ACA-Europe Seminar

Catania, 23-24 November 2026

Technological challenges, with particular focus on the introduction of digital technologies and artificial intelligence into the organisation of public administration and administrative justice

GENERAL REPORT
by
the Italian Council of State

Co-funded by
the European Union

Index

Session 1 - The Digitalisation of Administrative Justice: Infrastructure, Digital Court Proceedings, Cybersecurity, AI and Future Perspectives 4

1.1 The Level of Digital Maturity of Supreme Administrative Jurisdictions: Infrastructure, Equipment and Technological Organisation 4

Digital equipment and operational maturity – 4

Technological infrastructure, business continuity and remote working – 4

National and cross-border interoperability – 6

1.2 The Dematerialisation of Administrative Judicial Proceedings: State of Implementation, Digital Services and Accessibility 7

Dematerialisation of proceedings and management of digital documents – 7

Digital services for citizens, legal professionals and public administrations – 9

Accessibility, digital inclusion and involvement of legal professionals – 9

1.3 Cybersecurity, Data Protection and Publication of Judicial Decisions 10

Compliance, System Security, Management of cyber incidents and business continuity – 11

Online publication of judicial decisions and protection of personal data – 12

Publication, privacy and the governance of judicial data – 13

1.4 Governance of Digital Transformation, Use of Artificial Intelligence and Future Perspectives 14

Digital training and the involvement of judges in technological innovation – 15

AI tools and level of deployment – 15

Governance safeguards applied to the use of AI – 17

Risk assessment, human oversight and traceability – 17

Ongoing digital innovation projects, obstacles, investment priorities and transferable best practices – 17

Session 2 - Automated Administrative Decisions and Judicial Review by Administrative Courts 19

2.1 Legal basis of instruments enabling the use of digital technologies or AI in administrative acts 19

Sector-specific legislation and legislation generally applicable to any type of administrative procedure - 19

General principles derived from the legal system or referred to in sector-specific provisions, applicable to automated administrative acts – 25

Co-funded by the European Union

Sectors in which the use of digital technologies or AI tools for the adoption of administrative acts is subject to prior authorisation or is frequently excluded - . 26

2.2 Access to, transparency of and challenges to administrative decisions involving the use of digital technology or AI systems 28

The possibility of exercising the right of access to ascertain how digital technology or an AI tool has influenced the administrative decision and whether it has functioned correctly - 28

Possibility of challenging the use of digital technologies or AI tools by a public administration - 30

2.3 Automated administrative acts based on the use of digital technology or AI tools: an analysis of the case law 30

Criteria for assessing the lawfulness of automated administrative decisions and principles that must be upheld - 30

Limits of the judicial review that the competent court may exercise over automated administrative acts - 34

Access to the algorithm, or other AI tools, and judicial protection: scope and limits - 34

Session 3 The Administrative Judge and the Use of Artificial Intelligence 35

3.1 National Legislation and Implementation of Regulation (EU) 2024/1689 35

Constitutional principles and national legislation on judicial process automation - 35

Different approaches to the implementation of Regulation (EU) 2024/1689 – .. 35

3.2 Use Cases and Ongoing Pilot Projects 37

AI use cases supporting judicial functions – 37

Ongoing pilot projects – 38

The use of generative AI – 38

3.3 Safeguards Governing the Use of AI 38

Guarantee of human oversight – 39

Mitigating automation bias and judicial training – 40

This report has been prepared in compliance with 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC' (General Data Protection Regulation - GDPR).

Co-funded by the European Union

Session 1 - The Digitalisation of Administrative Justice: Infrastructure, Digital Court Proceedings, Cybersecurity, AI and Future Perspectives

1.1 The Level of Digital Maturity of Supreme Administrative Jurisdictions: Infrastructure, Equipment and Technological Organisation

The questionnaire responses show that the digital maturity of supreme administrative jurisdictions cannot be assessed on the basis of a single indicator. Individual digital equipment, technological infrastructure, cloud deployment, remote working, interoperability and business continuity represent distinct dimensions of digital transformation, which do not necessarily evolve in parallel. A court may have advanced technological tools while operating within a judicial system that remains fragmented or partially paper-based. In other cases, digitalisation serves as a means of strengthening institutional resilience.

Digital equipment and operational maturity – A first common finding is the gradual convergence in the digital tools and equipment available to judges and court staff. In most participating jurisdictions, judges and administrative staff have access to computers, institutional email accounts, legal databases, videoconferencing facilities, secure authentication systems and, in many cases, VPN access, digital signatures and collaborative tools. This convergence is particularly evident in jurisdictions displaying a high level of digital maturity, including **Denmark**, **Estonia**, **Finland**, **Italy**, **Norway**, **Portugal**, **Sweden** and **Türkiye**.
The availability of advanced digital equipment does not, however, necessarily correspond to full operational maturity.
The questionnaire responses reveal a varied picture. **Albania** and **Cyprus**, for example, report adequate digital equipment or infrastructure, but administrative proceedings have not yet been dematerialised. **Lithuania** reports having a relatively adequate technological infrastructure, while identifying a need to update its technological solutions relating to security. **Poland** has technologically advanced digital services and access platforms, although the dematerialisation of administrative proceedings remains at an intermediate stage. It also reports limitations in interoperability with other judicial information systems and with the applications used by public administrations. **Austria**, where most of the eleven first-instance administrative courts and the Supreme Administrative Court use different case-management systems, shows that even a highly digitalised court may operate within a system that is not fully integrated across the different levels of the administrative court system. Digital maturity should therefore be assessed not only within each individual court, but also in terms of the capacity of the system as a whole to function as a coherent digital system.

Technological infrastructure, business continuity and remote working – The responses reveal a variety of models that cannot be reduced to a simple hierarchy between cloud-based and on-premises solutions. It is necessary to distinguish, on the one hand, the extent of cloud deployment and, on the other, the governance model adopted for the underlying infrastructure.

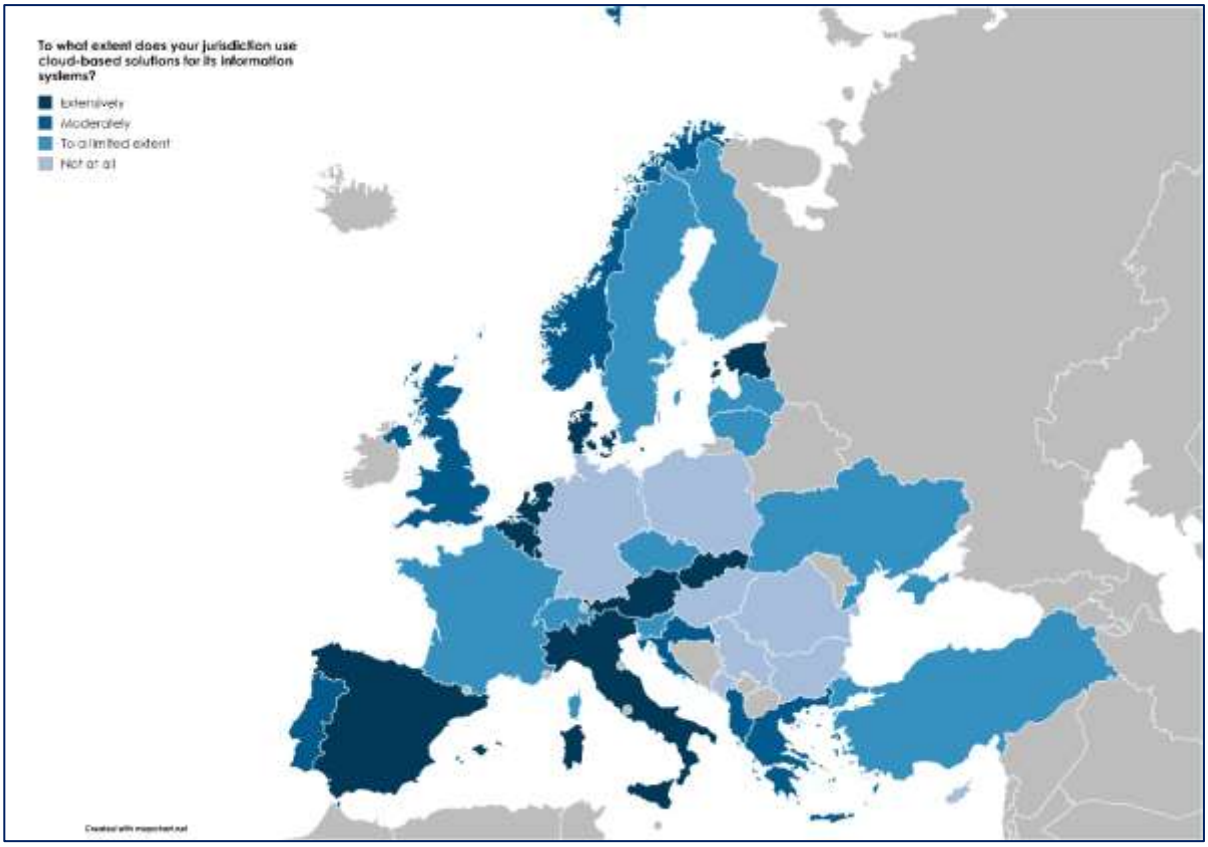


Figure 1 – Intensity of cloud use

A first group comprises **Austria**, **Belgium**, **Denmark**, **Estonia**, **Italy**, **Luxembourg**, **the Netherlands** and **Spain**, all of which report extensive use of cloud technologies, albeit through different approaches ranging from collaborative and office productivity services to components of case management systems or the digital judicial environment. **Italy** and **Luxembourg** illustrate two significant variants of this model: in Italy, a redundant cloud infrastructure integrated with digital judicial proceedings; in Luxembourg, reliance on State-owned rather than commercial servers.

A second group includes jurisdictions in which cloud deployment remains moderate or is confined to specific components of the digital environment. **Albania**, **Croatia**, **Greece**, **Portugal**, **Slovakia** and **the United Kingdom** use cloud services for collaborative tools, digital services or application components, while retaining national servers, public data centres, physical infrastructure or central judicial systems that have not been fully migrated to the cloud. **The United Kingdom** also illustrates significant fragmentation across its different judicial systems, whereas **Slovakia** continues to host its principal judicial systems within the Court's internal infrastructure.

A third group retains the core judicial infrastructure within internal, on-premises, national or otherwise closely controlled environments, using cloud services only to a limited extent or for non-core functions. **The Czech Republic**, **Finland**, **France**, **Latvia**, **Lithuania**, **Norway**, **Slovenia**, **Sweden**, **Türkiye** and **Ukraine** fall, to varying degrees, within this cautious model. Finally, **Bulgaria**, **Cyprus**, **Germany**,

Montenegro, **Poland**, **Romania** and **Serbia** report either no use or only negligible use of cloud technologies, relying instead on their own or publicly operated data centres. **Germany** demonstrates particularly clearly that the absence of cloud deployment is compatible with a high level of digital maturity in judicial proceedings, an issue that will be revisited in the section on dematerialisation. **France** notes that discussions are under way at national level on the possible use of external cloud services, highlighting the complexity of the decision and the need to balance performance, security and sovereignty.

Cloud deployment should therefore not be regarded as an autonomous indicator of digital maturity. The decisive considerations are which components of the judicial system are hosted in the cloud, where procedural data are stored, who exercises governance over the infrastructure, and which safeguards ensure security, operational resilience and the institutional independence of the judicial function. From this perspective, particular significance attaches both to models based on public, State-owned or government-operated infrastructures, as in **Albania**, **Bulgaria**, **Croatia**, **Greece**, **Luxembourg**, **Türkiye** and **Ukraine**, and to models emphasising digital sovereignty, data localisation and institutional control, as illustrated by **France** and **Switzerland**.

Remote working has now become an established feature in many judicial systems, primarily through the use of institutional devices, VPN access, strong authentication mechanisms and secure access to internal applications. In other jurisdictions, it remains possible but is constrained by technical, organisational or security-related factors, as illustrated, for different reasons, by **Albania**, **Croatia** and **Ukraine**.

Business continuity constitutes a further indicator of digital maturity, as it reflects the capacity to combine digital infrastructure, cybersecurity, redundancy, disaster recovery arrangements and user support within a coherent framework.

National and cross-border interoperability – The third, and probably the most critical, dimension concerns interoperability. Many judicial systems display a high degree of internal digital development but remain insufficiently interoperable with other courts, public authorities, national registers or cross-border systems.
At national level, **Estonia** and **Italy** demonstrate significant integration with the wider public digital ecosystem and national digital platforms. **Bulgaria**, **Croatia**, **Hungary**, **Latvia** and **Türkiye** likewise report connections with public registers, administrative platforms or central public digital infrastructures.

