Observatoire ARGA

ARGA Atlas

ARTIFICIAL INTELLIGENCE, JUDICIAL SYSTEMS AND DUE PROCESS: AUTOMATED DECISION-MAKING AS A NEW RISK TO JUSTICE

Authors:

Sergei Khrabrykh — President of ARGA, PhD

Tsmakalova Nataliia

Organization: Observatoire ARGA, ARGA Atlas

Mailing address: 21 route de l'Aviation, 12 C, 64600 Anglet, FRANCE

Contacts: info@argaobservatory.org, +33 7 58 49 62 27

Website: www.argaobservatory.org, https://www.arga-atlas.com/

Anglet, 2 may 2026

Purpose of the Document

This report has been prepared to analyze how artificial intelligence systems and other automated tools are used in judicial and law-enforcement activities and to identify the legal risks arising from their application. Particular attention is given to the impact of algorithmic models on the right to a fair trial, the presumption of innocence, the right to effective legal defense and the principle of independent assessment of evidence.

The practical purpose of this document is to identify situations in which automated assessments, predictive models, data-analysis systems, digital filtering tools and algorithmic recommendations begin to influence procedural decisions in practice. This may affect decisions concerning pre-trial detention, risk assessment, case allocation, evidence review, migration procedures, financial monitoring and other areas where decisions directly affect fundamental rights.

For ARGA, this topic is of strategic importance because in international matters involving extradition, international alerts, sanctions, compliance and financial investigations, digital systems are increasingly used to generate conclusions regarding risk, reliability, likelihood of misconduct and the alleged necessity of restrictive measures. Where transparency is insufficient, such tools may amplify errors and significantly hinder effective legal protection.

This report examines the use of artificial intelligence as part of the broader relationship between technological efficiency and procedural safeguards. Its purpose is to develop a practical analytical framework suitable for lawyers, courts, regulators, human rights organizations and compliance professionals.

CONTENTS

Executive Summary

Artificial intelligence and automated data-analysis systems are increasingly being integrated into judicial, law-enforcement and administrative practice. They are used to predict risks, prioritize cases, identify suspicious transactions, analyze documents, estimate the likelihood of future misconduct and generate recommendations for decision-makers.

These technologies can improve efficiency and reveal complex patterns within large volumes of information. At the same time, they create significant legal risks. Algorithmic models may rely on incomplete or biased data, use opaque criteria and reproduce errors that are difficult to detect and challenge.

A particularly important issue is that, although decisions are formally taken by human officials, automated recommendations may substantially influence their conclusions. As a result, algorithmic outputs may be treated as objective and neutral, even though they are products of specific models trained on limited datasets and shaped by institutional assumptions.

The central conclusion of this report is that the use of artificial intelligence in justice should be regarded not merely as a technological issue, but as a matter of fundamental procedural guarantees. Any system that materially affects decisions concerning individual rights must be subject to scrutiny in terms of legality, transparency, explainability, proportionality and effective challenge.

Context & Problem Statement / Why This Topic Has Legal and International Significance

The use of artificial intelligence in judicial and administrative processes is no longer a theoretical prospect. Algorithmic systems are employed to allocate cases, analyze case law, identify suspicious transactions, assess the likelihood of unlawful conduct, sort documents and generate recommendations for officials. In a growing number of situations, these tools have a direct impact on decisions affecting liberty, property, business reputation and other fundamental rights.

Particular significance attaches to the use of automated systems in criminal proceedings, migration and asylum procedures, financial monitoring, sanctions compliance and international legal cooperation. Algorithmic models may be used to assess the risk of reoffending, absconding, non-compliance or suspicious financial activity. If the resulting assessments are accepted without adequate scrutiny, a technological tool may effectively become a source of legal consequences.

The central concern is not the use of technology as such, but the tendency to treat automated outputs as more objective than human judgment. In practice, algorithms depend on the quality of the underlying data, the training methodology, selected parameters and the assumptions built into the model. Errors, statistical distortions and hidden biases may lead to systematic reproduction of inaccurate or unfair outcomes.

The importance of this issue is international in scope. States, international organizations, banks, digital platforms and private analytics firms are increasingly deploying algorithmic tools. Their outputs are used in extradition matters, asylum cases, sanctions decisions, asset freezes, banking restrictions and compliance reviews. As a result, individuals may face serious consequences without receiving full information about how the relevant conclusions were generated.

