Oxford Institute
of Technology and Justice

SPAIN

Tools	ADIA | Delfos | EPV-R | RisCanvi | Veripol | VioGén | Specialised systems
Tasks	Administrative support | Case management | Data review and analysis | Legal research, analysis and drafting support | Predictive analytics
Users	Law enforcement | Prosecutors | Courts | Defence
Scope	Nationwide
Training	No, but individual courses offered
Regulation	There is no single, comprehensive framework governing the use of AI in criminal proceedings, but several regulations include express references to the use of AI in the administration of justice, notably the EU AI Act, and the Royal Decree-Law 6/2023 of 19 December. The government has also issued guidance on the use of AI in the administration of justice (Policy on the Use of Artificial Intelligence in the Administration of Justice) and is in the process of adopting new legislation on AI.
Insights	In one study on the Basque Country's EPV-R tool (which assesses the likelihood that an individual may commit severe acts of domestic violence) found that the tool's ability to correctly identify high-risk cases was only 48%.

AT A GLANCE

In law enforcement, AI is used for predictive analytics, notably RisCanvi in Catalan prisons and VioGén for gender-based violence risk assessment, though both face transparency concerns. The police also piloted Veripol to flag false robbery reports, but it was discontinued in 2024 after EU regulatory changes. **Courts and prosecutors use AI for anonymisation, summarisation, and transcription**, while the defence relies on LexNET for document exchange with AI support. Training and oversight structures are emerging, including a judicial AI working group and digital competence frameworks.

Information uploaded as at September 2025. The material collected in this mapping tool is intended for general information purposes only and must not be used as a substitute for professional or legal advice. It is updated periodically but may not reflect the most recent developments. The Oxford Institute of Technology and Justice, the University of Oxford, the Clooney Foundation for Justice, and their representatives, as well as the law firms and lawyers that have contributed to this mapping tool make no guarantees or warranties regarding the accuracy or completeness of the information provided in the mapping tool and exclude liability for any loss or other result arising from any reliance placed on information presented in this mapping tool.

There is no single framework governing the use of AI in criminal proceedings but several regulations include express references to the use of AI in the administration of justice. This includes the Royal Decree-Law 6/2023 of 19 December, which permits the use of AI to support the preparation of judicial decisions, and the EU AI Act, which classifies AI systems used in the administration of justice and law enforcement as high-risk, subjecting them to strict obligations and safeguards. The Comprehensive Law 15/2022 on Equality and Non-Discrimination requires that algorithms used in decision-making processes in public administrations are transparent, minimise bias, and uphold accountability. The Organic Law 5/2024 on the Right of Defence also imposes transparency obligation for certain AI uses. The Spanish government has issued guidance on the use of AI in the administration of justice and is adopting new legislation on AI. Several regions have also adopted legal instruments for the responsible use of AI.

USE

As at August 2025, **Spain's Ministry of Justice is leading a major project to implement AI through the justice system**. This initiative is part of a broader government push for digitalisation and aims to streamline the processing of legal documents, using natural language processing to extract information from written documents. Technology and AI are being progressive incorporated into all phases of criminal proceedings, although their use is still being consolidated and remains subject to strict legal oversight.

LAW ENFORCEMENT

Predictive analytics

In Catalonia, '**RisCanvi**' is an algorithm used by prison administration to calculate the risk of an inmate committing a reoffence based on a series of weighted characteristics. The algorithm was initially intended to target reoffending among particular crimes, such as murder or sexual offences, but it has been expanded to include several types of offenders.

In Spain, a judge typically receives a report about a prisoner who is applying for parole that has information about where the inmate is housed and a history of their behaviour while in prison. Conclusions made by *RisCanvi* are included in this report. Inmates undergo interviews every six months where their collected data is then put into the system and reviewed by over 100 validators. The algorithm assigns each inmate a score on 43 risk factors across five different categories including level of education, history of violence, or mental health and addiction issues. They are then assigned a determinant of risk: red for high, yellow for medium and green for low. The risk determinants are used by prison professionals such as psychologists, social educators, and legal experts within the technical teams of penitentiary centers, although human oversight is retained. ***RisCanvi* has been fully deployed at the regional level in the Catalan prison system since 2010** and is regularly used in all centers managed by the Generalitat de Catalunya. Concerns have been raised about *RisCanvi*'s transparency.

> "RisCanvi is a system that is not known by those whom it impacts the most, inmates; that is not trusted by many of those who work with it, who are also not trained on its functioning and weights."
>
> *ETICAS, 2024*

A prevalent area of predictive analytics in Spain is in the context of **domestic gender-based violence**. The Spanish Secretary of State for Security has implemented '**VioGén**'(The Comprehensive Monitoring System in Cases of Gender Violence) under *Organic Law 1/2004* on Comprehensive Protection Measures against Gender Violence. VioGén is a risk-assessment tool used by the Spanish security forces and other entities involved in fighting against domestic gender-based violence. Though the system was first launched in 2007, a pilot scheme to improve the algorithm with AI was conducted in 2022. VioGén takes the form of a web application to exchange information on reported cases of domestic gender violence.