In other jurisdictions, however, interoperability remains limited or entirely absent. **France** has a common technical environment shared by all administrative courts and a secure network infrastructure extending to the overseas territories. However, it reports that the IT applications used by the administrative courts do not interoperate with those of other national or international judicial systems. **Austria**, **Belgium** and **Poland** have achieved a high level of internal digitalisation, while reporting limitations in their integration with other systems. **Romania**, the **Czech Republic**, **Serbia** and **Montenegro** likewise show, to varying degrees, an absence of full interoperability, in a context of less developed digital infrastructure, where the dematerialisation of administrative proceedings is still at an early stage or has not yet begun. In **Romania**,

for example, "the specific information system used by judicial bodies enables communication between them for the transmission of case files", despite the absence of dematerialisation of administrative proceedings.

Cross-border interoperability remains even more limited. The independent development of national platforms, differences in technological architectures, the absence of sufficiently widespread common standards and the diversity of institutional governance models for judicial IT systems continue to prevent full procedural interoperability. Against this background, the European Case Law Identifier (ECLI) remains the principal common European standard, widely implemented across most participating jurisdictions and important for the uniform identification of judicial decisions.

In conclusion, the digital maturity of supreme administrative jurisdictions should be understood as a multidimensional phenomenon. It cannot be equated with the mere availability of digital equipment, the use of cloud technologies or the existence of online portals. Rather, it depends on the capacity of the technological infrastructure to support the entire judicial process in a secure, resilient and interoperable manner. The common finding is not the emergence of a single European model of digital justice, but the coexistence of different models in which technology, security and institutional organisation are combined according to different institutional, organisational and operational balances.

1.2 The Dematerialisation of Administrative Judicial Proceedings: State of Implementation, Digital Services and Accessibility

The dematerialisation of administrative judicial proceedings constitutes a distinct dimension from infrastructural maturity. A jurisdiction may possess advanced digital infrastructure, secure infrastructure or sophisticated online services without the digital case file having become the ordinary working environment for the conduct of judicial proceedings. The decisive criterion is not the mere existence of online portals, case-law databases or electronic notifications, but the role that digital technology plays throughout the entire procedural cycle: the filing of procedural documents, the creation and consultation of the case file, the conduct of proceedings, judicial decision-making, communication, archiving and the reuse of procedural data.

Dematerialisation of proceedings and management of digital documents – A first group comprises jurisdictions in which administrative judicial proceedings are fully or substantially dematerialised. **Denmark**, **Estonia**, **Finland**, **Germany**, **Italy**, **Norway**, **Portugal**, **Sweden** and **Türkiye** operate systems in which the digital case file and electronic communications constitute the ordinary working environment for judicial activity. In **Italy**, the Electronic Administrative Judicial Proceedings system (Processo Amministrativo Telematico – PAT), integrated within the Administrative Judicial Information System (SIGA), covers the entire procedural lifecycle. In **Finland**, judicial workflows have been fully electronic since 2020, while in **Portugal** the CITIUS platform constitutes the central infrastructure for digital judicial proceedings. **Germany** confirms that full dematerialisation is compatible with a non-cloud-based infrastructure.

Effective dematerialisation depends not solely on technological architecture but on the central role assigned to the digital case file. The common feature of these systems is that digital technology no longer functions as a mere electronic replica of paper documentation but as the ordinary environment for the judicial function.

A second group comprises jurisdictions that are digitally advanced but have not yet fully integrated digital processes across the entire procedural chain. **Austria**, **Belgium**, **Bulgaria**, **France**, **Greece**, **Lithuania**, **the Netherlands**, **Ukraine** and **the United Kingdom** have developed sophisticated digital platforms offering electronic filing, digital access to case files and electronic notifications. However, dematerialisation does not yet extend uniformly to every procedural stage or every level of the administrative judiciary. **Austria** illustrates the possible divergence between the high level of digital maturity achieved by the supreme administrative court and the uneven integration of first-instance courts. **Belgium** operates an advanced electronic procedure through the eProAdmin platform, although without full external interoperability.

It should be noted, however, that the persistence of aspects not fully paperless may be attributable to different factors. In **Bulgaria**, although the dematerialisation of proceedings is reported to be at an advanced stage and the information systems are capable of creating, storing and exchanging documents in digital format, judges and court staff do not yet, in their day-to-day work, process and sign documents exclusively in digital format. In this regard, the questionnaire reports that an update to the system is under way, which is intended to enable the electronic signing of documents in the near future. In **France**, proceedings initiated by applications lodged electronically are conducted entirely in digital format. However, the use of digital tools remains optional for individuals who are not represented by a lawyer. In addition, final judicial decisions and certain documents formally concluding proceedings continue to be signed on paper to ensure their authenticity.

A third group consists of hybrid or dual-track systems in which digital and paper case files continue to coexist. **Croatia**, **Hungary**, **Latvia**, **Poland**, **Slovakia**, **Slovenia**, **Spain** and **Switzerland** display different forms of coexistence between electronic procedures and physical documentation. In **Croatia**, systems such as eSpis, e-Communication and e-Građani enable digital case registration and the electronic exchange of documents, while physical case files remain in use. In **Switzerland**, the Justitia 4.0 programme reflects a structured transition towards a more mature system of electronic judicial communication.

A fourth group comprises jurisdictions in which digital services and secure infrastructure are available but judicial proceedings have not yet been fully dematerialised. **Cyprus**, the **Czech Republic**, **Luxembourg** and **Romania** fall within this category. In **Romania**, the Electronic File system and the TDS platform have improved access to proceedings and judicial communications, yet the paper case file remains the primary procedural record. In the **Czech Republic**, the case-law database is highly developed, although the digital case file has not yet reached full maturity. **Luxembourg** benefits from a secure State-operated infrastructure and has planned a gradual transition towards fully digital judicial proceedings, while **Cyprus**

reports advanced digital equipment but has not yet implemented a fully dematerialised administrative procedure. **Albania**, **Montenegro** and **Serbia** remain among the jurisdictions where proceedings continue to be predominantly paper-based or are only at an initial stage of digital transition.

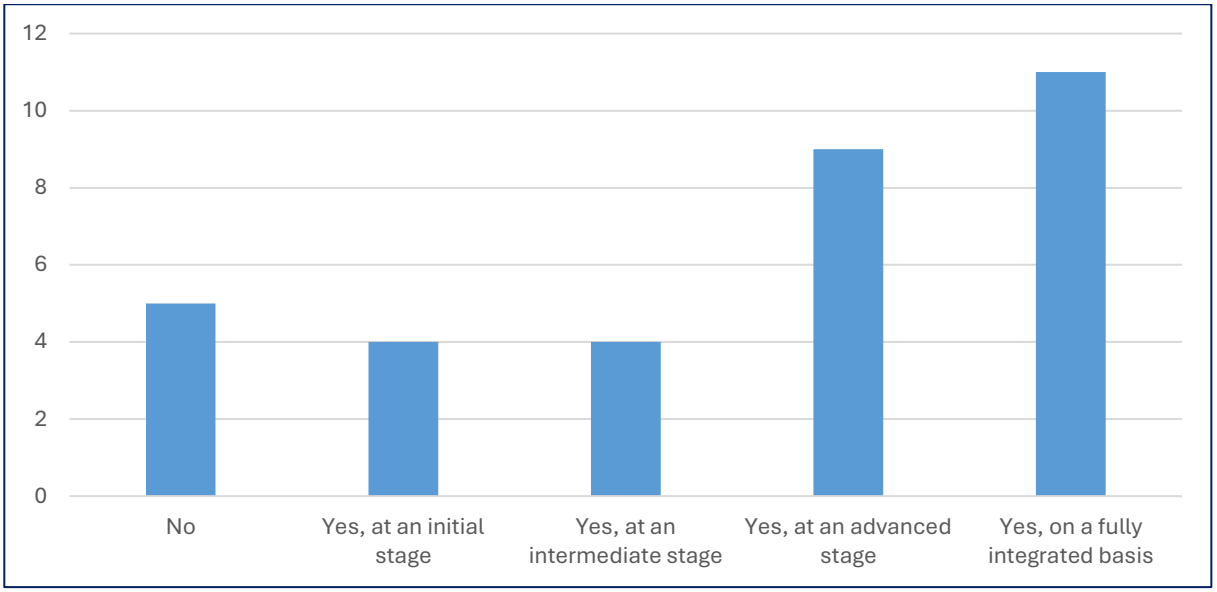


Figure 2 – Level of dematerialisation

Digital services for citizens, legal professionals and public administrations – The second dimension concerns digital services provided to external users, including electronic filing, online consultation of case files, electronic notifications and communications, online payments, tracking of proceedings and access to procedural information. In fully dematerialised systems, these services do not constitute ancillary channels but are integrated components of the judicial process itself.
Other jurisdictions have introduced mandatory electronic procedures for certain categories of users. In **Belgium**, electronic proceedings through eProAdmin are compulsory for public authorities and for parties represented by a lawyer, while self-represented litigants may continue to use paper-based procedures. Similarly, in **Austria**, lawyers are generally required to submit procedural documents electronically, although full integration between the different levels of the administrative judiciary has not yet been achieved. In **Bulgaria**, recent reforms have strengthened the use of electronic filing by public institutions and legal professionals, although the system is not yet fully paperless.

Accessibility, digital inclusion and involvement of legal professionals – A third aspect concerns the accessibility of digital services and the participation of professional users. The quality of dematerialisation depends not only on the technical availability of digital platforms but also on their effective usability by citizens, legal professionals, public authorities and persons with disabilities.

The responses reveal considerable variation across jurisdictions. **Austria**, **Belgium**, **Denmark**, **Finland**, **France**, **Hungary**, **Italy**, **Latvia**, **Luxembourg**, **the Netherlands**, **Portugal**, **Romania**, **Slovenia** and **Sweden** report high levels of accessibility of digital services for persons with disabilities. Bulgaria reports a very low

level of accessibility, with the exception of the Court's public website. Other courts fall within intermediate or medium-high ranges: **Croatia** and **Poland** fall within the intermediate range, while the **Czech Republic**, **Norway**, **Slovakia** and **Türkiye** fall within the medium-high range. In jurisdictions undergoing digital transition, such as **Albania, Cyprus, Montenegro** and **Serbia**, accessibility cannot yet be fully assessed because digital procedural services are not yet available in a structured form.

The involvement of the legal profession constitutes a further indicator of the quality of digital transformation. **Belgium, Croatia, Italy, Poland, Denmark, Estonia, Greece, Luxembourg** (administrative courts), **the Netherlands, Portugal, Slovakia, Slovenia, Türkiye, Switzerland, the United Kingdom** and **Ukraine** provide examples of lawyers being involved in the design, updating or practical use of digital platforms. Some courts involve legal professionals only in specific aspects of the operation of platforms, particularly in areas where they are the main users. This is the case, for example, in **Sweden**. **Spain** does not provide for the direct involvement of lawyers in the design, development and implementation of the platforms, but reports active cooperation with the Bar Associations in training their members in the use of the platforms and digital tools implemented by the judicial administration, including AI tools.

In conclusion, the dematerialisation of administrative judicial proceedings requires the digital case file to become the ordinary setting for the exercise of the judicial function and the entire procedural workflow to be managed in a digital, secure, accessible and coherent manner. The comparative analysis reveals a general movement towards digital proceedings while at the same time highlighting significant asymmetries: between the technological resources available and their effective use; between online services and the digital case file; between mandatory use for professional users and accessibility for citizens; and between the digital maturity of an individual supreme court and integration across the judicial system as a whole. The common finding is the progressive emergence of the digital case file as the key criterion for assessing the effective maturity of administrative justice based on dematerialised proceedings.

1.3 Cybersecurity, Data Protection and Publication of Judicial Decisions

The digitalisation of administrative justice makes cybersecurity, the protection of personal data and the online publication of judicial decisions structural components of the proper functioning of the judicial system. Electronic case files, remote working, digital services, online access to case-law and the use of advanced digital tools all require secure infrastructure, effective data protection, operational resilience and clear rules governing anonymisation or pseudonymisation. The questionnaire responses reveal broad convergence regarding the importance of these issues, while also highlighting considerable diversity in the solutions adopted and differing degrees of detail in distinguishing between declared compliance and compliance that is structurally demonstrable.