For ARGA, this topic is particularly significant because effective legal defense in cross-border matters requires the ability to analyze not only legal arguments, but also the technical systems that influence decision-making. As artificial intelligence becomes more deeply embedded in legal and regulatory processes, the right to due process increasingly depends on the transparency and verifiability of algorithmic systems.

Legal Framework / Normative and Institutional Framework

The legal regulation of artificial intelligence in the field of justice is developing at the intersection of human rights law, procedural guarantees, data protection, administrative law and specialized legal instruments governing digital technologies.

The European Convention on Human Rights provides the core normative framework. Article 6 guarantees the right to a fair hearing, including equality of arms, independent adjudication and the opportunity to challenge evidence. Article 8 protects the right to respect for private life, while Article 13 guarantees an effective remedy. Where automated systems affect ownership interests, Article 1 of Protocol No. 1 may also be engaged.

Within the European Union, particular importance attaches to the General Data Protection Regulation (GDPR), the Artificial Intelligence Act and sector-specific legislation governing the use of digital systems in both public and private contexts. These instruments emphasize transparency, data quality, human oversight and specific obligations applicable to high-risk systems.

Additional guidance is provided by Council of Europe instruments, materials of the European Commission for the Efficiency of Justice (CEPEJ), OECD principles and United Nations documents concerning the use of digital technologies in a manner consistent with human rights.

At the national level, criminal, civil, administrative and procedural laws regulate the admissibility of evidence, the use of automated systems, the duty to provide reasons and the scope of judicial review.

Private institutions also play an important role. Banks, digital platforms, analytics providers and compliance departments increasingly rely on algorithmic models to assess risk and make decisions. Although these processes are formally private, their consequences may directly affect fundamental rights and economic interests.

Accordingly, the use of artificial intelligence in judicial and related processes is governed not only by technical standards, but by fundamental principles of legality, transparency, explainability, proportionality and effective judicial protection.

Mechanisms of Practice / Abuse / Key Mechanisms of Practice, Abuse or Conflict

Artificial intelligence is used in legal and administrative systems in a variety of ways. In some cases, algorithmic tools perform an auxiliary function by organizing documents and analyzing large datasets. In other cases, they generate recommendations that substantially influence the final decision. The greater the reliance on automated outputs, the more significant the legal implications become.

One of the principal mechanisms is algorithmic risk assessment. Such models are used to estimate the likelihood of reoffending, absconding, violation of migration rules, suspicious financial activity or other events. The resulting score may influence decisions concerning detention, enhanced monitoring, further investigation or the application of restrictive measures.

Another mechanism is automated sorting and prioritization of cases. Systems may determine which matters receive heightened attention, which applications are processed first and which documents are subject to additional review. While such tools are intended to improve efficiency, they may materially affect the allocation of institutional resources and the intensity of scrutiny.

Artificial intelligence is also used to analyze documents and identify patterns. Systems may compare texts, extract key information, detect links between persons and events and generate analytical summaries. Without adequate review, preliminary outputs may be treated as established facts rather than working hypotheses.

A particularly important mechanism is the integration of algorithmic systems into private procedures of banks, digital platforms and analytics providers. Assessments of clients, transactions or projects may be based on automated models whose outputs are used to block operations, deny services or transmit information to competent authorities.

Potential abuse arises where algorithmic conclusions are relied upon without meaningful disclosure of methodology, without the possibility of verifying the underlying data and without an effective mechanism for challenge. In such circumstances, an automated system becomes a non-transparent factor capable of influencing decisions that affect fundamental rights and legitimate interests.

Case Patterns / Typical Scenarios and Models of Application

One common scenario is the use of algorithmic risk assessments in decisions concerning pre-trial detention, release conditions or the level of procedural supervision. A court or other authority may take into account an automated estimate of the likelihood of reoffending or absconding. If the methodology is not disclosed and subjected to meaningful scrutiny, the algorithmic output may exert an influence comparable to that of an independent item of evidence.

Another typical scenario arises in migration and asylum procedures. Automated systems may be used to sort applications, identify apparent inconsistencies in documentation and determine which cases should receive enhanced review. Errors in underlying data or inappropriate criteria may result in delays, refusals and other adverse consequences.

In financial monitoring and sanctions compliance, algorithms are employed to identify suspicious transactions, relationships between persons and indicators of heightened risk. On the basis of these outputs, transactions may be blocked, access to assets restricted and additional reviews initiated. Where transparency is limited, affected individuals may find it difficult to understand the reasons for the restrictions and to prepare targeted objections.

