8567>; AI in risk assessment: <https://efsa.onlinelibrary.wiley.com/doi/epdf/10.2903/sp.efsa.2022.e200501>

⁷ For a comprehensive analysis on Frontex's use of AI technologies see https://www.frontex.europa.eu/assets/Publications/Research/Frontex_AI_Research_Study_2020_final_report.pdf. The report underlines that many of the governments across Europe and globally (especially the US) have begun to test the use of border gate technology that will enable more *autonomy* for processing the passage of goods and people through BCPs. Machine learning is already being used in border security across the globe, in particular in the gathering and processing of vast quantities of data. Despite already being in operation in several countries, it has yet to become fully optimised.

⁸ See O. Mir, *Algorithms, Automation and Administrative Procedure at EU Level*, in H.C.H. Hofmann, F. Pflücke (eds.), *Governance of Automated Decision-Making and EU Law* (2024), 35 ff.

According to Gartner’s forecasts, however, 70% of States are already using or planning to use generative AI in this sector within the next three years⁹.

IV. What legal requirements - e.g. in terms of privacy, cybersecurity, quality of the datasets, impact assessments, transparency obligations, access to codes, the right to explanations, compulsory human involvement, and the right to obtain a review or remedy - apply to the use of algorithmic automation or AI by public authorities? Are there sector-specific regulations on Automated Administrative Decisions (e.g., public procurement, taxation etc.)?

To answer this question, we must first provide a general overview of the regulation and its associated risk categories. Regulation 2024/1689 establishes different rules depending on the risk level of the AI system. Article 5 sets out the list of prohibited practices. Some of these may concern European administrations, such as real-time remote biometric identification systems in public spaces, emotional AI systems, and social scoring systems. For these types of systems, the regulation sets a general prohibition – with some exceptions specified in Article 5 – meaning that, as a rule, European administrations cannot develop or use such applications.

At the lower end of the risk pyramid are low or minimal-risk systems. In these cases, Union institutions and other bodies may create or use these systems for their purposes, provided they comply with the transparency obligations set out in Article 50. This article states that “Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties unless those systems are available for the public to report a criminal offence”.

⁹ Ministry of Economy and Finance, *AI in public settings: Status and Next Steps*, Economic Focus, February 2024.

This applies, for example, to chatbots and virtual assistants often used by public administrations in their communications with citizens, where users must be informed that they are interacting with a machine and not a human.

However, most of the regulation is dedicated to establishing the circulation regime for high-risk systems, which – as previously mentioned – are identified in Article 6 based on two criteria. Under the first criterion, a system is classified as high-risk if:

(a) the AI system is intended to be used as a safety component of a product, or the AI system itself is a product, covered by the Union harmonisation legislation listed in Annex I; (b) the product whose safety component, pursuant to point (a), is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to placing the product on the market or putting it into service pursuant to the Union harmonisation legislation listed in Annex I.

Both conditions must be met simultaneously, meaning the regulation identifies potentially affected products, but they only fall into the high-risk category only if they require third-party conformity assessment to ensure compliance with the relevant standards. These products include, for example, Directive 2009/48 on the safety of toys, Directive 2014/33 on lifts and safety components for lifts, Regulation 2016/424 on cableway installations, Regulation 2017/745 on medical devices, and others.

To answer our question, we must focus on the second criterion for identifying high-risk AI systems, set out in Annex III of Regulation 2024/1689. This criterion covers several types of AI systems with significant potential impact on various areas of public and private life:

1. Remote biometric identification systems in public spaces, where permitted by law.

2. AI systems as safety components in managing critical infrastructure such as digital networks, road traffic, or utilities such as water, gas, heating, and electricity.

3. AI systems in education and vocational training, particularly those used for determining access, admission, or assignment to institutions.

4. AI in employment and workforce management, including systems used for recruitment, job advertising, application filtering, and candidate evaluation.

5. Access to essential services: AI used by public authorities to assess eligibility for public services (e.g., healthcare, benefits). Among them are AI systems intended for use by public authorities or on their behalf to assess the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services.

6. Law enforcement: AI used by national authorities or by Union institutions, bodies, offices, or agencies to support law enforcement authorities in assessing the risk of a natural person offending or re-offending, provided this is not based solely on the profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680. This also applies to AI systems used to assess personality traits, characteristics, or past criminal behaviour of natural persons or groups.