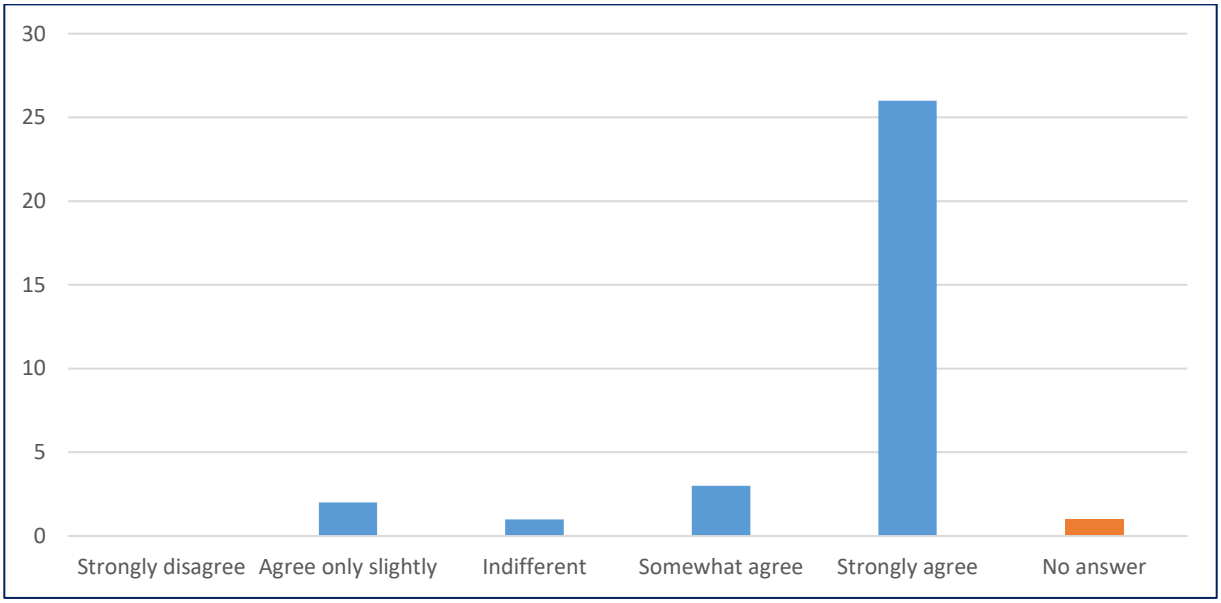


Figure 3 - Standards for security, data protection and digital preservation

Compliance, System Security, Management of cyber incidents and business continuity – A first group of jurisdictions demonstrates particularly mature arrangements for cybersecurity and business continuity. **Austria**, **Belgium**, **Denmark**, **Finland**, **Germany**, **Italy**, **the Netherlands**, **Norway**, **Poland**, **Portugal**, **Sweden** and **Türkiye** report, through different approaches, secure infrastructures, authentication systems, controlled access management, institutional IT support and data protection procedures. In **Austria**, the Supreme Administrative Court reports full compliance with both European and national standards, prompt incident management and regularly tested business continuity arrangements. **Belgium** combines secure remote access, user authentication, internal policies and institutional IT support. In **Italy**, cybersecurity is closely linked to the underlying technological architecture, the business continuity, the electronic administrative judicial proceedings system (Processo Amministrativo Telematico – PAT) and the governance of judicial data.

A second group comprises jurisdictions in which cybersecurity appears well developed or is being further strengthened, although elements of transition or opportunities for further consolidation remain. **Bulgaria**, **Croatia**, **the Czech Republic, Estonia**, **France**, **Greece**, **Hungary**, **Latvia**, **Lithuania**, **Slovakia**, **Slovenia**, **Spain**, **Switzerland** and **the United Kingdom** display varying degrees of maturity, particularly with regard to business continuity and disaster recovery. In some cases, cybersecurity is based on public or State-operated infrastructures; in others, it relies on closed networks, internal data centres, on-premises systems or models based on sovereign control of digital infrastructure. **Bulgaria**, **France** and **Switzerland** illustrate, through different approaches, the close relationship between cybersecurity, infrastructure governance and institutional autonomy. **Croatia** and **Hungary** respectively underline the need to strengthen long-term digital preservation and the importance of logging, monitoring and robust authentication mechanisms.
A third group comprises jurisdictions in which digital transformation remains at an early stage or where the available information is incomplete.
Cyprus reports that its infrastructure is adequate to meet operational needs and that its systems comply to a high degree with security standards, but provides incomplete

information on interoperability, remote working and business continuity. **Albania** highlights its efforts to align with the EU acquis on data protection, including through the adoption of Law No. 124/2024, which, among other things, introduced an obligation to anonymise judicial decisions, as well as through an agreement under the United Nations Development Programme (UNDP) to develop a digital tool for the anonymisation of judicial decisions using artificial intelligence.
Luxembourg benefits from a secure State-operated infrastructure, but the dematerialisation of judicial proceedings remains at an early stage. **Montenegro** and **Serbia** are at an even earlier stage of digital transition. **Ukraine** represents a particular case, as cybersecurity and business continuity must be assessed in the context of the ongoing armed conflict, in which digitalisation also serves as an instrument of institutional resilience. In this context, **Ukraine** has launched a project to digitalise the judicial system through cooperation between the Supreme Court, the Swedish International Development Cooperation Agency (SIDA) and the Laboratory of Legislative Initiatives. The project includes the development of a unified judicial information system (UJICS) for all Ukrainian judicial bodies. The initiative aims to modernise the IT infrastructure and automate routine processes. Cooperation with SIDA is also intended to ensure the interoperability of systems and strengthen the cybersecurity of the judicial system in wartime conditions. The project further provides for the introduction of innovative artificial intelligence solutions designed to promote consistency in case law and develop digital services, including the Ukrainian-language version of the ECHR-KS platform, which is intended to improve access to the case law of the European Court of Human Rights.

The management of cybersecurity incidents appears, in most jurisdictions, to be governed by established procedures. Greater variation exists, however, regarding the updating and testing of business continuity and disaster recovery plans. This aspect is particularly significant because digital justice requires not only systems that function under normal operating conditions but also the capacity to maintain the judicial function in the event of cyber incidents, infrastructure failures or other major disruptions.

Online publication of judicial decisions and protection of personal data – The second dimension concerns the online publication of judicial decisions. The comparative analysis shows that the digital publication of case-law has become a widespread, although not uniform, practice. These models should not be regarded as mutually exclusive. A single jurisdiction may publish a large proportion of its decisions, systematically anonymise personal data, select particular categories of judgments for publication and simultaneously develop governance arrangements for judicial data.
A first model consists of broad, or substantially comprehensive, publication combined with systematic anonymisation. **Croatia**, **Romania**, **Slovakia**, **Slovenia**, **Spain**, **Türkiye** and **Ukraine** fall within this broad approach**,** as does **Italy,** although with its own particular characteristics. **Croatia** provides a particularly significant example, since, from 1 January 2025, all judicial decisions are required to be made available online in their entirety following anonymisation. In **Spain**, decisions are published through the CENDOJ database, covering all decisions delivered by collegiate courts together with a selection of judgments delivered by single judges, all of which are anonymised.

A second model consists of structured publication supported by internal anonymisation or pseudonymisation policies. **Austria**, **Belgium**, **Bulgaria**, **Germany**, **Hungary** and **Türkiye** illustrate approaches in which the protection of personal data is ensured through internal rules, established administrative practice or organisational procedures. In **Austria**, judicial decisions are published through the Federal Legal Information System, with personal data anonymised in accordance with an internal policy. In **Belgium**, guidelines on the pseudonymisation of judicial decisions have applied since 1 February 2024. In **Bulgaria**, the Court has adopted internal rules governing the removal of personal data from decisions prior to publication. In **Hungary**, the publication of final judicial decisions through the Bírósági Határozatok Gyűjteménye (BHGY) online portal, managed by the Hungarian judicial system, involves anonymisation using techniques ensuring non-identifiability, generalisation and human validation. These examples demonstrate that anonymisation is not merely a technical process but also a legal and organisational procedure.

A third model consists of selective publication based on the legal significance or precedential value of the decision. **Portugal**, **Sweden**, **the United Kingdom** and, in relation to decisions delivered by single judges, **Spain** illustrate that not all jurisdictions have opted for systematic publication of all judicial decisions. In some systems, publication focuses primarily on judgments of precedential value, decisions of particular legal significance, decisions of higher courts or judgments selected according to institutional criteria. This model reflects a different balance between the publication of case law, the protection of personal data and the management of legal information.
A fourth and a fifth model - namely anonymisation supported by advanced digital technologies or artificial intelligence, and governed judicial open data enabling the reuse of case law data - are referred to here only briefly. These approaches, already implemented, under development or at an experimental stage in several jurisdictions, are examined in the following paragraph 1.4, which specifically addresses advanced digital tools and their governance. For present purposes, the relevant point is functional: these technologies do not affect the substance of judicial decision-making but rather the relationship between the publication of case law, the protection of personal data and the subsequent reuse of judicial information.

Publication, privacy and the governance of judicial data – The comparative analysis demonstrates that the online publication of judicial decisions, the protection of personal data and the governance of judicial data are closely connected but should not be treated as identical concepts. In several jurisdictions - including **Croatia**, **Montenegro**, **Romania**, **Serbia**, **Ukraine** and, through the CENDOJ system, **Spain** - the publication of judicial decisions has progressed further than the dematerialisation of judicial proceedings. It is therefore necessary to distinguish between three separate dimensions: digital judicial proceedings, the publication of judicial decisions and the governance of judicial data.
The decisive issue is not merely whether judicial decisions are published online, but according to which legal criteria, subject to which safeguards, with what level of data quality and with what possibilities for subsequent reuse.
In conclusion, cybersecurity, data protection and publication of judicial decisions constitute a central pillar of digital administrative justice. Digitalisation broadens access to case law and enhances judicial transparency, but it also increases the responsibility of judicial institutions in the protection of personal data, management of

cyber risks, judicial services continuity and governance of the subsequent use of case law data. The principal common finding is not the existence of a single model for the publication or anonymisation of judicial decisions, but the shared recognition that every published judgment simultaneously constitutes a judicial act, a source of public knowledge, personal data requiring appropriate protection and a potential resource for advanced digital technologies. The digital publication of case law should therefore be regarded not merely as a matter of transparency but as an essential component of the governance of digital justice.

1.4 Governance of Digital Transformation, Use of Artificial Intelligence and Future Perspectives

Governance of digital transformation constitutes the connecting framework between the dimensions examined in the preceding sections. Following technological infrastructure, the dematerialisation of judicial proceedings, cybersecurity, the protection of personal data and the publication of judicial decisions, the decisive factor becomes the capacity of the judicial organisation to govern digital tools, data, responsibilities, users, service providers and risks. This dimension assumes particular significance where digital transformation intersects with artificial intelligence (AI).
The questionnaire responses indicate that AI is not, at present, a widespread component of administrative justice. It is a technology that is largely absent or limited to auxiliary functions, either at the experimental stage or confined to controlled productivity tools.

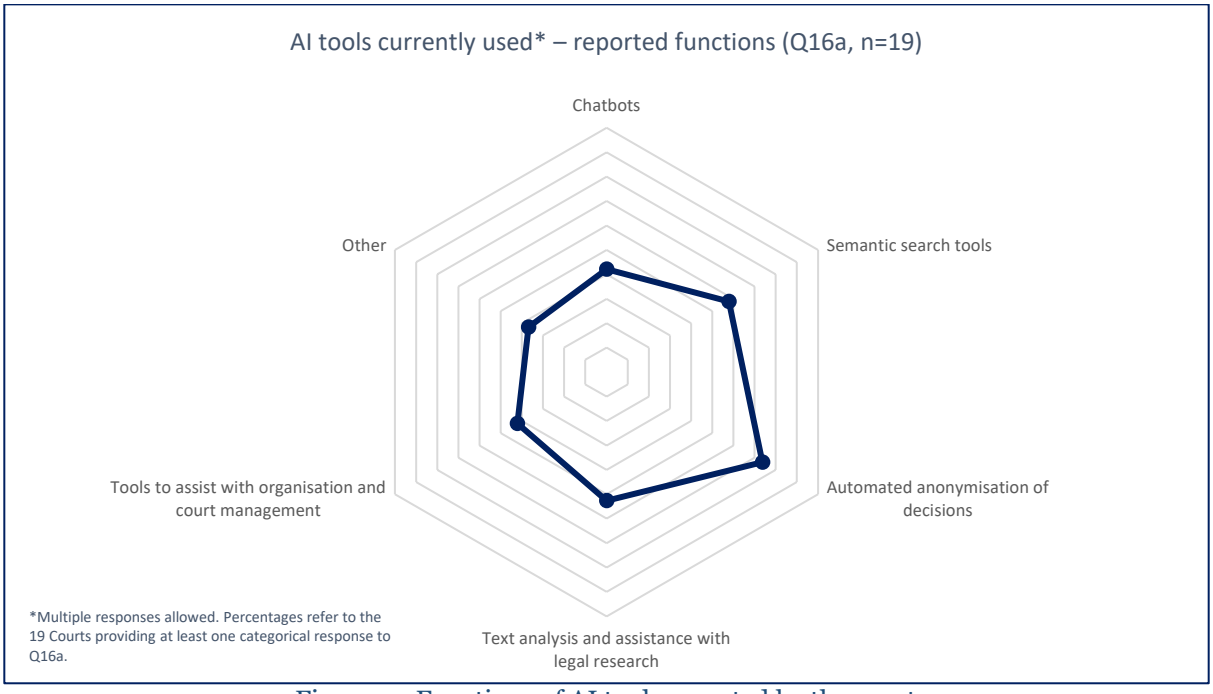


Figure 4 - Functions of AI tools reported by the courts

Recurring uses relate to activities far removed from the core of decision-making: anonymisation or pseudonymisation, semantic search, text analysis, translation, transcription, workflow management, consultation of case law and administrative management. No general trend emerges towards replacing judges or autonomously generating judicial decisions.