A further scenario concerns the analysis of digital evidence. Artificial intelligence may be used to process correspondence, contracts, banking records, case files and other large datasets. Although such tools can accelerate review, they do not eliminate the need for independent legal assessment and verification of the resulting conclusions.

Another significant scenario involves private decisions by banks, digital platforms and other institutions. Automated assessments may lead to account closures, refusal of service, operational restrictions or the persistence of adverse profiles even after the original concerns have been addressed.

Across all of these situations, the common risk is that a technological recommendation acquires the practical authority of a determinative finding, even though it remains an analytical tool dependent on data quality, model design and institutional context.

Risk Assessment / Main Risks and Legal Vulnerabilities

The principal risk is the opacity of algorithmic models. Individuals affected by automated assessments often have no meaningful access to information regarding the data used, the criteria applied or the reasoning by which the final output was generated. This significantly impairs the ability to challenge the result and to exercise the right to an effective defense.

A second major risk concerns the quality of underlying data. Incomplete, outdated, inaccurate or statistically unbalanced datasets may produce erroneous outcomes and systematically reproduce unfair or distorted conclusions.

A third vulnerability is excessive reliance on automated outputs. Judges, officials, banks and digital platforms may treat algorithmic recommendations as objective and neutral, without sufficient attention to the limitations of the model and the existence of alternative explanations.

A fourth risk is the transformation of probabilistic assessments into practical grounds for restrictive measures. A system may merely indicate a heightened statistical likelihood of a particular event, yet that output may lead to denial of services, enhanced monitoring, restricted access to assets or unfavorable procedural decisions.

A fifth risk is the persistence of adverse algorithmic profiles. Even after errors are corrected or the underlying circumstances change, internal databases and automated systems may continue to rely on outdated assessments, affecting future decisions.

A sixth risk is legal uncertainty. Judicial and administrative approaches to the admissibility, explainability and procedural treatment of algorithmic outputs are still evolving. This increases the importance of qualified legal and technical analysis in every case.

Institutional Gaps / Institutional Limitations and Systemic Weaknesses

One of the principal systemic weaknesses is that technological development is advancing more rapidly than the legal mechanisms designed to regulate and review automated decision-making. Algorithmic systems are being deployed before fully consistent standards exist for disclosure, methodological verification and procedural use.

A significant limitation is the insufficient technical expertise of many participants in the legal system. Judges, lawyers, regulators and administrative officials may not possess the specialized knowledge required to assess data quality, statistical models and the operational limitations of particular systems.

Another important concern is dependence on private developers and technology providers. Methodologies, software architectures and risk criteria are frequently protected as proprietary information, while access to the internal logic of the system may be restricted by claims of commercial confidentiality.

Information asymmetry remains a substantial obstacle. Institutions using automated tools often have far greater access to technical information and underlying data than the individuals whose rights are affected by the resulting decisions.

An additional weakness is the limited institutional capacity to correct errors promptly. Even where inaccurate data or unjustified conclusions are identified, updating records and restoring legal status may be delayed.

Taken together, these factors create an environment in which automated systems may exert significant influence over legal decisions despite the absence of fully developed safeguards ensuring transparency, verifiability and effective judicial control.

Practical Guidance / Practical Recommendations and Model of Legal Action

The first practical step is to determine whether an automated system has been used. In matters where conclusions concerning risk, reliability, suspicious activity or the likelihood of particular conduct play a material role, it is essential to establish whether algorithmic tools contributed to the decision and to what extent.

The second step is to request information about the model applied. Where possible, the affected person or legal representative should seek information concerning the type of system used, the data sources, general assessment criteria, methodological approach and the degree of human involvement in the final decision.

The third step is to verify the quality of the underlying data. It is necessary to determine whether the information relied upon is current, complete and accurate, and whether any errors exist in the identification of persons, transactions, documents or events.

The fourth step is to subject the model’s conclusions to critical review. Algorithmic outputs should be treated as analytical tools rather than independent proof. Their assumptions, statistical limitations and possible alternative explanations should be examined carefully.

The fifth step is to engage independent specialists where appropriate. In complex matters, experts in data analysis, digital technologies and statistics may be required to assess the reliability and significance of the automated conclusions.