7. Migration and border control: AI used for assessing risks related to security, migration, or health posed by individuals entering the EU. More specifically, (a) AI systems intended for use by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies as polygraphs or similar tools; (b) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of unlawful migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State.

8. Administration of justice and democratic processes.

Given these categories, it is clear that many tasks linked to European Union administration involve high-risk AI systems, particularly in areas such as law enforcement, border control, employment, and public services. When EU institutions, agencies, or bodies deploy or supply AI systems for these purposes, they must comply with a series of requirements.

These obligations apply both to providers (Articles 9-15) and deployers (Articles 26, 27, 86).

However, the use of AI in these sectors does not automatically classify the system as high-risk. The EU legislator has introduced exceptions where a system does not play a determinative role in decision-making and thus does not pose a “significant risk of harm to the health, safety, or fundamental rights of natural persons” (Article 6(3)).

An AI system may be exempted from high-risk classification if:

- it performs a narrow procedural task
- it improves a result previously determined by human activity

- it detects patterns or deviations but does not influence the final decision without proper human review
- it performs a preparatory task related to the use cases listed in Annex III.

Despite these exemptions, an AI system in Annex III will always be classified as high-risk if it involves profiling individuals.

The distinction between a system that influences a decision and one that plays a limited procedural role is not always easy to establish. This distinction is particularly important in determining whether a system must comply with the more stringent requirements of the regulation.

The European Commission is expected to issue guidelines by February 2025 to clarify these case studies and assist with the practical interpretation of the provisions. These guidelines will be crucial in helping stakeholders understand when a system should be classified as high-risk, particularly when its influence on decision-making is ambiguous.

When European authorities develop an AI system themselves, several obligations arise under Regulation 2024/1689. These obligations, primarily aimed at providers of high-risk AI systems, also apply to the authorities in their role as developers.

Here is an outline of the main requirements:

1. Risk Management System (Article 9): providers must establish a risk management system to ensure the continuous identification, evaluation, and mitigation of risks associated with the AI system. This system must account for risks related to individuals' safety, health, and fundamental rights throughout the AI system's lifecycle.

2. Retention of Logs (Article 12): the regulation requires providers to ensure that logs relating to the operation of the AI system are retained to enable continuous monitoring and review. These logs are essential for tracing decisions and identifying malfunctions or potential biases.

3. Technical Documentation (Article 11): providers are required to maintain detailed technical documentation of the AI system. This documentation must include information on the system's design, development, and performance, ensuring that the system can be assessed for compliance with the regulation's requirements.

4. Accuracy, Robustness, and Cybersecurity (Article 15): the system must be designed to achieve an appropriate level of accuracy, robustness, and cybersecurity, ensuring its consistent performance

throughout its lifecycle. These requirements address the resilience of the system against potential cyber threats and the reliability of its outputs.

5. Data Governance (Article 10). Perhaps one of the most critical sets of obligations relates to data management. Providers must implement a data governance system to ensure the relevance of training, validation, and testing data; they will be “sufficiently representative”, free from errors, and as complete as possible for the AI system’s intended purpose. The regulation acknowledges the technological limitations in ensuring perfect data, hence the phrasing “to the best extent possible.” Still, the system must be designed to minimise bias and ensure that data is of high quality, following the principle of “trash in, trash out” – i.e., good data is essential for generating good results¹⁰. Art. 10, para. 3, establishes specifically that “training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof”.

In addition to ensuring data relevance and representativeness, the deployer must also exercise control over input data, ensuring its appropriateness for the AI system’s intended use (art. 26 Reg.). This reflects the dual responsibility of both providers and deployers in safeguarding the quality and accuracy of data¹¹.

¹⁰ J.V. Fernandez, *Artificial Intelligence in Government: Risks and Challenges of Algorithmic Governance in the Administrative State*, 1 Ind. J. Global Legal Stud. 65 (2023); K. Glaze, D. E. Ho, G.K. Ray, C. Tsang, *Artificial Intelligence for Adjudication: The Social Security Administration and AI Governance*, in J. Bullock et al. (eds.), *The Oxford Handbook of AI Governance*; A. Rachovitsa, N. Johann, *The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons learned from the Dutch SyRI Case*, 22 Hum. Rts. L. Rev (2022) 1; C. Coglianese, *A Framework for Governmental Use of Machine Learning*, available for download at <https://www.acus.gov/sites/default/files/documents/Coglianese%20ACUS%20Final%20Report%20w%20Cover%20Page.pdf>.