The most significant comparative factor is not the number of tools adopted, but the degree of institutional control over the tool, the data and the technical environment. Internal tools or those managed within supervised judicial ecosystems are not equivalent to experimental tools built for specific judicial functions, nor to general-purpose commercial tools used on the basis of internal policies, technical conditions or contractual guarantees. Security, data ownership, verifiability of use and the autonomy of the judicial function all depend on this distinction.

Digital training and the involvement of judges in technological innovation – Digital training is becoming increasingly widespread, although with varying levels of development. **Belgium**, **Bulgaria**, **Estonia**, **Finland**, **France**, **Hungary**, **Italy**, **Latvia**, **Portugal** and **the United Kingdom** report training programmes or awareness-raising initiatives relating to digital technologies or AI. In some jurisdictions, such training forms an integral part of judicial administration. In others, it remains linked to specific projects or guidance on the responsible use of digital tools. Judicial involvement likewise takes different forms. In **Belgium**, **Poland** and **Portugal**, judges participate directly through consultations, mixed working groups, technical committees or platform testing.
In **Lithuania**, judges are involved indirectly through the bodies responsible for judicial self-government. In particular, through the Judicial Council, which is composed mainly of judges, they can participate in discussions and decisions concerning the operation and development of the judicial system, including matters relating to digitalisation. Technical development and the administration of information systems, however, remain the responsibility of the National Courts Administration. With different governance arrangements, the involvement of judges is also structural in **Germany**, **Finland** and **Italy**. At the German Federal Administrative Court, the main issues relating to the introduction of new digital solutions are discussed with judges in advance, and the person responsible for IT within the judiciary is involved in all matters concerning information technology. In **Finland**, the law provides that the National Courts Administration and the Legal Register Centre (two independent authorities under the Ministry of Justice) are responsible for the maintenance and development of the information systems of the courts. Judges and court IT staff are always involved in the design process relating to technological innovation and the digital transformation of justice.
In **Italy**, judicial participation is institutionalised, as the Information Technology Service is headed by a judge and operates on a permanent basis with other members of the judiciary in close cooperation with technical specialists. Digital governance is therefore not limited to technical management alone: it requires the involvement of institutional users, as digital platforms and AI affect the organisation of work, data management and ultimate accountability.

AI tools and level of deployment – The responses reveal a number of trends, which are neither rigid nor mutually exclusive. A first group comprises jurisdictions in which judicial AI is absent, not operating in a structured manner, not widespread, or not yet deployed on a stable basis: **Austria**, **Bulgaria**, **Cyprus**, **Hungary**, **Lithuania**, **Luxembourg**, **Montenegro**, **the Netherlands, Poland**, **Romania**, **Serbia** and **Slovakia**. In some cases, such as Austria or Lithuania, this is not due to a digital lag, but to the absence of institutionally validated use cases. **Cyprus**, **Montenegro** and **Serbia** attribute the absence of AI to a digital transformation that is still incomplete.

Slovakia is noteworthy because the use of AI systems at the Supreme Administrative Court is prohibited; there is no evidence of deployment, and an internal directive is currently being drafted. **The Netherlands**, by contrast, presents a different picture: AI is under development, with a transition from proof of concept to plans for the implementation of GenAI tools, but without structured, widespread or large-scale use.

A second group comprises digitally mature jurisdictions adopting a cautious approach to AI: **Denmark**, **Finland**, **Germany**, **Norway**, **Sweden** and **Türkiye**. These countries demonstrate that a high degree of digitalisation of judicial proceedings or technological infrastructure does not necessarily entail extensive use of AI. In some instance, general-purpose tools are permitted for administrative or productivity tasks, but with restrictions on data and a ban on the inclusion of personal or confidential information.

A third group illustrates AI as a governed support tool. **France**, **Italy** and **Switzerland**, although at different stages of maturity, have developed models based on institutional control over both the technical environment and the underlying data. **Italy** provides a particularly structured example: AI tools are integrated within an already operational internal ecosystem based on judicial data and subject to human oversight. They are intended exclusively for support functions, including case management, legal research, document analysis and anonymisation, without the use of generative AI for drafting judicial texts or making judicial decisions. The Italian model is further characterised by integration with the administrative justice information system, data validation, quality assurance, traceability, bias mitigation and multidisciplinary oversight.
France has developed a model characterised by strong technological sovereignty and institutional control exercised by the administrative judiciary. This includes a large language model deployed within a segregated and controlled State-operated environment, isolated from the internet and integrated with retrieval-augmented generation mechanisms developed and operated on the servers of the administrative judiciary. **Switzerland** provides a noteworthy example through the progressive development of institutional tools supporting legal research, semantic search and anonymisation, together with its participation in the Swiss Justice Base Model initiative.

Estonia, **Latvia**, **Portugal** and **Spain** report structured forms of institutional experimentation. In Portugal, AssessorIA and the automated anonymisation project are conceived as support tools accompanied by an ethical charter and ex ante risk assessments. In **Estonia**, the tools under development concern case-file summarisation, document querying and translation. In **Spain**, automated anonymisation, semantic search, text analysis, summarisation, correction and translation are identified as occasional or limited use cases within a comprehensive governance framework. Latvia prohibits the use of AI for judicial decision-making or the drafting of decisions but permits or develops support tools for anonymisation, translation, transcription, document structuring and legal research.

Belgium, **Denmark**, **Norway** and **the United Kingdom** illustrate a different model based on the use of general-purpose commercial AI tools within institutional environments governed by internal policies, restrictions on use and technical or

contractual safeguards. The key point, in this context, is to prevent personal data, case materials or confidential information from being entered into AI systems that are not institutionally governed. Finally, **Albania**, **Croatia**, the **Czech Republic**, **Greece**, **Slovenia** and **Ukraine** report isolated or peripheral uses of AI, primarily for anonymisation or preparing judicial decisions for publication. These tools do not participate in judicial decision-making but may influence the manner in which judges access information, consult case-law and organise their work.

Governance safeguards applied to the use of AI – The most common safeguards are human oversight, data protection, restrictions on the use of non-governed tools, risk assessment, internal guidelines, ethical charters, traceability and auditability. In almost every jurisdiction permitting or experimenting with AI, AI-generated outputs are non-binding and must be verified by a responsible individual. **Italy**, **Latvia**, **Portugal** and **the United Kingdom** illustrate, through different approaches, support tools whose outputs require confirmation, multidisciplinary teams, critical review of AI outputs and the individual responsibility of the judge.
The protection of data constitutes a second essential safeguard. **Belgium**, **Denmark**, **Latvia** and **Lithuania** emphasise the importance of clear rules governing data, case materials, confidential information and the use of publicly available AI tools that are not institutionally controlled. Risk assessment is less uniform. **Portugal** provides one of the clearest examples; **Italy** emphasises accuracy, integrity, robustness and bias mitigation; while **Spain** has developed a multi-layered framework combining internal policies, testing procedures and institutional oversight. **Portugal**, **Latvia**, **Lithuania**, **Slovakia**, **Spain** and **the United Kingdom** also highlight the role of ethical charters, internal rules, judicial guidance, recommendations concerning the secure use of AI or temporary prohibitions.
A central finding emerges from the comparative analysis: the absence or prohibition of AI may itself constitute a legitimate form of governance, provided that it is accompanied by clear rules, appropriate training and awareness of the associated risks.

Risk assessment, human oversight and traceability – Human oversight, data protection and the verifiability of AI outputs must accompany the entire lifecycle of an AI system, from the identification of the use case, the selection of datasets, the development or procurement of technology, testing and validation, through to user training, monitoring, updating and auditing. Nevertheless, a gap remains between general principles and operational methodologies. Many jurisdictions affirm the necessity of human oversight without specifying procedures for disregarding, correcting, suspending or terminating AI-generated outputs. Others indicate that questions concerning risk assessment, transparency and traceability are not applicable because judicial AI is not currently in use. At this early stage in the development of judicial AI, traceability of use, dataset quality, log retention, human validation and auditing are essential to prevent experimental tools from evolving into uncontrolled informal practices.
Ongoing digital innovation projects, obstacles, investment priorities and transferable best practices – Future priorities extend well beyond AI alone. The responses identify infrastructure modernisation, cybersecurity, interoperability, external digital services, automation, digital training and the completion of the dematerialisation of judicial proceedings as the principal objectives.

The most frequently identified obstacles are financial, organisational, technical and cultural. These include insufficient financial resources, shortages of specialised personnel, organisational complexity, resistance to change, gaps in digital skills and cybersecurity risks. The transferable good practices identified do not necessarily consist of the most technologically advanced tools but rather of sound governance methodologies, including judicial involvement, multidisciplinary working groups, controlled technical environments, prohibitions on entering confidential information into unauthorised systems, training on automation risks, ex ante risk assessment, human oversight, anonymisation policies and documentation of the entire system lifecycle.

In conclusion, the governance of digital transformation cannot be reduced to the choice of whether or not to use artificial intelligence. The decisive issue is to determine which tools may be used, for which functions, on which data, subject to which limitations, by which users, under what form of institutional control and with what allocation of responsibility. At present, AI in administrative justice remains predominantly auxiliary, experimental or confined to limited use cases. Its introduction does not replace the fundamental prerequisites of digital justice - namely the digital case file, interoperability, cybersecurity, data quality, user training and operational resilience - but presupposes them. The common denominator across all jurisdictions is the centrality of human oversight. Even in the most advanced systems, the decision ultimately rests with the judge or the competent authority, while digital and AI tools can only support activities that remain transparent, verifiable and institutionally accountable.

Co-funded by
the European Union

Session 2 - Automated Administrative Decisions and Judicial Review by Administrative Courts

2.1 Legal basis of instruments enabling the use of digital technologies or AI in administrative acts

Sector-specific legislation and legislation generally applicable to any type of administrative procedure - An examination of the reports received from individual countries reveals, first and foremost, that in many cases no national legislation has yet been adopted that specifically regulates the use of automated decisions and that, at present, the use of advanced artificial intelligence (hereinafter simply 'AI') or algorithms is, in most cases, governed by sector-specific provisions scattered throughout or contained within the respective national laws on administrative procedure.

The use of automated administrative decisions is based on general provisions in **Austria**, where AI tools may be used to adopt fully or partially automated decisions, the latter being characterised by the requirement for a body to personally validate the automated decision generated by the AI. A similar general provision, however, stipulates that fully automated decisions must be covered by a specific provision. The absence of sector-specific legislation, and therefore the need to apply the general rules on administrative procedure, is also noted by **the Czech Republic, Italy, Luxembourg, Montenegro, the Netherlands**, **Romania, Serbia, Slovenia, Spain, Turkey, Ukraine** and **the United Kingdom.**

Similarly, in **France** there are no specific provisions authorising the use of digital or AI-based systems, but for over 20 years French law – in particular thanks to the legal doctrine developed by the Council of State – has established a regulatory framework based on a set of fragmented provisions drawn from European law, personal data protection legislation and other sector-specific legislation. In this way, the use of algorithms has gradually become part of administrative practice, to prepare, guide or facilitate decision-making, without replacing the human element. In general, algorithms may also be used in discretionary decisions, provided that they do not replace human judgement. Currently, the use of AI is permitted at all stages of the administrative process. During the design phase, to improve data quality and traceability and to avoid bias; during the implementation phase, the use of AI must be based on a specific legal basis and comply with general principles; during the operational phase, human oversight must be guaranteed.

Some states share a system characterised by the fact that a general provision permits the use of AI or algorithmic systems in cases expressly provided for by another provision. In **Germany,** the Federal Administrative Procedure Act stipulates that an administrative decision may be based entirely on automated systems provided that this is permitted by a statutory provision and that the exercise of discretionary powers is not required. In essence, fully automated administrative decisions are prohibited unless expressly permitted by a statutory provision. The legislature has rarely exercised this power, doing so only in areas where

there is a massive volume of administrative acts, such as in the tax and social security sectors. In **Greece**, a 2022 law authorises the use of AI systems in the public sector to support decision-making, but only if a specific statutory provision permits such use and includes safeguards for the protection of individual rights. However, there are no provisions specifically authorising the use of algorithms for making discretionary decisions. This 2022 Act stipulates that any public sector body using algorithmic systems must carry out an algorithmic impact assessment before putting them into operation. The assessment must consider the public interests pursued through the use of algorithms, the categories of decisions that may be taken, the characteristics of the systems, the types of data that may be collected and processed, the risks to fundamental freedoms, and the expected benefits. The law also provides for transparency obligations; specific obligations for manufacturers and suppliers of AI systems intended for use by public bodies; and the establishment of a register of AI systems. In **Latvia**, the use of automated or algorithm-based administrative decisions is permitted, but only where expressly provided for by law: this is also in relation to the requirement that every administrative decision must bear a signature. The law permits the adoption of fully automated decisions, without an official's signature, for notices of property tax payments, which are based on official data and objective calculation criteria; decisions in favour of the data subject regarding tax refunds, again on the grounds that these involve only mathematical calculations without discretionary assessments; and penalties for breaches of the Highway Code. The rationale behind these provisions is that, in such cases, AI systems are used based on predefined legal criteria and a structured data-processing system, and primarily where the decision depends solely on objective data. The aim is to enhance the efficiency of administrative action, increase the volume of standardised decisions, and ensure the consistent and clear application of binding rules. In **Switzerland**, too, a general provision contained in a federal law stipulates that decisions taken by federal authorities exclusively on the basis of automated processing of personal data, which may have significant legal consequences for the data subject, must be identified as such; that is, they must specify that they are automated decisions. If they are likely to seriously affect the fundamental rights of the data subject, they are permissible only if a provision specifically allows for this. In general, automated decisions are permitted for decisions that are limited to simple classifications or for large-scale, repetitive tasks.