The sixth step is to develop a procedural strategy grounded in transparency, explainability, legality, proportionality and the right to effective challenge. Where an algorithmic assessment materially affects an individual's rights, legal defense should seek full scrutiny of the system and its outputs by the competent authority or court.

Policy Recommendations / Recommendations on Legal and Institutional Approach

The use of artificial intelligence in judicial and related proceedings should be based on the principle that the final decision must always be made by a human decision-maker who bears full legal responsibility for its content and consequences. Automated systems may assist analysis, but they should never replace independent evaluation of evidence and circumstances.

A meaningful level of transparency should be ensured. Individuals whose rights are affected by automated assessments should be able to obtain information regarding the nature of the system used, the categories of data considered, the general assessment criteria and the extent to which the algorithm influenced the outcome.

Uniform standards should be developed to ensure the quality of data used to train and operate artificial intelligence systems. Inaccurate, outdated or biased datasets should not form the basis for decisions that restrict rights and legitimate interests.

Courts and regulators should treat algorithmic outputs as evidentiary material subject to full scrutiny rather than as automatically reliable technical results. The methodology, limitations and alternative interpretations of such outputs should be examined in every material case.

Effective mechanisms must exist to correct errors and restore legal status. Where an automated system generates an unjustified conclusion, affected individuals should have a practical opportunity to obtain correction of the underlying data, review of the assessment and removal of the resulting consequences.

The legal framework should preserve a balance between the use of technology to improve efficiency and the protection of fundamental procedural guarantees. The speed of data processing cannot justify lowering the standards of due process and effective judicial protection.

Automated Outputs, Databases, and Risk Assessment in Law Enforcement: Minimum Procedural Safeguards for the Use of AI and Algorithms

The expanding use of algorithms, scoring models, and digital databases in judicial, investigative, regulatory, and quasi-public procedures is reshaping the architecture of evidence and decision-making. In practice, an automated output ("high risk," "suspicious activity," "database match," "probable association," "anomalous pattern") frequently becomes the trigger for real legal consequences: search and detention, seizure and freezing of assets, denial of services or access, migration restrictions, enhanced procedural controls, or the initiation of investigative or accusatory scenarios. The central risk lies in the fact that a probabilistic machine-generated output begins to be treated as an established fact, while the source of error is displaced into a "black box" of data, settings, and modelling assumptions. At the same time, the digital environment accelerates the propagation of errors, while the "digital trace" of suspicion often outlasts institutional memory of any individual human decision.

As a practical matter, it is important to distinguish between: (a) admissibility, (b) evidentiary weight, and (c) sufficiency in the aggregate of automated materials. An algorithmic output may be admissible as a trigger for further inquiry or as one element of a broader evidentiary picture, yet carry diminished evidentiary weight and, as a rule, should not alone constitute a sufficient basis for an adverse measure absent independent and verifiable corroboration.

1. Mandatory Disclosure of the Basis (and Recording in the Case File): The Right to Know That a Decision Relies on an Algorithm, Database, or Scoring Model

The decision-making authority should record in the procedural document (and disclose to the affected party where appropriate):

· the fact that an automated system has been used (model, scoring mechanism, rule, matching database);
· the role of the system (investigative trigger, recommendation, evidentiary source, or factual basis of the measure);
· the consequences resulting from the use of automation.

Purpose of the Safeguard: without knowledge of automation and its role, it is impossible to challenge errors effectively, while courts are impeded in properly assessing admissibility, evidentiary weight, and sufficiency.

2. Separation of Three Levels: Data → Model/Rule → Legal Conclusion

Primary data (records, documents, logs, registries) should be methodologically distinguished from algorithmic processing (features, thresholds, rules, trained models), and in turn from legal characterization and measures.

Judicial reasoning should demonstrate which facts have been independently established and where probabilistic interpretation remains present. Legal conclusions should not be reduced to the formula: "the system assigned a high-risk score," detached from the individual circumstances of the case.

3. Verifiable Data Provenance and Dataset Quality (Data Governance)

Case materials should verifiably identify:

· the source of the data;
· the date and method of acquisition;
· access logs and records of modifications;
· rules governing updates and corrections;
· indicators of completeness and timeliness;
· known classes of error (duplicates, outdated records, mistaken identity, merged profiles, geographic, linguistic, or transliteration bias).

An error within a database should not automatically worsen a person's legal position. Where provenance and data quality are unverifiable, evidentiary weight should be reduced and the need for independent corroboration increased.