¹¹ On this, see B. Marchetti, *Artificial Intelligence and Public Authorities: Does the European AI Act Protect Public Values*, 36 ERPL/REDP 67 (2024); O. Mir, *The AI Act from the Perspective of Administrative Law: Much Ado About Nothing?*, 16 Eur. J. Risk Regul. 63 (2024); C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell’Unione europea in materia di intelligenza artificiale*, 3 Biolaw Journal 415 (2021); F. Donati, *Diritti fondamentali e algoritmi nella proposta di regolamento sull’intelligenza artificiale*, in 3-4 Il Diritto dell’Unione europea 453 (2021); C. Novelli, F. Casolari-A.

Art. 10 para. 5 regulates the use of personal data, permitting the processing of special categories of personal data (e.g., data on race, health, or political opinions) under exceptional circumstances, “when necessary to detect and correct biases, providers may process special categories of personal data, subject to strict safeguards”.

This can only occur if bias correction cannot be achieved by processing other data, such as synthetic or anonymised data. In any case, the data must be protected by state-of-the-art security measures, such as pseudonymisation and strict access controls, and personal data must be deleted once bias correction is complete, or after the retention period expires.

Lastly, records of the data processing activities must include justifications for why processing special categories of personal data was necessary.

Article 13 of the EU Regulation focuses on the need for transparency in high-risk artificial intelligence systems. This article mandates that providers must ensure these systems are designed and developed in such a way that their operations are sufficiently transparent. This transparency is essential for deployers—those who ultimately use the systems—so they can understand and appropriately interpret the system's outputs.

According to this regulation, high-risk AI systems must come with clear instructions for use, which should be available in digital format or another accessible form. These instructions should be concise, complete, correct, and accurately reflect how the system works. They must be clear, i.e. easy to understand, even for users who may not have advanced technical knowledge. They must provide relevant details that will enable proper interpretation of the system's outputs and guidance on how to use the system as intended.

Furthermore, Article 13 highlights the importance of making the operational logic of the system transparent so that the deployer should be able to understand how the system arrives at its conclusions or decisions. By having a clear grasp of the system's workings, the deployer can take the necessary technical and organisational measures to use the system in accordance with the provided instructions.

In conjunction with this, Article 26 para. 1, outlines the responsibilities of the deployer, stating that they must take active steps to ensure that the system is used in line with the instructions provided.

Rotolo-M. Taddeo-L. Floridi, *AI Risk Assessment: A Scenario-based Proportional Methodology for the AI Act*, 3 *Digital Society* (2024).

This includes ongoing monitoring of the system's performance to guarantee that it is being used correctly and in compliance with the guidelines.

In summary, the regulation emphasises the provider's duty to ensure transparency in AI systems, allowing deployers to use these systems responsibly by providing clear, complete, and easily accessible information. This approach seeks to minimise risks linked to the improper or uninformed use of AI technologies.

The provision takes into account the impossibility of ensuring the explainability of machine learning algorithms due to the so-called *black box* phenomenon, which, as is well known, prevents explaining the reasons why, given certain inputs, the machine produces specific outputs. This represents one of the main obstacles to the admissibility of using machine learning algorithms for decision-making purposes in the public sphere. The opacity of how these systems operate makes it impossible to justify decisions, as this is understood within national laws and the jurisprudence of the Court of Justice.

This lack of transparency raises significant concerns regarding accountability and the right to understand the rationale behind decisions that may affect individuals' lives¹².

Consequently, there is a pressing need for regulations that not only recognise these challenges but also promote mechanisms to enhance the transparency and interpretability of AI systems, ensuring that they can be integrated into public decision-making processes in a manner that upholds democratic values and respects fundamental rights.

The last fundamental requirement for the marketing of a high-risk system is established in Article 14, titled "Human oversight".

¹² C. Coglianese, D. Lehr, *Transparency and Algorithmic Governance*, 71 Admin. L. Rev. 1 (2019); H. Palmer Olsen, J. Livingston Slosser, T. Troels Hildebrandt, *What's in the box?*, in H. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio, *Constitutional Challenges in the Algorithmic Society* (2022); in the same book, F. Pasquale, *Inalienable due process in an Age of AI: limiting the contractual creep toward automated adjudication*, 42; D. Freeman Engstrom, D.E. Ho, C. M. Sharkey, M.-F. Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*, available at <https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf>; P. Hacker, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination Under EU Law*, in 55 CMLR 1143 (2018); B. Casey, A. Farhangi, R. Vogl, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, in 34 Berkeley Tech. L. J. 143 (2019); S. Watcher et al., *Why a Right to explanation of Automated Decisionmaking Does Not Exist in the General Data Protection Regulation*, 7 Int'l Data Privacy L. 76 (2017).