In other countries, automated decisions are governed by sector-specific legislation. In **Belgium**, there is no general legislation permitting the use of digital or algorithmic decisions, but there are sector-specific laws. For example, a 1990 Act allows social security institutions to process the data necessary for the performance of their duties, namely the prevention, detection and punishment of infringements; in particular, this legislation permits the use of algorithms to carry out *data mining* and *data matching* operations in order to create profiles that help determine which cases should be subject to checks. A 2018 law permits identical measures for the purpose of processing the personal data of taxpayers and carrying out targeted tax inspections and audits. In the French Community, too, a decree of July 1997 permits the use of algorithms by educational institutions to optimise the allocation of pupils across different schools. It should also be noted that the Flemish Region provides local

authorities with software to assist them in drafting the traffic-related documents falling within their remit. In **Denmark**, there are legislative provisions authorising the use of digital tools, which consist mainly of self-service digital platforms and the collection of information: these tools are primarily intended to provide the basis for administrative decisions based on calculations or objective criteria, where digital technologies are appropriate. For example: to update the platform used by students to apply for benefits. In **Estonia,** there is specific legislation governing not so much the tools and purposes, but rather the competent authorities and which decisions may be automated. For example, in relation to *environmental* charges, the tax authorities may take fully automated decisions; the Unemployment Insurance Fund may, within the scope of its powers, issue fully automated decisions where possible under the circumstances. Similar powers are also granted to the competent forestry authority. In **Lithuania**, legislation allows public administrative authorities (PAAs) to use, during administrative proceedings, IT systems, registers and electronic platforms relating to public services, as provided for in the Law on Public Administration of the Republic of Lithuania and the Law on the Management of State IT Resources. The main objectives are to improve the efficiency of administrative procedures, facilitate access to public services, and ensure the effective processing and exchange of administrative data, in accordance with data protection legislation. Lithuanian legislation does not contain any provisions specifically authorising the use of algorithms for the exercise of discretionary powers, and the public administration is required to exercise such powers in accordance with the principles of legality, proportionality and reasonableness. More specifically, Lithuanian legislation permits the use of automated decisions in certain penalty proceedings. The Code of Administrative Penalties provides that decisions may be generated on the basis of data recorded in computerised systems relating to enforcement. In **Finland**, only regulated systems may be used in the decision-making process: to this end, the Administrative Procedure Act sets out the specific conditions which, in addition to the other conditions laid down by law, a public administration must comply with in order to adopt a decision based on the automated processing of data, without human supervision. The Act on the Management of Public Administration Information contains provisions that ensure consistency and high quality in the management of public authorities' databases, regulate individual responsibilities and ensure secure data processing in order to guarantee public access to information, whilst also ensuring the efficient use of such data. Automated decisions are used, for example, in matters relating to taxation or social assistance. There is also the Act on Electronic Services and Communication in the Public Sector, which contains provisions aimed at ensuring the efficiency and speed of transactions, information security within public administration bodies and the courts, whilst promoting the exchange of information. The Act on the Supervision of Certain Artificial Intelligence Systems contains further provisions that complement the regulation on AI. In **Poland**, there is legislation governing the computerisation of public bodies' activities, i.e. the digitisation of the public administration. In **Portugal,** various provisions authorise and encourage the use of digital and algorithmic tools in the work of the public administration. The Code of Administrative Procedure sets out the principle of e-government, expressly permitting the creation of purely digital documents, facilitating

the dematerialisation of procedures and replacing paper-based or oral procedures with purely electronic ones, subject to respect for fundamental rights, transparency and procedural safeguards. A 1999 decree provides the legal framework for the digitisation and interoperability of public information systems, promoting their use to improve the efficiency, speed and quality of services for citizens and businesses: the main instrument is SIMPLEX 2025. A decree of 2024 regulated the drafting of provisions relating to digital services by public administrations, with the aim of enabling citizens to experience integrated access to services via a single channel. This requires the implementation of a centralised public channel (Single Digital Service Portal). The Strategy for the Digital Transformation of the Public Administration for 2021–2026 and the National Strategy for Artificial Intelligence (AI Portugal 2030) recognise and promote the use of automated or semi-automated decision-making, through systems, data analysis algorithms, robotic processes, AI for the assessment of screening requests, risk assessment and decision support, as well as the use of interoperable platforms. The National Action Plan for the Digital Strategy for 2026/2027 highlights the need to simplify interaction between citizens, businesses and the state. Overall, this is a legal framework comprising legislative provisions and soft law, which aims to increase the efficiency and speed of administrative procedures, ensure transparency and traceability in the decision-making process, guarantee equal treatment, eliminate discrimination and modernise public administration. Where AI systems are used, responsibility for the final decision always lies with a human, in line with the general principles of legality, proportionality and the protection of individual rights. In **Slovakia**, there is a series of legislative acts (which came into force between 2013 and 2019) governing and authorising the use of AI tools. The matter is also addressed in the National Concept of Informatisation of Public Administration for 2026–2030, which establishes a basic framework for the use and development of AI systems within public administrations. The aim of these provisions, contained in the various bodies of legislation, is to provide services to citizens and businesses more securely, whilst utilising resources more efficiently and cost-effectively; to establish electronic communications as the primary means of communication with public administrations, whilst also introducing new tools such as document conversion, electronic mailboxes, electronic identification and authentication, payments to public administrations, electronic authorisations and *reference registers*. The legislation also addresses security in electronic transactions, regulating signatures, seals and time stamps in accordance with the eIDAS Regulation; as well as cybersecurity. On the basis of the provisions contained in these laws, a wide range of acts may be carried out using AI tools: identification, authentication, authorisations, electronic applications, electronic documents and electronic deliveries – in short, virtually any act that is not expressly excluded. However, there is no provision allowing the use of AI systems for the adoption of discretionary decisions. In **Sweden,** there are provisions that specifically authorise the use of digital or AI systems for the exercise of administrative powers. In particular, the 2017 Administrative Procedure Act does not impose any specific restrictions on the tools that may be used for automated decision-making. However, limitations arise from the EU General Data Protection Regulation. There are also sector-specific provisions that restrict the use of automated decisions to cases where a

statement of reasons may be omitted or is not specific to an individual case: this applies, for example, to decisions on pension claims. Discretionary decisions are not suitable for adoption via automated systems; moreover, when AI systems are used, the public administration is not relieved of its responsibilities to ensure that the final decision is objective and impartial.

In the United Kingdom, **the development, implementation and use of AI tools are regulated by various bodies of soft law**, in the form of guidelines. In particular, the Data and Ethics Framework sets out seven principles that guide the use of AI systems in the public sector, namely: transparency, accountability, due process, security, social impact and environmental sustainability. The UK Government's Artificial Intelligence Playbook, on the other hand, sets out ten principles to be followed for the responsible, effective and secure use of AI within the government organisation. Responsibility for developing standards relating to the development, implementation and use of AI lies with the Department for Science and Innovation, specifically the Digital and Defence Service.

In other countries, the use of automated administrative decisions is lawful within the framework of the AI Act. In **Bulgaria**, amendments have been made to the Code of Administrative Procedure, providing for the possibility of submitting applications electronically. In 2025, a law was passed – though it has not yet come into force – stipulating that applications to public authorities, whether from organisations or professionals, must be submitted exclusively by electronic means, and further providing that all administrative and judicial proceedings must be conducted solely by electronic means. Only private individuals will continue to have the option of submitting applications on paper. In 2025, a bill was introduced to regulate the use and development of AI: this law aims to implement EU Regulation 2024/1689, to limit risks to national security, to train workers, employees and civil servants in the use of AI tools, to regulate the use of AI in the public sector and in electronic administrative services, to promote investment in the use and development of AI, and to mitigate risks to minors arising from the use of AI. In **Croatia**, too, the regulation of AI systems is primarily set out in the law implementing the AI Act: the regulatory framework specifically addresses certain risks, prohibiting manipulative or biometric AI systems, requiring transparency and assessments for high-risk systems, and mandating human oversight. Other provisions currently undergoing approval further specify the national strategy for the implementation and use of AI in order to meet European standards.

In **Norway**, there are no general or specific provisions governing the use of automated decision-making, nor are there any provisions governing the development, implementation and use of AI tools. This does not mean that the sector can be considered unregulated: the general rules on administrative procedures set out in the Public Administration Act must apply. In 2025, the Public Administration Act was passed, which contains provisions allowing for the automation of procedures provided that the general conditions of the procedure are met. This Act does not specify which AI tools are permitted, nor the objectives to be pursued: it is technology-neutral. However, according to the preparatory documents, the main purpose of automation is to process procedures more quickly and with fewer resources. One of the provisions

prohibits automated decisions if the rules establishing the relevant powers exclude their use, or if the procedures in question fall within the scope of Article 22 of the EU General Data Protection Regulation. Within these limits, automated decisions are permitted even in cases where discretionary powers are involved. The Public Administration Act has not yet entered into force. The AI Act is not yet applicable in Norway as it has not yet been incorporated into the European Economic Area (EEA) Agreement, and it is unclear when this will happen: a draft bill to implement the AI Act is currently under consideration.

The questionnaire also provides an overview of the implementation of the AI Act and the associated obligation to designate the relevant national authority as provided for by that legislation. In **Bulgaria**, the Communications Authority has been designated as the Digital Services Coordinator; it will be responsible for monitoring the implementation of the AI Act, resolving out-of-court disputes, gathering information from a wide range of stakeholders in the digital ecosystem, and will also have the power to carry out inspections and apply urgent measures to prevent serious harm, including blocking access to digital services. Bulgaria plans to achieve a full digital transformation of all key sectors by 2030. In **Croatia,** the regulation of AI systems is primarily set out in the law implementing the AI Act: the national implementing measures include the designation of competent authorities, such as the Ombudswoman and the Personal Data Protection Agency. The Ministry of Industry and Trade acts as the main coordinating authority for the implementation of AI systems and is responsible for the entire agenda. An agency has also been established which is the main body responsible for the digital transformation of the public administration; it is also tasked with identifying the technical and methodological standards relating to digital services; it is the body that ensures that every digital or algorithmic tool used by the State is interoperable and complies with legislative standards. In **Denmark**, an agency has been established which is the principal regulatory authority for the use of AI systems by public authorities and which also acts as the Authority under the AI Act: it is tasked with identifying the measures necessary to implement the Act and ensuring its enforcement. This process is still at a fairly early stage. It has also been assigned monitoring tasks and inspection powers aimed at ensuring compliance with legislative provisions within public administrations. In **Finland,** there is no specific authority tasked with developing regulations to govern the use of AI: generally speaking, the Minister of Finance has adopted guidelines for the use of generative AI in public administrations, whilst individual public administrations have produced their own specific guidelines. The regulation of decision-making based on automated systems is set out in legislation. Generative AI systems are not currently permitted for administrative decisions. In **Germany**, a draft bill to implement the AI Act is currently under consideration, which provides for the establishment of a special federal agency to act as a supervisory authority. The Ministry of the Interior has developed non-binding guidelines for the federal public administration, whilst the Ministry for Digital Transformation and Administrative Modernisation has also developed guidelines for the planning and implementation of AI in the public administration. Both sets of guidelines recommend transparent communication. There are also provisions adopted by individual federal states. Overall, the regulatory framework comprises both federal

and state-level legislation, as well as soft law. The draft bill currently under consideration provides for the establishment of an Agency, which will be tasked with supporting market supervisory authorities, coordinating cooperation between the authorities to which powers are conferred by this Act, facilitating the adoption of codes of conduct, and ensuring the involvement of civil society. In **Greece**, by decision of the Minister for *Digital Governance*, an authority has been established responsible for the implementation and development of AI, for the adoption of guidelines, and for the drafting of proposals, actions and recommendations. A supervisory authority has also been established within the Ministry for *Digital Governance*, acting as the executive arm of the former. In addition, an observatory has been established, whose main mission is to collect data on the implementation of the national strategy and to prepare reports on the use of AI in the country's activities. There is also a private-law body, the 'Hellenic Artificial Intelligence Factory Limited', under the supervision of the Ministry of Digital Governance, whose mission is to create, support and explore AI technologies. In **Portugal,** the authorities responsible for designing and implementing general rules and standards for the use of AI systems are the State Agency for Technological Reform, the National Data Protection Commission and the National Communications Authority. In 2026, the Council of Ministers approved the National AI Agency, which provides the legal framework for the use of AI during the period 2026–2030 and whose main pillar is the implementation of regulations that protect citizens and enable businesses to adopt innovative systems safely. In **the United Kingdom**, responsibility for developing standards relating to development, implementation and use of AI lies with the Department for Science and Innovation, specifically the Digital and Defence Service. A draft bill on the use of AI in administrative decisions has also been announced. In **Slovakia,** the authorities responsible for drawing up general regulations and technical standards are the Ministry of Investment, Regional Development and Informatisation, and the Commission for Ethics and Regulation of AI, which is an independent body: the latter is tasked with assessing the ethical, social and legal impact of the use of AI tools. The National Security Office, meanwhile, is the national authority on cybersecurity. In Sweden, the Swedish Agency for Digital Administration has been established.