The VioGén system uses different police forms to collect the information needed to predict the risk of a perpetrators' recidivism:

Initial diagnosis: **Police Risk Assessment ('Valoración Policial del Riesgo') (VPR 4.0)**	The VPR form is used by police officers when a victim first reports an incident of gender-based violence. Through a series of standardised questions, the VPR categorises the risk levels of each reported case.
Follow up: **Police Evolution of the Risk Assessment ('Valoración Policial de Evolución') (VPER 4.0)**	The VPER form is used by the police, social services, and law enforcement to monitor the situation and update the risk-assessment on a regular basis. Along with the VPER, a Forensic Risk Assessment Form (VFR) permits a deeper and more nuanced risk-assessment, complimenting the VPER information. It is used by forensic professionals, providing additional insight, and supporting a more nuanced evaluation of each case.

The **Police Risk Assessment** (VPR 4.0) form includes 39 risk indicators, grouped into four thematic dimensions. Each indicator carries an empirical weight based on its predictive capacity for recidivism and serious violence. Actuatorial algorithms are used to calculate the level of risk: (1) low; (2) medium; (3) high; (4) extreme. The assessment result generated by the *VioGén* system may be adjusted upward at the end of each completed evaluation, based on the automatic classification and the judgment of police personnel.

The indicators are as follows:

CATEGORIES	FACTORS	RISK INDICATORS
(1) History of violence - assessment of the reported episode	1. Has there been any type of violence by the aggressor?	• Psychological violence • Physical violence • Sexual violence • Defensive reaction of the victim to the aggression
	2. Has the aggressor used weapons or objects against the victim?	• Use of weapons by the aggressor • Access to weapons by the aggressor
	3. Has the victim received threats or plans aimed at causing physical/psychological harm?	• Type of threat or plan directed by the aggressor
	4. Has there been an escalation in the severity and/or frequency of assaults or threats of violence in the last six months?	• Evolution of the history of violence in the couple in the last six months (increase in severity/frequency)
	5. Exaggerated jealousy, control and	• Exaggerated and irrational jealousy about the victim

Information uploaded as at September 2025. The material collected in this mapping tool is intended for general information purposes only and must not be used as a substitute for professional or legal advice. It is updated periodically but may not reflect the most recent developments. The Oxford Institute of Technology and Justice, the University of Oxford, the Clooney Foundation for Justice, and their representatives, as well as the law firms and lawyers that have contributed to this mapping tool make no guarantees or warranties regarding the accuracy or completeness of the information provided in the mapping tool and exclude liability for any loss or other result arising from any reliance placed on information presented in this mapping tool.

	harassment in the last six months	• Controlling behaviours over the victim (psychological/social/school/work, economic, cyber) • Harassment behaviour towards the victim
(2) Factors related to the aggressor	6. Has the aggressor shown any of these behaviours in the last year?	• Property damage against belongings or other objects • Disrespect for authority • Physical assaults on third parties and/or animals • Provocation, contempt, confrontation, threat or verbal aggression to third parties
	7. In the last six months, are there signs of problems in the aggressor's life?	• Stressors in the aggressor's life in the last 6 months
	8. Does the aggressor have criminal and/or police records?	• Police or criminal records • Physical and/or sexual assaults on third parties • Gender-based violence against other victim(s).

	9. Are any of the following circumstances present in the aggressor?	- Diagnosed mental and/or psychiatric disorder - Suicide attempts or ideation - Any type of addiction - Family history of gender or domestic violence
(3) Factors related to the vulnerability of the victim and the quality of the relationship?	10. Are any of the following vulnerability circumstances present in the victim?	- Recognised disability - Pregnancy - Serious physical illness - Foreign victim - Lack of family or social support network - Mental and/or psychiatric disorder - Suicide attempts or ideation - Any type of addiction - History of gender-based violence - Economic dependence on the aggressor - Has minors or relatives in her care
	11. Aggravating circumstances	- The victim has reported other aggressors in the past

		- Prior intention to end the relationship - Episodes of reciprocal violence - Fear for the integrity of minors or dependents
(4) Victim's perception of her situation	12. The woman believes that the aggressor is capable of assaulting her with great violence or even killing her	- Degree of awareness the woman has about the seriousness of her current situation

The **Police Evolution of the Risk Assessment** (VPER 4.0) form, used to reassess risk over time and adjust protective measures, contains 43 indicators, which are also grouped into thematic dimensions similar to the VPR.