This provision is crucial in preventing the dehumanisation of many decision-making processes, which would be inevitable if there were a complete delegation to machines. The underlying idea is that high-risk systems, intended to operate in sensitive contexts for the protection of fundamental rights, “shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use”.

The oversight measures must be proportionate to the risks, level of autonomy, and context of use of the high-risk AI system. These measures can be incorporated into the high-risk AI system itself, if technically feasible, or they can be implemented by the deployer. Specifically, the individual tasked with overseeing the system must be able to properly understand the relevant capacities and limitations of the high-risk AI system and monitor its operation, including detecting and addressing anomalies, dysfunctions, and unexpected performance. They must remain aware of the potential tendency to rely excessively on the output produced by the high-risk AI system (known as *automation bias*), especially in systems used to provide information or recommendations for decisions made by humans. They should also be able to correctly interpret the output of the high-risk AI system, and, in any specific situation, decide not to use the high-risk AI system or to disregard, override, or reverse its output. Furthermore, they should intervene in the operation of the high-risk AI system or stop it using a ‘stop’ button.

Among the requirements for high-risk systems, this one probably poses the most critical challenge to overcome¹³. Not only because, as Garapon and Lassegue have noted, there is the *Moutonnier effect*¹⁴ (or anchoring effect), referring to the natural tendency to trust machines too much, as demonstrated by numerous behavioural psychology experiments, but also because the ability to supervise such systems requires a level of competence (AI literacy) that is not easily found within public administrations. Personnel are often better trained in legal and economic fields than in technology or computer science.

¹³ B. Wagner, *Liabile, but Not in Control? Ensuring Meaningful Human Agency in Automated Decision-Making Systems*, in 11 *Policy and Internet* 104 (2019); C. Langer, *Decision-making power and responsibility in an automated administration*, <https://link.springer.com/article/10.1007/s44163-024-00152-1>; B. Marchetti, *La garanzia dello human in the loop alla prova della decisione amministrativa algoritmica*, in 2 *Biolaw Journal* 367 (2021).

¹⁴ A. Garapon, J. Lassègue, *Justice digitale* (2018).

Beyond competence, the practical implementation of human oversight also depends on how the responsibility and liability of human decision-makers are regulated in two scenarios: firstly, if they disregard the outputs produced by the system during human oversight, leading to a harmful event; and secondly, if they follow the system's recommendation, leading to negative consequences.

This raises significant questions about the nature of responsibility and the implications of relying on AI-generated outputs in sensitive areas.

The regulation establishes two additional obligations for deployers, which are particularly relevant to public authorities in terms of guarantees. The first concerns the assessment of the impact on fundamental rights, required only for deployers that are bodies governed by public law, or private entities providing public services.

For this purpose, the deployers are required to conduct an assessment that involves identifying any potential risks to fundamental rights that may arise from the AI system's deployment, evaluating its impact on the protection of fundamental rights – particularly in relation to privacy, non-discrimination, and equal treatment – and mitigating those risks by implementing measures to prevent, reduce, or eliminate harmful effects on fundamental rights.

This obligation aims to ensure that any public or essential service using high-risk AI systems does so with a clear understanding of the implications for citizens' fundamental rights, thereby promoting transparency and accountability.

More specifically, deployers are required to perform an assessment consisting of: (a) a description of the processes in which the high-risk AI system will be used in line with its intended purpose; (b) a description of the period of time and frequency within which each high-risk AI system is intended to be used; (c) the categories of natural persons and groups likely to be affected by its use in the specific context; (d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information supplied by the provider under Article 13; (e) a description of the implementation of human oversight measures in accordance with the instructions for use; (f) the measures to be taken in the event of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms (Article 27, para. 1).

Once the assessment referred to in paragraph 1 of the article has been performed, the deployer must notify the market surveillance

authority (the European Data Protection Authority) of its results, submitting the duly compiled template referred to in paragraph 5 as part of the notification (Article 27 para. 3).

Lastly, it is important to focus on Article 86 of the Regulation, which establishes the right to explanation of individual decision-making. It provides that:

“Any affected person subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken”.