4. Transparency of Logic (Explainability): Not a "Formula," but Verifiable Meaning

Disclosure of source code is not always necessary. However, the following should be available, and reflected to a degree sufficient for meaningful review:

· a description of the logic applied (which factors are considered and how);
· trigger thresholds and their significance;
· limitations on applicability;
· sensitivity to data errors.

Where fundamental rights are affected, the statement "the system identified a risk" — without disclosure of logic, thresholds, and limitations — should be treated as material carrying reduced evidentiary weight and should not constitute the sole basis for an adverse measure.

5. Calibration of Reliability: Error Rates and False Positives

Authorities relying on scoring systems or algorithms should be prepared to substantiate known quality metrics, including false-positive and false-negative rates, validation procedures, monitoring for model degradation, and, where relevant, methods for detecting bias or discriminatory effects.

Where error rates are unknown or undisclosed, the sound approach is to treat the output as an investigative lead rather than as an autonomous basis for restricting rights.

6. Individualization and the Prohibition of "Automated Decision-Making": A Human Decision-Maker Remains Responsible

Even where AI is used, the final measure should result from independent human evaluation and contextual assessment. Individualized decision-making must not be replaced by a system threshold.

The responsible official should justify the applicability of the automated result to the particular person in light of individual circumstances and address material alternative explanations and objections. Reliance solely on a "high system risk score" without independent factual assessment should not be regarded as sufficient reasoning.

7. Adversarial Fairness: Access to Materials, Right to Counter-Verification, and Independent Expertise

Effective challenge requires:

· access to the minimum underlying data and parameters necessary for review (which records, matches, features, thresholds);
· the possibility of presenting an independent expert opinion;
· the opportunity to question a responsible representative concerning data, thresholds, error rates, applicability, and limitations.

Where secrecy, security, or commercial confidentiality constraints exist, balancing mechanisms may be employed (restricted expert access, redactions, closed hearings), but not total elimination of the possibility of meaningful review.

8. Correction Procedures: The Right to Correct Data and Remove the "Digital Trace"

Mechanisms should exist for:

· correction of inaccurate records;
· notation that data are disputed or under challenge;
· synchronization of corrections across systems and copies;

· restoration of status following exoneration or correction, so that a risk profile does not persist indefinitely without updated justification.

9. Proportionality and Graduated Consequences

Automated outputs should trigger consequences proportionate to their reliability and verifiability:

· low or unknown reliability → only limited, precautionary verification measures;
· stronger corroboration plus independent supporting evidence → potentially stricter measures;
· inability to verify in high-error-cost situations → prohibition or substantial restriction of use.

The less transparent and verifiable the result (data, methodology, error metrics), the lower its evidentiary weight should be and the more constrained its legal consequences must remain.

It should also be separately recognized that risks arise not only from scoring systems and databases but from the use of generative systems in drafting procedural documents. “Hallucinations” (including fictitious citations to case law or doctrine) may transform a text into a source of procedural error, while responsibility for source verification inevitably remains with legal representatives and parties. Consequently, where such tools have been employed, heightened importance attaches to disclosure of automation, verification of every factual and legal assertion, and preservation of adversarial scrutiny.

Concluding Formula

To ensure that algorithms and digital risk-assessment systems do not undermine procedural fairness, decision-making authorities should simultaneously ensure: disclosure of automation and its role, recorded in procedural acts; verifiable provenance and quality of data; explainability of logic, thresholds, and limits of applicability; known or at least assessable model error rates; adversarial fairness and genuine opportunities for counter-verification, including independent expertise; individualized human decision-making not displaced by “system thresholds”; effective mechanisms for correction of data and restoration of status; proportionality of consequences to uncertainty; and a clear distinction between admissibility, evidentiary weight, and sufficiency of automated materials when assessed cumulatively.

Conclusion

Artificial intelligence and automated data-analysis systems are becoming increasingly visible elements of modern judicial, law-enforcement, administrative and financial infrastructure. Their use may improve the efficiency of information processing, accelerate the identification of links between data and assist public authorities or private institutions in handling large volumes of material.

However, technological efficiency does not displace the requirements of due process. Where an automated output influences a decision concerning liberty, property, migration status, banking access, assets or another legally significant sphere, that output must be verifiable, explainable and open to challenge.