They are as follows:

CATEGORIES	FACTORS	RISK INDICATORS
(1) History of violence - assessment of reported episode	1. Has there been any type of violence by the aggressor?	- Psychological violence - Physical violence - Sexual violence - Victim's defensive reaction
	2. Has the aggressor used weapons or objects against the victim?	- Use of weapons - Access to weapons
	3. Has the victim received threats or plans to cause harm?	- Type of threat or plan by the aggressor

(2) Factors related to the aggressor	4. Breach of judicial orders or penalties since last assessment	- Contact with victim despite restraining order
	5. Jealousy, control, and harassment in the last 6 months	- Irrational jealousy - Control behaviours (psychological, social, economic, cyber) - Harassment behaviours - Fugitive or unlocatable aggressor
	6. Fugitive or unknown whereabouts	- Fugitive or unlocatable aggressor
	7. Responsible behaviour since last assessment	- Distancing from victim - Peaceful attitude - Respect for law and cooperation - Remorse - Participation in support programmes - Compliance with separation and family duties
	8. Criminal or police records	- Criminal/police records - Violence against third parties

(3) Victim vulnerability and relationship quality		• Gender violence against other victims
	9. Other circumstances	• Diagnosed mental disorder • Suicidal ideation or attempts • Addictions • Family history or domestic/gender violence
	10. Victim obstructs police/judicial actions	• Resumes cohabitation • Refuses to testify or retracts • Engages in unsafe behaviours
	11. Victim vulnerability	• Recognised disability • Pregnancy • Serious physical illness • Lack of social/family support • Mental disorder • Suicidal ideation • Addictions
	12. Recent developments	• Economic dependence • Has dependents

		• Divorce/separation proceedings • New relationship not accepted by aggressor • Aggressor has new relationship • Aggressor has stable job/economy • Conflicts over child custody
(4) Victim's perception of risk	13. Victim's perception of risk	• Victim has an accurate perception of her own risk

The precise weighting assigned to each indicator is not disclosed. However, they are derived from empirical studies on recidivism, periodically adjusted with new data, and calibrated to maximise sensitivity while minimising false negatives. The overall score is calculated by summing the weighted presence of each indicator. This means that all relevant indicators contribute to the result, with their individual weights varying according to the empirical data obtained.

One of the **most criticised aspects** of *VioGén* is the **lack of transparency** of the algorithm on which the risk assessment is based. As at August 2025, the exact functioning of the *VioGén* algorithm and the databases it draws from remain undisclosed.

> "After conducting the audit, we can confirm that: VioGén is not transparent. We were unable to access any data or information about the system beyond what was produced by the experts involved in defining it. Neither external auditors nor women's groups have any access to VioGén data. For a publicly funded high-impact system like VioGén, this is unacceptable."
>
> *ETICAS, 2022 (unofficial translation)*

In January 2025, the Ministry of Interior launched the '**VioGén 2'** system. According to the Ministry, this new platform includes revised risk assessment forms and improved algorithm calibration (for more trustworthy and accurate predictions) **to determine risk levels more accurately**, thereby reducing the likelihood of assessment errors. However, as at August 2025 no further technical details have been disclosed.

In the Basque Country, the **EPV-R** (*Escala de Valoración del Riesgo de Violencia de Género, or Revised Intimate Partner Violence Risk Prediction Scale*) is a tool designed to **assess the likelihood that an individual may commit severe acts of domestic violence.** It was developed by a multidisciplinary team of professionals in criminology, psychology, and law enforcement, and is primarily used in police and judicial contexts to support decision-making regarding protective measures for victims of gender-based violence.

The EPV-R consists of 20 items grouped into five thematic blocks: personal data, relationship status, type of violence, aggressor profile, and victim vulnerability. Each item is scored from 0 to 3 based on its discriminative capacity (i.e. statistical weight in predicting the risk of severe violence). Not all items use the same scoring range. The total score ranges from 0 to 48, allowing cases to be classified into three risk levels: low (0–9), medium (10–23), and high (24–48).

The data used in the EPV-R tool was gathered through interviews made by the police. Once a report is filed at the police station by the victim, the police officer (after interviewing both the victim and the aggressor) applies the EPV-R scale to the aggressor and classifies the level of risk of severe assault into one of three categories: low, moderate, or high, based on the aggressor's score.

🔍 Closer look

The EPV-R tool has undergone empirical studies assessing its reliability and predictive accuracy. The original validation was conducted using 450 police case files from the Basque Country, showing that the tool was reasonably consistent with its results. However, the sensitivity of the scale (i.e. its ability to correctly identify high-risk cases) was relatively low (48%). Specificity was 81%, and diagnostic accuracy (ie. how often the tool gave the correct result overall) was 73%. In another study conducted in Mexico, however, the sensitivity of the EPV-R tool was stated to be 70%, with a specificity of 87% and a diagnostic accuracy of 79%.

Data review and analysis

In 2018, the Spanish National Police launched an AI-driven tool, '**Veripol**', to detect false robbery reports using natural language processing and statistical models. It processed police reports to identify linguistic patterns that could indicate deceit. It was among the earliest of its kind globally, developed in collaboration with Complutense University, Carlos III University, and other academic partners. **Veripol** was trained on a dataset of 1,122 true and false robbery reports from 2015. Natural language processing was used to process the text; words rarely or overly used were filtered out, and regression techniques identified which terms correlated with false and true claims. Words that tended to determine that the claim was false were: 'lawyer', 'security', 'day', 'insurance', and 'back'. Meanwhile, mentions of buses, license plates, or specific phone brands were more often associated with genuine reports.