General principles derived from the legal system or referred to in sector-specific provisions, applicable to automated administrative acts – In virtually all the countries that responded to the questionnaire, there is consensus on identifying, among the general principles that must be observed to ensure the lawfulness of (wholly or partly) automated administrative decisions: the **principle of legality**, which in some cases is interpreted to mean that there must be a legal provision expressly permitting the use of automated decisions; **the principle of algorithmic transparency**, which gives rise to the administration's obligation to inform the data subject of the automated nature of the decision and, in certain cases, also to specify immediately the characteristics of the AI system or algorithm used; the **principle of accountability**, from which it follows that an automated decision cannot be attributed to a machine, but must be attributed to a public authority vested with the relevant powers, and must be signed by an official – a natural person – who assumes responsibility for it; the ***'human-in-the-loop'* principle**, according to which human intervention must be

provided for, at least at the review stage, where requested by the data subject; the principle of **due process and the right of appeal** to a judicial authority; the **principle of transparency and comprehensibility of the algorithm**, from which it follows that the public authority must inform the data subject of the use of an algorithm, or other AI tool, in a comprehensible manner, specifying at which stage of the procedure and for what purposes the tool was used, as well as the inputs and operating criteria; the **principle of non-discrimination**; the **principle of justification**, which requires the administration to explain the reasons why the recommendation provided by the AI system or algorithm is considered reliable and accepted.

Germany highlighted that a law of one of the federal states (the IT Act of the Federal State of Schleswig-Holstein) also provides, for the purposes of the lawfulness of automated decisions, for compliance with the principles of technical robustness and security, (protection of) diversity, equity, and the right to social and environmental well-being.

Latvia also referred to the principles of **proportionality and legitimate expectations**.

The United Kingdom also highlights **the principles of consideration of social impact and environmental sustainability**, as well as the **principle of rationality**, according to which an automated decision must not give rise to irrational results or consequences.

Portugal also refers to the **principle of the protection of individual rights**.

Sectors in which the use of digital technologies or AI tools for the adoption of administrative acts is subject to prior authorisation or is frequently excluded - A significant proportion of the States that responded to the questionnaire reported that, at present, no specific legislation has yet been adopted to regulate the lawfulness of automated administrative decisions, nor are there any provisions expressly prohibiting their use – either generally or in specific cases – or permitting them subject to specific authorisation. In this context, there is a tendency to regard automated decisions as permissible where they do not require the exercise of discretionary powers, in particular for standardised or mass decisions, or where AI/algorithmic systems are used solely to support the final decision (**Croatia, Denmark, Poland, the Czech Republic, Finland, Latvia, Switzerland**). In several cases, it is simply acknowledged that the relevant legislation provides for neither specific prohibitions nor cases subject to prior authorisation (**Montenegro, Norway, the Netherlands, Portugal, the United Kingdom, Romania, Slovakia, Slovenia, Spain, Sweden, Ukraine**), subject to compliance with general principles.

In other cases, certain restrictions or prohibitions have been reported.

In **Austria,** fully automated decisions are subject to specific provision in a statutory instrument.

In **Albania**, there is currently no provision for the adoption of automated administrative decisions, except within the scope of certification/attestation activities and the granting of authorisations. In general, the regulatory framework does not contain specific provisions on the use of AI and algorithmic systems.

In **Estonia**, in the absence of specific restrictions, the Supreme Court has recognised the legitimacy of an automated decision of a discretionary nature, specifying that the public administration must ensure, in every procedure, that all relevant circumstances are taken into account: therefore, if no technology is available to ensure this outcome, a human body must also intervene in the decision-making process. In principle, no sectors are excluded, provided that the technology ensures that all relevant factors are taken into account. A specific legal basis is required only for decisions involving the processing of personal data.

In **France**, the ban on facial recognition applies, including in accordance with the GDPR

In **Belgium**, a law passed in 2022 introduced a ban on the *Agence autonomiseè externe du droit public* from relying on fully automated decisions made without any human intervention when such decisions affect an individual's legal rights or have similar consequences for that person; however, the legislation provides for an exception where the system has no impact on the decision (for example: verifying the validity of a residence permit). A similar prohibition was introduced by another Act of 2022 for the autonomous external private-law agency 'Flemish Public Services', in this case without any exceptions to the principle.

In **Germany,** legislation is always required that expressly permits the use of automated administrative decisions, in accordance with Article 35 of the General Administrative Procedure Act. Furthermore, the IT Act of the Federal State of Schleswig-Holstein excludes the use of technology in the following cases: for the purpose of adopting enforcement measures involving the direct use of force against a person's life and physical integrity; for the purpose of assessing the personality, physical and psychological performance, resilience, cognitive or emotional abilities of human beings, in order to make predictions about their propensity to commit crimes; for the identification of individuals among the public; and for the adoption of measures involving the exercise of discretionary powers.

In **Greece**, the 2022 Act stipulates that the use of AI systems is permitted only where provided for by specific legislation. Furthermore, it excludes decisions made by the Ministries of National Defence and Citizen Protection, the bodies under their supervision, and the secret services from the scope of the AI regulations. Nevertheless, AI systems are also used in the defence sector, expressly permitted by a law of 2024, which reserves the development and integration of AI technologies into military systems to the Artificial Intelligence Department

In **Hungary,** legislation is required that expressly permits the use of automated administrative decisions for the adoption of decisions involving discretionary powers. The Digital State Act of 2023 sets out in detail a decision-making process that allows

entire procedures to be carried out, from start to finish, without human intervention, whilst still allowing the administration to intervene. Indeed, to safeguard their interests, the addressee may always request a reassessment through ordinary proceedings. In any case, sector-specific provisions must determine the circumstances in which automated decisions may be adopted. The implementing decree of the Digital State Act of 2024 provides for voice identification mechanisms for certain procedures. However, the use of automated procedures is excluded where discretionary powers are involved or where they are precluded by statutory provisions or a government decree in specific cases. Within this legal framework, the body providing digital services may, at the request of the data subject, conclude the procedure with a decision that does not involve human intervention, of which the data subject must be informed. The 2016 General Act on Administrative Procedures permits the use of automated decisions provided that the conditions set out in the Digital State Act are met and there are no opposing parties. A Government Decree of 2024 laid down all the technical details of automated administrative decisions. Essentially, in Hungary there must be a legal basis authorising the adoption of automated decisions: at present, such decisions are permitted in proceedings for the cancellation of attachments on immovable property, for the cancellation of mortgages registered by the tax authorities, and for the imposition of administrative penalties for breaches of the Highway Code. In any case, automated decisions are permitted, but not decisions based on AI (it is unclear whether this exclusion applies to any AI system or only to generative or deep learning systems).

In **Italy,** certain provisions expressly permit the use of automated decisions in public procurement procedures; in the healthcare sector, to support diagnosis and treatment; for the purpose of strengthening national resilience under the supervision of the National Cybersecurity Agency; and in areas covered by copyright. Law No. 132/2025, which grants the Government the power to issue regulations on AI, excludes certain sectors from its scope of application (activities carried out for national security purposes and subject to secrecy, cybersecurity and resilience activities, police activities, and similar), all of which are aimed at safeguarding national security: in these sectors, therefore, the use of AI systems for administrative decision-making is subject to the discretionary assessment of the competent administrative body, which must identify both the acts that may be adopted using AI systems and the AI systems that may be used. Outside these cases, AI systems may be used to support the decision-making process, which remains the responsibility of an official of the competent administrative body.

2.2 Access to, transparency of and challenges to administrative decisions involving the use of digital technology or AI systems

The possibility of exercising the right of access to ascertain how digital technology or an AI tool has influenced the administrative decision and whether it has functioned correctly - In most countries, there are no rules specifically requiring the administration adopting an automated administrative decision to specify that the decision was adopted with the aid of an AI system or an algorithm, and/or to specify its characteristics. Nor are there any rules requiring public authorities to disclose to the public the use of AI systems, or allowing the public to challenge such a decision

(**Croatia**, **the Czech Republic**, **Estonia**, **Italy**, **Latvia, Luxembourg**, **Norway**, **the Netherlands, Poland, Spain, Sweden, Turkey**). However, in such cases, an obligation to disclose the use of AI or algorithmic systems for the purposes of the decision may be derived from the general principles of good administration, transparency and the provision of reasons (**Denmark**, **France**, **Portugal**).

In other cases, however, provisions are cited which impose specific transparency obligations on public authorities.

In **Belgium**, there is a national law – which, however, has not yet come into force – requiring federal authorities to make available to the public a document explaining whether, and if so which algorithms are used in the decision-making process regarding applications: this law requires authorities to act proactively, making information on the algorithms used available without waiting for specific requests from members of the public. However, the law does not specify what information regarding the functioning of the algorithms must be made available: a royal decree, approved by the Council of Ministers, could specify this information, but this power has not yet been exercised. Apart from this provision, there is no general rule requiring authorities to disclose, on their own initiative, that an algorithm has been used. It should also be noted that when an administrative act is challenged before the Council of State, the public administration is required to produce all the evidence on which the decision was based: therefore, if an algorithm has been used, this must be specified, and the Council of State may, if it deems it necessary, order the public administration to produce all information relating to its operation. Furthermore, Article 22 of the GDPR applies; with regard to the processing of personal data, this requires the data controller to inform the data subject as to whether a decision concerning them has been made by automated means.

In **Finland**, an automated administrative decision must specify that it is an automatically adopted decision and must indicate how to access the relevant information, as set out in the Act on the Management of Public Administration Information. This Act also stipulates that the decision to use automated decision-making must be published on the public authority's website, together with the reasons and documents on which that decision is based.

In **France**, if a decision is based on algorithms or AI systems, the administration has a heightened duty of transparency towards the data subject and must explicitly inform them of the use of such a system, specifying its purpose and the procedures for exercising the right of access. At the data subject's request, the administration must disclose the essential characteristics of the algorithm, subject to the need to protect trade secrets.

In **Germany**, the IT Act of the Federal State of Schleswig-Holstein requires that the data subject be informed, in a comprehensible manner, when data are processed by a machine rather than a human being, so that the data subject understands beyond any doubt that they are not interacting with a human being. Communication by a human being must also be ensured. This law also requires that decisions include a reference to the disclosure of the algorithm – subject to the protection of third parties' personal data – which must be accompanied by information on how the algorithm works: in this case,

the purpose of using the technology must also be stated, the level of automation must be explained, and information must be provided regarding the possibility of challenging the legal and factual consequences of the use of AI

In **Greece,** under the 2022 Act, every public sector body using AI systems must publicly disclose such use and must ensure that the recipients of automated decisions are informed, in a comprehensible and easily accessible manner, of the characteristics of the decision-making criteria, including accessible information for persons with disabilities (for example: via forms written in Braille for the blind).

In **the United Kingdom**, the guidelines on the use of AI in the public sector stipulate that the use of AI tools and the extent of such use should be disclosed, and that the public should be informed about where and how AI systems are used. Other soft-law provisions recommend transparency through explanations of the algorithm used; however, it is also recognised that full transparency is not possible when deep learning systems or large language models are involved, and it is further acknowledged that in some cases transparency may be limited by intellectual and industrial property rights.

Possibility of challenging the use of digital technologies or AI tools by a public administration - In general, the States that responded to the questionnaire recognise the possibility of challenging the use of AI systems for the purposes of automated administrative decision-making, in the context of appealing against a specific decision (**Albania, Belgium, the Czech Republic, Finland, France, Germany, Italy**).

In **the United Kingdom**, the guidelines recommend maximum transparency, which should also entail an obligation to disclose the use of AI systems as soon as possible.