The principal danger is that an algorithmic assessment may acquire the practical authority of evidence without undergoing proper procedural scrutiny. In such circumstances, the affected person may face an adverse decision based on a model whose methodology is unknown, whose underlying data are not disclosed and whose correction mechanisms are limited.

For ARGA, the principal conclusion is that the use of artificial intelligence in justice and related procedures must be treated as a distinct field of legal protection. Defense strategies should include

analysis of data sources, model logic, the degree of human oversight, the availability of challenge mechanisms and compliance with basic guarantees of due process.

Technologies may be used within legal systems only where they do not replace independent judicial reasoning and do not deprive individuals of the ability to understand, verify and challenge the grounds of decisions affecting their rights.

Appendix A. Terminology

Artificial Intelligence. A software or technical system capable of generating outputs, recommendations, predictions or decisions on the basis of data, influencing subsequent actions by individuals or organizations.

Automated Decision-Making System. A system that fully or partially processes data and produces an output used in making a legally significant decision.

Algorithmic Risk Assessment. A model assigning a level of risk to a person, transaction, case or event on the basis of predefined parameters and input data.

Explainability. The ability to understand which factors influenced the system's output and how the relevant conclusion was generated.

Transparency. Availability of information concerning the nature of the system used, the data sources, the general logic of operation and the degree of influence on the final decision.

Human Oversight. The genuine ability of a responsible official to independently assess the output of an automated system, reject it and adopt a reasoned decision of his or her own.

Digital Profile. A set of data, conclusions and assessments generated in relation to a person, transaction or object through automated processing.

Algorithmic Bias. A systematic distortion of results arising from the quality of the underlying data, model design, selected criteria or historically embedded inequalities.

Effective Challenge. The ability of an affected person to obtain sufficient information about an adverse output, submit objections, request review and secure correction of an error.

Appendix B. Risk / Powers / Legal Consequences Matrix

Action	**Legal Risk**	**Legal Limitation**	**Possible Consequences**	**Practical Comment**
Use of algorithmic risk assessment	Giving probabilistic output the status of a factual basis	Risk assessment must not replace individual judicial or administrative review	Enhanced scrutiny, refusal, restrictive measure or adverse decision	Data, model criteria and the degree of influence on the decision must be examined
Automated sorting of cases or applications	Unequal allocation of attention and resources	Sorting must not result in hidden discrimination or denial of access to review	Delays, prioritization of some cases and practical marginalization of others	Prioritization criteria and review mechanisms should be analyzed

Use of a closed model	Inability to understand the basis of an adverse output	Commercial secrecy or technical complexity must not exclude the right of defense	Impaired ability to challenge and procedural inequality	Disclosure of general criteria, data sources and the role of the model should be sought
Use of inaccurate or outdated data	Creation of an incorrect digital profile	Decisions must be based on current, accurate and verifiable data	Misclassification, refusal of service or restriction of rights	Correction of data and reassessment should be requested
Use of algorithmic output in court	Formal acceptance of a technical result as evidence	The court must assess methodology, data sources and alternative explanations	Erroneous findings, inequality of arms and restriction of defense rights	Independent technical expertise and procedural challenge may be required
Automated assessment in banking or compliance context	Restriction of access to financial infrastructure without adequate explanation	Private risk assessment must not become an indefinite restriction of rights	Transaction blocks, account closure or persistence of adverse profiles	A documented position should be prepared and review should be requested
Persistence of an adverse digital profile	Continuation of consequences after an error is corrected	Data and assessments must be updated when circumstances change	Repeated restrictions, reputational harm and further refusals	Removal or updating of outdated information should be sought

This matrix reflects typical situations in which artificial intelligence and automated systems may generate legally significant consequences for individuals. Its practical purpose is to identify risk points in advance, require transparency and prevent individual legal assessment from being displaced by automated outputs.

Official Sources

European Union, Artificial Intelligence Act.

European Union, General Data Protection Regulation (Regulation (EU) 2016/679).

Council of Europe, Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.

Council of Europe, European Convention on Human Rights.

European Commission for the Efficiency of Justice (CEPEJ), European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment.

Organisation for Economic Co-operation and Development (OECD), OECD Principles on Artificial Intelligence.

United Nations, materials on human rights and digital technologies.

Office of the United Nations High Commissioner for Human Rights (OHCHR), materials on the right to privacy in the digital age.

European Court of Human Rights, case law concerning Article 6 of the European Convention on Human Rights.

European Court of Human Rights, case law concerning Article 8 of the European Convention on Human Rights.