In pilot tests in Málaga and Murcia in 2017, Veripol flagged false reports with high accuracy: **over 83% of cases identified as false ended with the complainant admitting to the falsity**. Between the tool's launch and October 2020, the tool analysed approximately 84,000 reports, identifying thousands as fraudulent (alongside other investigative methods). Use of

Veripol sharply declined by 2022, with just 3,762 reports processed that year and 511 flagged as false. In October 2024, shortly after the announcement of the *EU AI Act* (which classified similar systems as high-risk), the Ministry of the Interior officially ceased using *Veripol*, citing its lack of validity in judicial proceedings.

PROSECUTORS

Case management

The Ministry of Justice has implemented **'ADIA'** (Asistente de Documentos con IA), an AI application that is designed to optimise the processing of judicial documents through **two main functions: anonymisation and automatic summarisation.** This tool replaces or obscures personal identifiers, mitigating risks of misuse and enhancing data privacy. By late 2023, the anonymisation service was projected to be used approximately 20,000 times. The tool is available from the *SARA* internal network, which connects Spanish public administrations with European institutions, or through the internal platform known as Escritorio Integrado (accessible to judicial staff). *ADIA* is deployed nationwide.

As at August 2025, the Ministry of Justice is working to extend **Delfos**, the AI-based search engine mentioned below, within the Public Prosecutor's Office procedural management system.

Prosecutors also have access to the information available on VioGén, the risk-assessment tool mentioned above.

COURTS

Case management

The **ADIA** tool, discussed above, is available to and used by judicial staff.

The Ministry of Justice has developed a system that **transcribes judicial hearings**—including recorded testimonies and videoconferences—into text. This AI-driven tool enables legal professionals to search specific statements without reviewing entire recordings, significantly reducing time spent on case preparation. By April 2021, over 23,000 hearings had been transcribed, and it was reported that the system was available across 30% of the Ministry territory. The Ministry reported that transcription has saved 60% of time in search and location of key words, and has increased reliability, with over 80% accuracy in textualisation. The tool includes optional human oversight, allowing users to review, edit, or flag errors in the transcription when necessary. As at August 2025, the tool is being deployed nationally.

DEFENCE

Administrative support

'**LEXNET**' is a secure digital platform used by legal professionals in Spain to exchange documents and communications with judicial bodies. *LexNET* has incorporated AI functionalities for tasks such as automatic extraction of participant data in proceedings and intelligent classification of documents based on their content. Although the AI suggests and extracts information automatically, users can review, edit, or reject the extracted data, maintaining a high-level of human oversight.

Legal research, analysis and drafting support

Judges and prosecutors in Spain have begun gaining access to an AI-based search engine, entitled '**Delfos**', that allows them to query judicial documents and precedents using natural language. *Delfos* is in a pilot phase, and is integrated with Fortuny, a procedural file management system used in Spanish courts. Through that integration, legal users can query documents already within the procedural system. Users can also upload their own files and search for the necessary data. *Delfos* also offers document summarisation capabilities, automatically generating summaries of judicial documents.

TRAINING

Systematic AI training is **not currently available** for law enforcement, prosecutors, courts and defence in Spain. However, as at August 2025, within the framework of continuing education activities available to these professionals, **courses** on AI are offered, and conferences and seminars on the topics are regularly held.

In September 2024 the General Council of the Judiciary also established a **Working Group**dedicated to exploring how judges might use AI in their judicial functions. The Working Group's mandate includes, among other things, fostering training activities for the judicial career, ensuring judges understand AI tools and their oversight.

Finally, in 2023, the Centro de Estudios Jurídicos (CEJ) published the **Digital Competence Framework** for Justice Personnel, which outlines the key competencies that digital training programs should target. This framework includes a specific competency titled 'Robotic Process Automation and Artificial Intelligence Applied to Justice', which defines progressive levels of proficiency—from basic understanding of AI concepts and ethical principles to advanced use of AI tools in procedural management and the generation of draft judicial decisions.

REGULATION

There is **no single, comprehensive regulation governing the use of AI in criminal proceedings or in judicial proceedings**, more broadly, as at August 2025. However, several laws include express references to the use of AI in the administration of justice, notably the *EU AI Act*, and the *Royal Decree-Law 6/2023* of 19 December. The government issued guidance on the use of AI in the administration of justice and is in the process of adopting new legislation. In addition, several regions have adopted their own legal instruments that aim to establish ethical, technical, and governance conditions for the responsible use of AI.

AI REGULATIONS

The Royal Decree-Law 6/2023 of 19 December

The *Royal Decree-Law 6/2023* – which has implemented legal changes to modernise and digitalise the Spanish justice system – introduces the concepts of automated, proactive, and assisted actions within judicial procedures, which also apply to criminal proceedings.

Royal Decree-Law 6/2023 specifically permits the use of AI to generate ´a full or partial draft of a complex document' (defined as 'assisted action' in article 57) that may serve as 'a basis or support for judicial decisions', provided that it is subject to review and approval by the competent judicial authority. The Royal Decree-Law 6/2023 makes clear that, to constitute 'a judicial or procedural resolution', the final text must have been validated 'by the judge, magistrate, prosecutor, or lawyer of the Administration of Justice, [acting] within the scope of their respective powers and under their responsibility'.