2.3 Automated administrative acts based on the use of digital technology or AI tools: an analysis of the case law

Criteria for assessing the lawfulness of automated administrative decisions and principles that must be upheld -Many of the States that responded to the questionnaire report that, at present, there are no case law precedents specifically addressing the lawfulness of automated administrative decisions, i.e. those based wholly or partly on the use of AI systems or algorithms (**Bulgaria, Cyprus, Croatia, Finland, France, Latvia, Luxembourg, Montenegro, Norway, Poland, Portugal, the Czech Republic, Romania, Serbia, Slovenia, Sweden, Switzerland, Turkey, Ukraine, Hungary**).

In **Austria,** a 1987 ruling by the Constitutional Court established that automated decisions are lawful provided that there is no doubt as to the binding nature of the task 'delegated' to AI systems, human supervision is maintained, and the decision is in any case attributable to an official of the public administration vested with the relevant power.

In **Belgium,** the Council of State has ruled that in proceedings leading to the adoption of a detrimental measure, such as a disciplinary sanction, the administration must allow the person concerned to participate in the proceedings, making available to them all the evidence on which it intends to base the decision (and therefore, where

necessary, disclosing the use of AI systems). In general, however, there is currently no judicial decision that has specifically ruled on the lawfulness of algorithmic decisions or those based on AI systems. Furthermore, the Council of State ruled on a case in which an administrative body had envisaged the use of algorithmic decisions to carry out part of the procedures for a competitive examination – specifically, the marking of aptitude tests – in order to suggest a mark to the selection board, whose discretion at that stage was limited by the algorithm's previous assessments: The Council of State annulled the final decision which rated the appellant as 'rather weak', on the grounds that it had deviated, without justification, from the algorithm's assessment, which had instead rated the appellant as 'rather good'. In another case, dating from 2004, the Council of State ruled that the award of a contract was unlawful on the grounds that it was based on a statement of reasons characterised by obscure language, which referred to the use of a certain piece of software and a specific application. It was therefore a statement of reasons that failed to meet the obligation to provide adequate reasons for every administrative decision, in particular as it did not adequately explain the reference to the software and application used for the purposes of the decision.

In **Denmark,** case law has held that automated administrative decisions are lawful provided they have a specific legal basis, comply with the provisions of Article 22 of the GDPR (the right not to be subject to a decision based solely on automated processing), and comply with Danish national legislation. The Council of State has stated that decisions based on algorithms are subject to the same general principles applicable to other administrative acts: the need for a specific legal basis, the obligation to state reasons, and *'proper case handling*'. According to case law, automated decisions must comply with the principles of transparency, non-discrimination, knowledge and understanding of the algorithm, delegation of power to an authority, the principle of legality, 'proper administration', the right to a statement of reasons, and must ensure a *'human in the loop*'. There are currently no precedents that have ruled on the legal status or nature of the algorithm.

In **Estonia**: the Supreme Court had the opportunity, in 2023, to rule on an automated decision issued by the competent forestry authority, establishing that the decision was not unlawful merely because it was automated. It should be noted that, at present, no comprehensive data is available on the extent of public administrations' power to adopt automated decisions. However, it is clear from the aforementioned precedent that an automated decision is lawful provided that it complies with the principles ordinarily applicable: preliminary investigation, the precautionary principle, and the duty to provide information – principles from which the public administration cannot derogate merely because it uses automated systems, even if these have specific characteristics. A specific legal basis is required for automated decisions involving the processing of personal data. Case law has, in particular, identified the principle of non-discrimination and the requirement that the decision be attributed to an authority vested with the relevant powers as the legal criteria for automated decisions.

In **Greece**, the Council of State, in a 2024 ruling, had the opportunity to rule on disputes concerning acts adopted, in whole or in part, on the basis of automated systems: the issue at hand did not concern the technical soundness of the tool used, but

rather the interpretation and application of the legal conditions set out in the relevant legislation in the case in question. The Council of State therefore affirmed the public administration's obligation to give reasons for its decision, in accordance with the principles of transparency and legality in administrative action. In particular, it held that, in the case of automated decisions, the public administration must specify both the various stages of the mathematical calculation carried out by the authority and the variables taken into account: in this way, the person concerned is able to ascertain whether the relevant rules for the case have been complied with, and this also enables judicial review. In two further decisions, dated 2024 and 2025, the Greek Council of State, sitting in plenary session, examined the lawfulness of elections to university bodies based on algorithms, ruling that such a system does not infringe the principles of academic freedom, personal liberty or proportionality: this is because, whilst acknowledging the complexity of the AI system used, in the case in question it remained mathematically verifiable and possessed technical characteristics capable of guaranteeing the integrity of the voting process and the verifiability of the result.

In **Italy**, the Council of State has ruled on this matter on several occasions, repeatedly affirming the legitimacy of using AI tools, despite the absence of specific regulatory provisions: it has in fact been held that the decision to use algorithms is of an organisational nature and is legitimate if adopted in accordance with the principle of specificity applicable to administrative acts.

On another occasion, the Council of State stated that the administration is not obliged to justify the decision to use algorithmic systems, but must explain, in its reasoning, why it chose a particular type of algorithm, and must also ensure that the logic behind its operation is transparent. Even before the entry into force of Law No. 132/2025, the Council of State had affirmed the need to ensure the transparency and comprehensibility of the algorithm.

In **Lithuania**, in a 2022 ruling, the Supreme Administrative Court addressed the issue of the lawfulness of an automatically generated decision – in this specific case, an approval decision – resulting from the fact that the competent public authority had failed to issue a decision within the prescribed time limit.

In **the Netherlands,** case law has ruled on certain decisions adopted using AI tools, setting out the conditions for their validity. In a number of cases from 2017 and 2019, which concerned the use of a programme (AERIUS) that employed an algorithm to calculate nitrogen deposits, the courts held that, in order to prevent unequal treatment between proceedings concerning the calculation of such deposits, the administration was required to disclose its decision to use an algorithm, along with the data and assumptions employed, and to do so of its own accord and in good time to enable the parties concerned to access that data, assess it and, if necessary, challenge it in court, thereby ensuring an effective right of defence and enabling the courts to review the contested decisions.

There are, furthermore, a number of precedents relating to AI concerning applications used in the field of asylum law: in particular, in a 2025 ruling—albeit in an *obiter dictum*—the District Court of The Hague affirmed the Ministry's obligation to specify,

in its decisions, that these were based on automated systems; some decisions were consequently set aside by the courts on the grounds that the reasoning failed to specify that an AI system had been used and how. In other cases, mainly concerning illegal immigration, decisions were challenged on the grounds of the use of AI systems, but this was deemed implausible by the Court, in light of the reasoning provided by the administration, which indicated the contrary. In another case, where a decision had been challenged on the grounds that it had been taken on the basis of an AI system, the Court dismissed the appeal as the Ministry had demonstrated in court how that system had been used, and that it had not had any discriminatory effects.

Furthermore, in a 2024 ruling, Dutch case law held that certain automatically generated decisions concerning the granting of health service benefits could be attributed to human intervention. In these cases, the granting of the benefit stemmed from the AI system, which processed certain data and information that had been entered into the system through human intervention: for this reason, the Court held that the automated decision was attributable to a human decision-maker.

In **the United Kingdom,** too, the courts have ruled on this matter on several occasions.

A number of previous cases have shown that automated decisions must comply with the principle of rationality: this principle was affirmed in a 2020 judgement which ruled that a system was unlawful because it failed to pay certain social security benefits to some individuals who were entitled to them, solely on the grounds that they did not always receive their wages on a specific day of the week. The administration argued that the payment process was fully automated and that it was not rational to take the same pay day into account for all individuals. The English court deemed such a system irrational and detrimental to the individuals concerned.

In another ruling from 2020, the illegality of facial recognition systems used in public spaces to identify individuals wanted by the police was affirmed. In particular, this system was deemed unlawful because it left a margin of discretion to police officers (regarding whom to search for and where to place the devices). In the same ruling, the illegality of AI systems leading to discrimination, victimisation and persecution was also noted: in the case in question, the Court found not that the system was malfunctioning, but that it was prone to *bias*, in particular by mistaking people on the basis of race or gender.

In a 2018 precedent, the English courts ruled that a decision by a public authority to refuse access to the algorithm used to calculate financial assistance was unlawful.

There are no precedents in the United Kingdom in which the possibility of a public authority delegating decision-making power entirely to an algorithm has been discussed. The delegation of powers between human bodies is permitted within certain limits, but it cannot be assumed that these limits also apply to a delegation to an AI tool. It is also emphasised that, in cases where advanced AI systems, such as generative AI, have been used, effective *disclosure* may require access to the source code; however, this issue has not yet been addressed by English case law.

In **Slovakia**, a 2024 precedent ruled that judicial activity cannot be entrusted to AI tools, which can serve only as an aid. The Supreme Court stated in 2016 that, in a state governed by the rule of law, the entrusting of administrative decisions to technological systems cannot be done without a sufficiently detailed legal basis and on the condition that the conclusion can always be reviewed by a human being.

Furthermore, in 2019, the Slovak Constitutional Court stated in an *obiter dictum* that the use of automated systems by a public administration presupposes compliance with all constitutional guarantees; however, an automated decision cannot remain impersonal and without justification. The use of algorithms to generate suggestions or proposals should follow a specific organisational decision by the public authority, subject to public debate and subsequently authorised by the legislature. According to the Court, the lack of national regulation suggests that there is currently no legislative approval for the use of AI systems for the purposes of administrative decisions. It follows from this case law that: the use of AI systems or algorithms should be defined in detail by law, in accordance with the principle of legality; human oversight must be ensured; such decisions must be adequately reasoned and subject to review; judicial review remains subject solely to the Constitution and the rules in force; public administrations should also act in accordance with the Constitution and within the limits established by law, in particular those relating to the use of AI tools.

In **Spain,** case law has begun to recognise the legitimacy of automated administrative decisions, particularly in relation to the transparency and traceability of the AI systems used to make such decisions. Recent rulings have granted access to the source code of applications used by the public administration, as in the 2025 case concerning the BOSCO programme, used by the Ministry for Ecological Transition. These decisions have sparked public debate and drawn attention to the importance of transparency and the explainability of algorithms.

Limits of the judicial review that the competent court may exercise over automated administrative acts - The questionnaires reveal that in almost all Member States, in the absence of specific rules, the judicial review that can be exercised over automated administrative decisions is subject to the same limits that generally characterise the review of administrative acts.

Access to the algorithm, or other AI tools, and judicial protection: scope and limits - Reference is made to the points raised in the preceding paragraphs.

Session 3 The Administrative Judge and the Use of Artificial Intelligence

3.1 National Legislation and Implementation of Regulation (EU) 2024/1689

Constitutional principles and national legislation on judicial process automation - None of the jurisdictions that responded to the questionnaire provides for explicit constitutional principles governing the automation of judicial proceedings. This is readily explained by the fact that constitutional texts, including those adopted relatively recently (such as those enacted in the early 1990s), nevertheless date from periods in which the use of artificial intelligence in support of judicial functions remained a remote prospect.

The absence of an express constitutional framework enhances the interpretative role of the judiciary, which is required to derive the relevant principles from the constitutional order by reference to the guarantees of a fair trial, the protection of fundamental rights and the independence of the judiciary. In **France**, of particular interest in this regard is the already substantial body of case-law of the *Conseil constitutionnel* - beginning with *Decision No 2018-765 DC of 12 June 2018* - which, through the constitutional principles governing the protection of personal data, has indirectly outlined the legal framework for the use of artificial intelligence in judicial proceedings, placing particular emphasis on the protection of privacy, the principle of proportionality and the corresponding procedural safeguards.

At present, moreover, the information provided through the questionnaire indicates that only a limited number of jurisdictions have adopted dedicated national legislation on artificial intelligence. Examples include **Finland**, with the *Act on the Supervision of Certain Artificial Intelligence Systems*, and **Slovenia**.

Italy has likewise enacted a general legislative framework on artificial intelligence (Law No 132 of 2025), which contains a specific provision governing the use of AI systems in judicial activity (Article 15). That provision reflects, and gives effect to, the principles laid down in Regulation (EU) 2024/1689 (Artificial Intelligence Act, hereinafter the "AI Act"). Proceeding from the classification of judicial AI systems as high-risk, Article 15 provides that, where AI systems are used in judicial activity, *all decisions concerning the interpretation and application of the law, the assessment of facts and evidence, and the adoption of judicial decisions shall remain exclusively reserved to the judge.*

Different approaches to the implementation of Regulation (EU) 2024/1689 – Regulation (EU) 2024/1689 (AI Act) establishes a common minimum regulatory framework for the Member States of the European Union. Owing to its horizontal scope, however, it is not specifically designed to regulate the use of artificial intelligence by judges, and in particular by administrative courts. It therefore requires implementation through national measures. The only provision directly relevant in this context is Annex III, point 8(a), which classifies as high-risk *AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution.*

The responses demonstrate that the Member States of the European Union are following different approaches to the implementation of Regulation (EU) 2024/1689. The regulatory landscape remains, however, in a state of development. In particular, the Digital Omnibus on AI, approved on 29 June 2026, postponed the application of the obligations relating to AI systems classified as high-risk in the administration of justice from 2 August 2026 to 2 December 2027. Furthermore, none of the jurisdictions surveyed has, to date, referred questions to the Court of Justice of the European Union concerning the interpretation or validity of the AI Act.