The regulation is important because it aims to reconcile the use of AI with the need to ensure the right to an explanation in individual decisions that are harmful or have an unfavourable impact on the recipient. This guarantee differs from the traditional requirement for justification as outlined in Article 41 of the Charter of Fundamental Rights of the EU. In the case of machine learning algorithms, it is impossible to express the specific reasons behind a decision, as normally required, but the regulation seeks to uphold the rule of law by offering an *alternative safeguard*.

Understanding how the inputs generated by a machine influence the decision-making process and the main elements of the decision is a crucial step in determining whether, and to what extent, the outcome of the algorithmic process may have harmed a recipient's rights. While this mechanism approximates the concept of justifying decisions, particularly for public administrations, its application extends beyond the public sector. It applies to any entity, including private ones, responsible for performing one of the tasks listed in Annex III (with the exception of critical infrastructure, where individual impact is unlikely). This includes public and private employers, universities and schools, and both public and private providers of essential services. Thus, this safeguard is not limited to public administrative bodies but also affects private entities in scenarios where AI plays a role in high-risk decision-making processes.

In the AI Act, there is no specific remedy to contest a decision made using an algorithm or based on outputs from an AI system. It

primarily provides citizens the right to file a complaint with a market surveillance authority. Article 85 of the regulation states that: “Without prejudice to other administrative or judicial remedies, any natural or legal person having grounds to consider that there has been an infringement of the provisions of this Regulation may submit complaints to the relevant market surveillance authority”.

In line with Regulation (EU) 2019/1020, such complaints are considered when conducting market surveillance activities and are handled in accordance with the established procedures of the market surveillance authorities.

However, this does not mean that decisions influenced by AI or made by an algorithm cannot be challenged in court under Article 263 of the Treaty on the Functioning of the European Union (TFEU) before the Court of Justice of the EU (CJEU). It is clear that the use of AI by EU institutions and bodies does not limit the right to judicial review as outlined in Article 47 of the Charter of Fundamental Rights of the EU, under the conditions set forth in Article 263.

In fact, the CJEU has dealt with a case involving an error caused by an automated decision, establishing that any such decision “must be subject to an individual reexamination by non-automatic means before an individual measure adversely affecting the persons concerned is adopted” (Case C-511/18, *La Quadrature du Net*, para. 182). This ensures that even when AI is involved, decisions affecting individuals must still undergo human review to ensure fairness and accountability (see hypothetical case n. 3.1).

Judicial control of algorithmic decisions poses different challenges depending on the algorithm used: model-based AI is less problematic than machine learning AI, as the first offers a certain degree of explainability, whereas ML algorithms are inexplicable due to the “black box” problem and carry the risk of errors, discrimination, and restricted access to justice.

V. Who builds the algorithmic technologies used by public authorities? Are these developed by public entities, private companies, or a hybrid body?

There is limited data on the use of AI by EU public institutions¹⁵, but what is clear is that the system is a mixed one. For instance, regarding

¹⁵ O. Mir, cit. at 8., 70, says that “the information available online or in previous publications is very scarce and fragmentary”. On this argument see *Buying AI. Is the*

the use of generative AI by public officials, the European Commission has established strict rules¹⁶, and the Joint Research Centre (JRC) has developed specialised AI systems for use by Commission staff, mainly to ensure data protection.

In general, the JRC provides scientific and technical support for EU policies on AI, e.g. the AI Act, and assists in sectoral applications such as transport, healthcare, education, and science. However, the majority of AI applications used by EU institutions are acquired externally through a public procurement process.

Regarding AI procurement, on October 5, 2023, the European Commission published the EU model contractual clauses for artificial intelligence (AI) systems for public organisations intending to procure AI solutions from external suppliers¹⁷. These model clauses were developed by the AI procurement community and peer-reviewed by experts, outlining responsibilities related to the ethical, transparent, and accountable development of AI technologies between suppliers and public entities.

The model AI clauses specifically address the requirements set by the AI Act but do not cover other obligations arising from relevant legislation, such as the GDPR. The clauses differentiate between high-risk AI and non-high-risk AI systems. For high-risk AI, the clauses follow the mandatory obligations from the AI Act, whereas these obligations are not mandatory for non-high-risk AI but are recommended to enhance trustworthiness when procuring AI systems.

Another important means of acquiring AI systems is through funding from the European Commission for projects developed by consortia of research institutions, universities, and both private and public entities, particularly under the Horizon 2020 programme. Examples include projects managed by organisations such as the European Space Agency (ESA) and the EFSA¹⁸.