Article 56 of the *Royal Decree-Law 6/2023* regulates 'automated actions', defined as procedural actions carried out by an appropriately programmed information system without the need for human intervention in each individual case. These may include simple procedural or resolution tasks that do not require legal interpretation, such as: (i) numbering case files; (ii) archiving cases when procedural conditions are met; (iii) generating copies and certificates; (iv) generating registers; (v) verifying legal representation; and (vi) declaring the finality of decisions, in accordance with procedural law.

Article 56 also regulates 'proactive actions', which are automated actions initiated by information systems without human intervention. These systems use data already incorporated into a case or administrative procedure for a specific purpose, generating alerts or direct effects for other purposes. Regarding both automated and proactive actions, article 56 establishes that judicial administration systems must ensure that such actions: (i) can be identified, traced, and justified; (ii) can be performed manually; and (iii) can be disabled, reversed, or nullified.

Article 58 of the *Royal Decree-Law 6/2023* sets out requirements for the management, supervision, quality control, transparency, and objectivity of these systems. There is, however, no obligation to disclose that AI was involved in the creation of a judicial or procedural resolution.

Judges have expressed concerns, particularly with regard to 'assisted actions' and calledfor 'a rigorous legal framework regarding [the] control, supervision and transparency [of AI]' in line with EU legislation 'since it involves high risk systems that could affect fundamental rights'.

> "Spanish judges are calling for legislation and demanding a high-level of transparency regarding the algorithm used, warning that 'whoever controls the algorithm, along with its biases, will influence the judicial decision, which can substantially affect judicial independence'."
>
> *XIX Conference of the Presidents of the High Courts of Justice, 2024*

EU AI Act (Regulation (EU) 2024/1689)

The *EU AI Act* – **the 'first-ever legal framework on AI'** – entered into force on 1 August 2024 and its provisions are applying gradually. Spain is obliged to implement and comply with the provisions of the Act, which set out a harmonised legal framework for the 'the development, the placing on the market, the putting into service, and the use' of AI systems across the EU.

The AI Act introduces a risk-based approach, categorising AI systems into four levels of risk, banning 'unacceptable-risk' systems, and imposing strict obligations on high-risk systems. The rules on prohibited uses have applied since 2 February 2025, while other obligations, including obligations related to the use of high-risk AI systems, are being introduced later.

The *EU AI Act* includes explicit references to AI systems related to the administration of justice, and to criminal proceedings. These are mainly classified as high-risk given 'their potentially significant impact on ... the rule of law, individual freedoms . . . the right to an effective remedy and to a fair trial' as well as the right to defence and the presumption of innocence, particularly if 'such AI systems are not sufficiently transparent, explainable [or] documented'. The Act highlights the potential 'difficulty in obtaining meaningful information on the functioning of those systems and the resulting difficulty in challenging their results in court, in particular by natural persons under investigation'.

Information uploaded as at September 2025. The material collected in this mapping tool is intended for general information purposes only and must not be used as a substitute for professional or legal advice. It is updated periodically but may not reflect the most recent developments. The Oxford Institute of Technology and Justice, the University of Oxford, the Clooney Foundation for Justice, and their representatives, as well as the law firms and lawyers that have contributed to this mapping tool make no guarantees or warranties regarding the accuracy or completeness of the information provided in the mapping tool and exclude liability for any loss or other result arising from any reliance placed on information presented in this mapping tool.

The EU AI Act's risk-based approach

Unacceptable risk *(prohibited)*

AI systems posing **'a clear threat to the safety, livelihood, and rights of people'** are **prohibited** under article 5. This includes uses in law enforcement and criminal justice such as: (i) assessing or predicting an individual's risk of committing a criminal offence based solely on profiling, personality traits, or characteristics; (ii) undertaking 'untargeted scraping of facial images from the internet or CCTV footage' to build or expand facial-recognition databases; and (iii) using 'real-time remote biometric identification' in public spaces, or biometric categorisation to infer race, religion, or other protected characteristics, although narrow exceptions exist.

High-risk *(subject to strict obligations)*

AI systems that **'can pose serious risks to health, safety, or fundamental rights'** are**deemed high-risk** under article 6. This includes the use of AI: (i) to assess the risk of persons 'becoming the victim of criminal offences'; (ii) to assess the risk of persons 'offending or re-offending' in certain circumstances, and to profile persons during investigations or prosecutions; (iii) to evaluate the reliability of evidence 'in the course of investigations or prosecution of criminal offences'; (iv) for remote biometric identification, biometric categorisation in certain circumstances, and emotion recognition; and (v) 'to assist judicial authorities in researching and interpreting facts and law' and 'applying the law to the facts'. AI systems used solely for ancillary administrative activities that do not affect the actual administration of justice in individual cases are not considered high-risk.

High-risk AI systems are not banned but are **subject to strict obligations** for developers, providers and users, due to their potential significantly to affect individuals' rights. The obligations include risk assessment, human oversight, the use of high quality training data, and ensuring explainability, accuracy, robustness, and cybersecurity. When AI systems assist judicial decision-making, the persons concerned must be informed about the use of AI systems and the role they play in the decision-making process.