Some Member States have opted to implement the AI Act through primary legislation. This is the case for **Denmark**, **Italy** and **Slovenia**. In **Germany**, **Hungary**, **Spain** and **Sweden** legislative proposals intended to implement the Regulation are currently under parliamentary consideration.

Other jurisdictions have chosen, at least for the time being, to implement Regulation (EU) 2024/1689 in the judicial sector through soft-law instruments. **Croatia, Estonia** and **Latvia** provide examples of this approach. In several instances, the preparation of such instruments has been entrusted to the supreme courts themselves. In **France**, the *Conseil d'État* adopted, in 2025, a Charter governing the use of artificial intelligence, reaffirming both the central role of the judge and the necessity of human oversight. In **Latvia**, the Supreme Court adopted internal rules in August 2025 governing the use of artificial intelligence and online tools. Likewise, in **Portugal**, the *Conselho Superior dos Tribunais Administrativos e Fiscais* adopted the *Carta ética para a utilização da inteligência artificial nos tribunais administrativos e fiscais* (Ethical Charter on the Use of Artificial Intelligence in the Administrative and Tax Courts). **Sweden** has also opted for the use of guidelines, entrusting their development, however, to the Domstolsverket (the central government authority responsible for administrative support, coordination and funding of the Swedish judicial system).

In **Spain**, the use of artificial intelligence systems in the exercise of judicial functions has likewise been regulated through instructions issued by the judicial self-governing body (Instrucción 2/2026 - BOE-A-2026-2205 Acuerdo de 28 de enero de 2026, del Pleno del Consejo General del Poder Judicial).

A sector-specific regulatory approach based on soft-law instruments has likewise been adopted in certain non-EU jurisdictions. **Switzerland**, for example, is moving towards the adoption of non-binding measures in implementing the Council of Europe Framework Convention on Artificial Intelligence, to which it is a Party. Similarly, in **the United Kingdom**, official guidance - *AI Guidance for Judicial Office Holders* - has been issued for judicial office-holders reporting to the Lady Chief Justice and the Senior President of Tribunals. **Serbia**, too, following the adoption of guidelines in 2023, established a working group within the Ministry of Science, Technological Development and Innovation to prepare a draft law on the matter, which will also take into account the provisions of the AI Act. In **Ukraine**, in September 2024, the judicial self-governing body approved an amendment to the Code of Judicial Ethics (Article 16), defining AI as a merely auxiliary tool. Subsequently, the Council of Judges of Ukraine adopted, by Decision No. 14 of 2 March 2026, provisions implementing these principles. The Secretariat of the Supreme Court of Ukraine, on the other hand, adopted, on 8 December 2025, provisions applicable exclusively to administrative staff.

This significant diversity of regulatory approaches to the use of artificial intelligence in support of judicial functions carries the risk of an increasing divergence in judicial practice. Such divergence can be contained and effectively managed only through the development of a common culture of digital justice and the strengthening of international judicial cooperation.

3.2 Use Cases and Ongoing Pilot Projects

The complexity of the framework described above is reflected in the practical ways in which artificial intelligence is being used in support of the judicial function.
These approaches vary significantly from one jurisdiction to another, including within the European Union legal order. The questionnaire nevertheless identified certain underlying common trends.

First, none of the legal systems examined permits the use of AI as a substitute for the judge. Rather, a model is emerging whereby AI is used in a supporting and preparatory capacity (see, for example, the aforementioned *Carta ética para a utilização da inteligência artificial nos tribunais administrativos e fiscais* adopted by the *Conselho Superior dos Tribunais Administrativos e Fiscais* and the *Charte d'utilisation de l'intelligence artificielle au sein de la juridiction administrative* adopted by the French *Conseil d'État*). The principle that human contribution cannot be replaced in the exercise of judicial functions has also occasionally been affirmed in domestic case-law. This is the case, for example, in Slovak case law (*Regional Court of Trenčín*, 19CoPr/2/2024), which held that the use of artificial intelligence can be beneficial in judicial activities but cannot replace the intellectual activity of a judge, whose task is to decide on individual disputes while taking fully into account all the contexts and nuances of a particular case.

AI use cases supporting judicial functions – Subject to this general approach, the specific uses of AI that are permitted and currently practised vary considerably.

A significant number of jurisdictions currently use AI only for purely ancillary administrative activities, such as searching for precedents or the pseudonymisation of judicial decisions (for example, in **Greece**, through the enhancement of the OSDDY-PP system, **France** and **Italy**, as well as, outside the European Union, **Albania** and **Switzerland**, through the ChatTF project, which also enables the translation and summarisation of decisions), or for identifying related proceedings (as in **Portugal**). Such applications do not, however, qualify as "high-risk" uses under the AI Act, pursuant to recital 61 of that Regulation, since they do not affect, even indirectly, the decision-making process.

National regulatory approaches diverge more significantly when considering the possible uses of AI in relation to the adjudication of disputes themselves.

In some jurisdictions, at least from a regulatory perspective, the use of AI systems is permitted both for legal research and interpretation and for the assessment of facts. This is the case in **Denmark** and **Italy**, where such use is expressly authorised under Article 15 of Law No. 132 of 2025. In other jurisdictions, such as **France** and **Latvia**,

the use of AI is envisaged solely for identifying the applicable legal framework, particularly through the identification and analysis of relevant case law.

Ongoing pilot projects – Several official pilot projects are currently being conducted directly by judicial institutions. These include, in France, the Jacepair project, aimed at using AI to assist in identifying the applicable law, and, in **Portugal**, the AssessorIA project, initiated by the *Conselho Superior dos Tribunais Administrativos e Fiscais*. The latter is designed to support judges during the decision-making process by preparing case-specific reports and summaries of procedural documents, structuring draft judgments, and identifying and verifying relevant factual elements.

The use of generative AI – A separate issue concerns the use of generative AI tools, namely the possibility of employing AI for the drafting of judicial decisions. None of the jurisdictions surveyed has introduced an express statutory prohibition in this respect. In practice, their use is generally left to the discretion of the individual judge (as, for example, in **the Czech Republic**), who remains fully responsible for reviewing and validating any draft produced.
In certain cases, such as **the Netherlands**, the use of generative AI for drafting judicial decisions is prohibited through internal court guidelines. In others, such as the Supreme Court of **Norway**, consideration is being given to introducing specific limitations on its use, again through guidelines. In **Germany**, the use of generative AI is expressly accepted in practice, as reflected in the document *"Strategy for the Use of Artificial Intelligence in the Judiciary. Coordinating the Development, Purchasing and Use of AI Systems in the Judiciary. Version 1.0 – April 2025"*, adopted at the meeting of the E-Justice Council of 2 April 2025. This document refers to the use of AI for the purpose of "support of action" (*Handlungsunterstützung*). In **Poland**, the use of publicly available generative AI systems is also permitted, on the basis of internal guidelines, but subject to a prohibition on using documents containing personal data, including correspondence with the parties to the proceedings.

It is also worth noting that, in **Italy**, although no express statutory prohibition exists concerning the use of generative AI, administrative case-law has addressed the improper use of such tools by legal professionals. In its judgment of 21 October 2025, No 3348, the Regional Administrative Court of Lombardy (TAR Lombardia - Milano) penalised the inappropriate use of AI tools by ordering the payment of additional procedural costs, following the submission of an application containing irrelevant legislative provisions and case-law references generated through the use of such technology.

3.3 Safeguards Governing the Use of AI

Despite the variety of approaches adopted, the different models for the use of AI in support of the judicial function are generally accompanied by safeguards concerning transparency, robustness, accuracy and, above all, human oversight.

As regards the first aspect, some jurisdictions impose, for example, an obligation to inform users of the justice system where artificial intelligence tools have been used to decide a specific case (for instance, in **Latvia**).

With regard to robustness and accuracy, internal regulatory frameworks frequently require the adoption of specific organisational measures. In **Italy**, for instance, Article 3 of Law No 132/2025, implementing in general terms Articles 13 and 15 of the AI Act, provides that the development of artificial intelligence systems and general-purpose AI models must be based on data and processes whose validity, reliability, security, quality, suitability and transparency are ensured and monitored, in compliance with the principle of proportionality depending on the sectors in which such systems are deployed.

Some jurisdictions already have specific legislation in place to ensure the robustness of the systems employed. In particular, **Estonia** has adopted the "Estonian Information Security Standard (E-ITS)" with the aim of enhancing the level of cybersecurity in the public sector. It provides for a risk assessment mechanism covering, among other things, the transparency of the system's operation and the comprehensibility of its outputs.

In other jurisdictions, such as **Germany**, in the draft legislation submitted in March 2026, and **the Netherlands**, the definition of standards relating to the robustness and accuracy of AI systems is essentially entrusted to the regulatory framework established by the relevant sectoral authorities.

Spain, even before the adoption of the AI Act, had already put in place a specific regulatory framework on safeguards governing the use of AI, which anticipates, in certain respects, the European framework. In particular, under Royal Decree 817/2023, a controlled testing environment was established for the testing of artificial intelligence systems, with particular attention to those classified as high-risk due to their potential impact on fundamental rights. Annex II to that Regulation explicitly includes systems intended for use by a judicial authority, entrusting the Secretary of State for Digitalisation and Artificial Intelligence with the task of assessing compliance with the requirements arising from the European Regulation during testing and experimentation, in accordance with the requirements applicable to conformity assessment bodies.
Furthermore, in the area of transparency, the Plenary of the State Technical Committee for Electronic Judicial Administration (CTEAJE) adopted a specific policy governing the use of AI, providing, among other things, for the collection and analysis of data generated by algorithms in order to assess their performance, identify possible biases, errors or undesirable behaviour, and ensure transparency and accountability.

Outside the European Union framework, **the United Kingdom** has developed an *Algorithmic Transparency Recording Standard* ("ATRS"), which enables public sector organisations, including the Ministry of Justice, to publish information on the algorithmic tools they use and the reasons for their use. The obligation to publish an ATRS document applies to algorithmic tools that have a significant influence on a decision-making process affecting the public or that interact directly with the public.

Guarantee of human oversight – Human oversight is ensured through a combination of organisational measures and requirements relating to the individual responsibility of judges. Organisational safeguards include, for example, arrangements whereby

access to AI tools is centrally managed by the internal court structure responsible for IT services, as in **Latvia**, in order to enable intervention in cases of inappropriate use.

In **Italy**, Article 15(1) of Law No 132/2025 expressly provides that the use of artificial intelligence systems in the exercise of judicial functions may take place only in an ancillary and supportive capacity, while the judge retains full decision-making power and the corresponding responsibility at all times. The software is authorised solely to formulate proposals concerning the interpretation and application of the law or the assessment of facts. Such proposals are submitted to the judge for examination, and it remains for the judge to decide whether or not to adopt them.

In **Spain**, the national supervisory authority for artificial intelligence - the *Agencia Española de Supervisión de la Inteligencia Artificial*, established pursuant to the AI Act - has issued specific guidance (*Guía vigilancia humana*) which also applies to the use of AI systems in the judicial sector.

Mitigating automation bias and judicial training – The issue of human oversight, and in particular its effectiveness in practice, is closely linked to the need to adopt measures aimed at mitigating the phenomenon of automation bias.

Also following the impetus provided by Regulation (EU) 2024/1689 (Article 14(4)(b)), several jurisdictions, including **Bulgaria**, have introduced AI literacy programmes specifically addressed to judges.

In **Germany**, for example, the German Judicial Academy (*Deutsche Richterakademie*) and the Federal Academy of Public Administration (*BAköV – Bundesakademie für öffentliche Verwaltung*), the central federal training institution, provide courses on artificial intelligence. Consideration is also being given, pursuant to Article 4 of Regulation (EU) 2024/1689, to making at least one basic AI training course offered by the Federal Academy of Public Administration compulsory.

Similar initiatives are currently being organised by the Judicial Academy of **the Slovak Republic** and by the Research Office of the Italian Administrative Justice System, also in compliance with Article 15 of Law No 132/2025.

Romania has planned specific training initiatives on the subject for 2026, including training on the use of a specific application (MindApp) as a tool for psychological support, assessment and testing within the judicial system.

In the absence of coordinated initiatives, there is a risk that, despite a shared commitment to common principles and values—first and foremost, the continued central role of the human judge—a common operational judicial culture regarding the use of AI may fail to develop. The establishment of a permanent forum among participating jurisdictions on this subject would therefore be particularly valuable, with the objective of developing and promoting common guidelines.