Public sector equipped to procure technology in the public interest?, Discussion paper, Ada Lovelace Institute, September 2024.

¹⁶ https://www.asktheeu.org/en/request/13063/response/45877/attach/3/guidelines%20on%20the%20use%20of%20online%20generative%20artificial%20intelligence%20tools.pdf?cookie_passthrough=1.

¹⁷ https://public-buyers-community.ec.europa.eu/system/files/2023-10/AI_Procurement_Clauses_template_High_Risk%20EN.pdf; https://public-buyerscommunity.ec.europa.eu/system/files/2023-10/AI_Procurement_Clauses_template_High_Risk%20EN.pdf.

¹⁸ D. Freeman Engstrom, D.E. Ho, C. M. Sharkey, M.-F. Cuéllar, *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*, which can be

VI. Is there a centralised infrastructure for digital data management, or are there several infrastructures? If the latter is true, is interoperability guaranteed, and to what extent? Are there any rules or procedures governing the exchange of information between different administrative bodies?

The European Union has entrusted the European Data Protection Supervisor (EDPS) with the role of notifying authority and post-market surveillance for the introduction and use of AI systems within EU institutions. This choice is justifiable for two principal reasons.

The first concerns the independence of the EDPS, an independent authority, in accordance with the requirements of Article 70 of the AI Act, which establishes that “Each Member State shall establish or designate as national competent authorities at least one notifying authority and at least one market surveillance authority for the purposes of this Regulation. Those national competent authorities shall exercise their powers independently, impartially and without bias so as to safeguard the objectivity of their activities and tasks, and to ensure the application and implementation of this Regulation”.

It is essential for the authority overseeing compliance with the regulations to remain independent of the entities it supervises. Given that EU institutions and agencies also use AI to perform their tasks, it is

downloaded at <https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf>, according to which, “building internal capacity, rather than simply embracing a default practice of contracting out for technical capacity, will be crucial to realizing algorithmic governance’s promise and avoiding its perils”. In the United States, about half of federal agencies (45%, or 64 out of 157) use AI systems for various tasks, including regulatory analysis and monitoring (e.g., the Food and Drug Administration), enforcement activities (such as the Securities and Exchange Commission and Customs and Border Protection), the management of public services, organisational functions, and adjudication, particularly in standardised procedures (like those handled by the Social Security Administration and the US Patent and Trademark Office).

One key difference in the U.S. system is that a significant portion of AI systems (84 out of 157) are developed internally by these agencies. However, budget constraints can sometimes hinder or limit the development of AI systems. In such cases, in addition to contracting out the development to external providers, agencies have the option to ‘borrow’ AI technologies. This involves collaborating with non-commercial entities or other government administrations to gain access to the necessary AI tools and expertise. This in-house development and flexibility in collaboration demonstrate a more self-sufficient and cooperative approach to AI technology in the public sector, allowing federal agencies to overcome financial limitations while maintaining access to advanced AI solutions. See L. Parona, “*Government by Algorithm*”: un contributo allo studio del ricorso all’IA nell’esercizio di funzioni amministrative. *Spunti per una regolazione più consapevole*, 1 *Giornale di Diritto Amministrativo* 10 (2021).

essential to have an external, impartial body monitoring compliance with the prohibitions and requirements set forth by the AI regulation.

The second reason is related to the strong link between data and AI. There is a close relationship between data (and its legal framework) and artificial intelligence. AI systems rely heavily on large, solid, complete, and representative datasets. The development of AI algorithms requires vast amounts of data, much of which is held by European administrations and is a result of data-sharing and cooperation across various sectors of EU law. Ensuring that AI systems can access the necessary data while remaining compliant with data protection regulations makes the EDPS a natural choice for this supervisory role.

Data interoperability across the EU is ensured by Regulation 2024/903, which establishes high-level public sector interoperability measures (Interoperable Europe Act). Furthermore, in December 2023, the European Commission awarded a €41 million contract to develop infrastructure for Common European Data Spaces. This project selected a consortium to create *Simpl*, a secure middleware platform aimed at facilitating data access and interoperability across European data spaces, thereby unlocking the potential for data-driven innovation. Again, in February 2024, the EU Commission adopted the implementing act for a data-sharing platform between Member States and the Commission. This platform will serve as the foundation for the supervision, investigation, enforcement, and monitoring of services covered by the Digital Services Act (DSA). This initiative highlights the growing focus on data interoperability and secure data-sharing as essential elements for the functioning of AI and digital services across the EU.