Limited risk *(subject to transparency obligations)*

This category refers to the risk associated with a need for transparency around the use of AI such as chatbots. Specific disclosure obligations apply for this category.

Minimal risk *(no requirements)*

Minimal risk or no risk AI systems are not subjected to any requirements.

Royal Decree 817/2023 of November 8

Royal Decree 817/2023 creates a regulatory sandbox, which is a controlled and supervised environment where public and private entities can test AI systems—especially those considered high-risk—under real or simulated conditions. The goal is to evaluate how these systems align with the *EU AI Act*, allowing for experimentation, feedback, and refinement of technical and legal compliance before full implementation.

Regional initiatives

Regions such as Galicia, Extremadura, Asturias, Aragón, and, in development, Andalucíaand Castilla la Mancha, have also adopted legal instruments—whether laws, decrees, or administrative orders—that aim to establish ethical, technical, and governance conditions for the responsible use of AI. These regional regulations share a common inspiration in the principles promoted by Spain's *National Artificial Intelligence Strategy* and by the European Commission, such as human oversight, transparency, absence of bias, safety, privacy, and non-discrimination. However, while there is general alignment with national and European principles, the regional strategies differ in scope, level of regulatory development, degree of stringency, and implementation mechanisms. Their main purpose is to regulate the use of AI within the public administrations of their respective territories.

Information uploaded as at September 2025. The material collected in this mapping tool is intended for general information purposes only and must not be used as a substitute for professional or legal advice. It is updated periodically but may not reflect the most recent developments. The Oxford Institute of Technology and Justice, the University of Oxford, the Clooney Foundation for Justice, and their representatives, as well as the law firms and lawyers that have contributed to this mapping tool make no guarantees or warranties regarding the accuracy or completeness of the information provided in the mapping tool and exclude liability for any loss or other result arising from any reliance placed on information presented in this mapping tool.

GUIDELINES FOR PRACTITIONERS

Policy on the Use of Artificial Intelligence in the Administration of Justice

In June 2024, State Technical Committee for Electronic Judicial Administration (CTEAJ), an administrative body consisting of representatives of the Ministry of Justice, the General Council of the Judiciary, the Attorney General's Office and the Autonomous Communities, issued the *Policy on the use of Artificial Intelligence in the Administration of Justice (CTJAE Policy)*. This policy establishes 'a series of minimum criteria in order to ensure responsible, lawful and ethical use of Artificial Intelligence in the field of the Administration of Justice'. **It applies to any system or service that uses judicial data**—that is, data produced within the framework of judicial proceedings.

The *CTJAE Policy* clarifies that unauthorised AI applications must not be used and includes a breakdown of permitted and prohibited uses based on the type of data being processed and the purpose:

Permitted uses	Prohibited uses
(i) *Generally permitted* are uses that do not involve personal or confidential data, are for internal audiences only, and whose results are not used in judicial or administrative decisions (e.g., summarising extensive documents or translating text from a public source).	(i) Use of personal or protected data not covered by the permitted use cases, especially to generate information or documents that affect citizens' rights or obligations. This does not include the "generation of support documentation" for e.g., administrative decision-making, which is allowed with prior authorisation.
(ii) *Uses requiring formal management approval* include those involving non-sensitive data that may be used to assist citizens, professionals, or companies, based on data	(ii) "Automated reporting of the status and details of the procedures" to the parties

provided by them or uses involving protected data that support the organisation's activities, provided the service is offered by the administration itself or approved by the security department (e.g., "listening to phone calls" and summarising these as part of investigations). Similarly, AI may be used to "support analysis of difficult evidence",to detect patterns in images, generate document drafts and to "simplify legal texts".

(iii) U*ses requiring IT approval* include the generation of "a code to run on any device in the organisation".

concerned without previous human supervision.

(iii) Predicting "future behaviour of people" to base a judicial action such as a parole decision "on their personal history or people of similar characteristics"

(iv) Use of generative AI systems to replace necessary human presence in committees, meetings, or similar settings.

The Policy is guided by a set of **basic principles**, including the five principles established by the Council of Europe European Commission for the efficiency of justice (CEPEJ) in the *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment* as well as additional principles:

Respect for fundamental rights	Effective judicial protection, judicial independence, and fairness between parties must be guaranteed. AI must never replace human decision-making in crucial matters of justice. Decisions must be made by judges and magistrates independently.
Non-discrimination	AI must not be developed or applied in ways that result in discrimination based on sensitive data (racial or ethnic origin, socioeconomic status, political opinions, religious or philosophical beliefs, union membership, genetic or biometric data, health data, sexual life or orientation).

Quality and safety	Systems must be developed with input from professionals such as judges and researchers. Certified sources must be used, and processes must be traceable. Models and algorithms must be stored and executed in secure environments to ensure system integrity.
Transparency, impartiality, and fairness	Systems must be accessible, understandable, and auditable, avoiding bias and prioritising justice. Intellectual property rights must be balanced with these principles.
User control / human oversight	Judicial decisions must remain subject to prior human review. Citizens affected by AI systems must be informed whether the system's results are binding, whether they may be used in judicial proceedings, and of their right to object and be heard directly by the judicial authority.
Equity and universal access	Ensuring all citizens have equal opportunity to assert their rights before the law.
Bias and discrimination prevention	AI systems must be designed to prevent bias and be periodically evaluated.
Data protection and privacy	Data protection measures must be implemented, including prior impact assessments.
Responsible innovation and continuous evaluation	Periodic impact assessments and necessary adjustments must be made to ensure effectiveness and fairness.
Training and capacity-building	Stakeholders must be trained in the use of AI in the justice system.

Co-governance	Collaboration and knowledge-sharing across different areas of the justice administration must be promoted.

Moreover, the *CTEAJE Policy* requires compliance with applicable regulations and requires that results from generative AI are 'identified' as such.

CRIMINAL PROCEDURE RULES

Organic Law 13/2015 of October 5 amended the *Criminal Procedure Act (LECrim)* to regulate new technological investigative measures, which are set out in articles 588 bis to 588 octies of the LECrim. Although the law does not expressly address the use of AI, all the principles and limits established for technological investigative measures would apply if AI systems were implemented to reinforce such measures – as the law governing criminal procedure, any use of AI within criminal proceedings would in any case be subject to its rules. Article 588 bis LECrim establishes that the new technological measures set out cannot be used to prevent or detect crimes without an objective basis. In accordance with the principles of exceptionality and necessity, they may only be authorised when less intrusive measures are ineffective in protecting the fundamental rights of the person under investigation. All such measures must be authorised by a reasoned judicial decision, processed in a separate and confidential file, and may not exceed the time strictly necessary to clarify the facts. They are always subject to judicial supervision. These measures include: (i) interception of telephone and online communications; (ii) capturing and recording oral communications using electronic devices; (iii) use of technical devices for image capture, tracking, and location; (iv) searches of mass data storage devices; and (v) remote access to computer equipment.

DATA PROTECTION LEGISLATION

Existing data protection legislation—especially the *General Data Protection Regulation (GDPR)* and *Organic Law 3/2018*—may also restrict and regulate the use of AI in criminal proceedings.

The GDPR provides a set of principles, rights, and obligations that ensure the responsible, transparent, and secure use of technology in the processing of personal data, including within the legal field. And *Organic Law 3/2018* on the *Protection of Personal Data and Guarantee of Digital Rights* adapts the Spanish legal framework to GDPR and strengthens the protection of fundamental rights in the digital environment. This law establishes principles regarding the processing of personal data, regulates rights such as access, rectification, erasure, and portability, and defines obligations for data controllers and processors.

HUMAN RIGHTS

National legislation, such as the *Comprehensive Law 15/2022 on Equality and Non-Discrimination*, as well as constitutional guarantees and regional and international instruments, including the *European Convention on Human Rights*, may also constrain the use of AI in criminal proceedings.

Comprehensive Law 15/2022 on Equality and Non-Discrimination

The *Comprehensive Law 15/2022 on Equality and Non-Discrimination* explicitly refers to the use of AI in article 23, establishing that, within the framework of *Spain's National Artificial Intelligence Strategy*, the *Digital Rights Charter*, and European initiatives, public administrations must promote mechanisms to ensure that algorithms used in decision-making processes are transparent, minimise bias, and uphold accountability, including through impact assessments to detect potential discriminatory effects. These mechanisms should consider algorithm design and training data. Public bodies must also prioritise the interpretability of algorithmic decisions. Also, both public administrations and private companies are encouraged to foster the use of ethical, trustworthy AI that respects fundamental rights, and a quality certification for algorithms will be promoted.

Information uploaded as at September 2025. The material collected in this mapping tool is intended for general information purposes only and must not be used as a substitute for professional or legal advice. It is updated periodically but may not reflect the most recent developments. The Oxford Institute of Technology and Justice, the University of Oxford, the Clooney Foundation for Justice, and their representatives, as well as the law firms and lawyers that have contributed to this mapping tool make no guarantees or warranties regarding the accuracy or completeness of the information provided in the mapping tool and exclude liability for any loss or other result arising from any reliance placed on information presented in this mapping tool.

Organic Law 5/2024 on the Right of Defence

In December 2024, Spain enacted *Organic Law 5/2024 on the Right of Defence*. The law includes one article that expressly refers to the use of AI. Article 12.4 stipulates a transparency obligation: 1ndividuals have the right to transparently understand the artificial intelligence criteria used by digital platforms, including those that facilitate the selection of legal professionals, intermediary firms, and any other entities or institutions providing legal services'. Commentators criticised this article for being overly vague.

Spanish Charter of Digital Rights

The *Spanish Charter of Digital Rights* is a soft law instrument that provides an ethical and guiding framework to ensure the protection of fundamental rights in the digital environment. Developed by an expert advisory group under the Spanish State Secretariat for Digitalisation and Artificial Intelligence, the Charter does not create new rights but adapts existing ones to the challenges posed by emerging technologies. It emphasises key principles such as data protection, algorithmic transparency, human oversight in automated decisions, and non-discrimination in the use of AI. In the legal services sector, the Charter supports the responsible and effective use of technology by requiring that digital tools respect human dignity, ensure equitable access to justice, and guarantee that automated legal decisions are understandable, auditable, and subject to human review.

Spanish Constitution, regional and international Instruments

Constitutional guarantees, such as the right to a fair trial (section 24), equality before the law (section 14) or privacy (section 18), may also constrain the use of AI in criminal proceedings. Section 18 of the Constitution guarantees the right 'to personal and family privacy' and provides that 'the law shall restrict the use of data processing in order to guarantee' this right. Section 117 of the Constitution, moreover, stipulates that the 'exercise of judicial authority in any kind of action… is vested exclusively in the courts and tribunals laid down by the law'.

Similarly, Article 6 of the *European Convention on Human Rights* guarantees the right to 'a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law', which applies comprehensively to all stages of criminal cases. Article 8 of the Convention guarantees the right to privacy.

Some additional international guidance is offered by the abovementioned *European Ethical Charter on the use of AI in the judicial systems and their environment*, which was adopted by the Council of Europe's European Commission for the Efficiency of Justice (CEPEJ) in 2018, and by the *Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. The latter, which as at August 2025 had not yet come into effect, requires states to ensure that AI systems are not used to undermine 'respect for judicial independence and access to justice'. Fair trial and privacy guarantees under other international human rights treaties to which Spain is a party, such as articles 14 and 17 of the *International Covenant on Civil and Political Rights*or articles 16 and 40 of the *Convention on the Rights of the Child*, may also be relevant.

CYBERSECURITY LAWS

The *National Security Framework (Esquema Nacional de Seguridad)*, regulated by *Royal Decree 311/2022 of May*, establishes basic principles and minimum requirements necessary to ensure adequate protection of the information processed and the services provided by entities within its scope. Its objective is to guarantee access, confidentiality, integrity, traceability, authenticity, availability, and preservation of data, information, and services used through electronic means in the exercise of their responsibilities.

The *Royal Decree-Law 12/2018 of September 7* on the security of networks and information systems, regulates the security of networks and information systems used to provide essential services and digital services. It has been further developed by *Royal Decree 43/2021 of January 26*.

OUTLOOK

This is a rapidly evolving field with a number of initiatives and laws that are in the process of being approved. Currently in preparation is, for example, **the *Spanish Draft Law on AI*** which establishes the sanctioning regime applicable to violations of the obligations set out in the EU regulation and develops the framework for the use of real-time remote biometric identification in publicly accessible spaces for law enforcement purposes. The draft law states that the use of such biometric identification systems must be aimed at identifying specific individuals, and it is subject to judicial authorisation, detailing the procedures for obtaining such authorisation and the limits applicable to their use. The draft law was approved by the Council of Ministers in March 2025 but has not yet entered into force.

It is likely that legislative development will continue, and new laws will be enacted in the medium term to further shape Spain's AI governance framework in line with *Spain's 2024 Artificial Intelligence Strategy* (an updated and accelerated version of *Spain's National AI Strategy*). **The strategy aims to promote the development and responsible use of AI**across all sectors, including legal services, through three main pillars: strengthening technological capabilities, facilitating adoption in both public and private sectors, and ensuring an ethical, transparent, and human-centred approach to AI. The strategy supports the use of AI in the justice system through specialised models supervised by the Spanish Agency for the Supervision of Artificial Intelligence, which ensures that applications respect fundamental rights, are auditable, and subject to human oversight.

CASES

On 11 September 2025, in an administrative case (1119/2025), the Spanish Supreme Court recognised the constitutional right to access, at least in part, the source code of algorithms used in public administration, when those algorithms determine public rights, especially entitlement to social benefits. The Court ordered that the NGO be granted access to the source code of an application used to determine the eligibility of citizens for electricity bills-subsidiaries. It remains

Information uploaded as at September 2025. The material collected in this mapping tool is intended for general information purposes only and must not be used as a substitute for professional or legal advice. It is updated periodically but may not reflect the most recent developments. The Oxford Institute of Technology and Justice, the University of Oxford, the Clooney Foundation for Justice, and their representatives, as well as the law firms and lawyers that have contributed to this mapping tool make no guarantees or warranties regarding the accuracy or completeness of the information provided in the mapping tool and exclude liability for any loss or other result arising from any reliance placed on information presented in this mapping tool.

to be seen how this judgment will affect claims to access the algorithms of applications used in criminal proceedings.

Information uploaded as at September 2025. The material collected in this mapping tool is intended for general information purposes only and must not be used as a substitute for professional or legal advice. It is updated periodically but may not reflect the most recent developments. The Oxford Institute of Technology and Justice, the University of Oxford, the Clooney Foundation for Justice, and their representatives, as well as the law firms and lawyers that have contributed to this mapping tool make no guarantees or warranties regarding the accuracy or completeness of the information provided in the mapping tool and exclude liability for any loss or other result arising from any reliance placed on information presented in this mapping tool.