O

Oxford Institute
of Technology and Justice

ESTONIA

Tools	Krat | Salme | Specialised systems
Tasks	Administrative support | Case management | Data review and analysis | Decision-making support | Evidence review and analysis | Legal research, analysis and drafting support | Operational support
Users	Law enforcement | Prosecutors | Courts | Defence
Scope	Nationwide
Training	No mandatory or systematic training
Regulation	The EU AI Act regulates the use of some AI tools in criminal proceedings. The Estonian Bar Association has issued a non-binding AI Guide for Lawyers. Even though they do not mention AI, existing criminal procedure rules and data protection laws may also apply.
Insights	In the context of civil proceedings, Estonia has introduced a semi-automated procedure for small claims (of up to EUR 8,000) in which computer-generated orders are automatically issued based on the information supplied by parties in the proceedings.

AT A GLANCE

Estonia describes itself as 'the world's most advanced digital society', leading in the use of e-governance and digital identities that underpin nearly every aspect of life. At the same time, it has integrated AI incrementally into its criminal justice system. Law enforcement in Estonia has tested AI for crime prevention on social media, licence plate recognition, and facial recognition, though deployment remains cautious. Prosecutors have trialled 'virtual autopsies' as a less invasive and more cost-effective way to determine causes of death. Courts mainly use AI for support tasks like transcription (Salme), anonymisation (Krat), and document analysis. Prisons provide inmates with secure digital access to legal documents via devices using facial recognition, reducing reliance on paper processes. Estonia is bound by the EU AI Act, which

regulates the use of some AI tools in criminal proceedings. The Estonian Bar Association has issued guidance on the use of AI for lawyers. Estonia's Code of Criminal Procedure and existing data protection laws may also apply.

USE

Estonia describes itself as 'the world's most advanced digital society', leading in the use of e-governance and digital identities that underpin nearly every aspect of life. At the same time, it has integrated AI incrementally into its criminal justice system.

LAW ENFORCEMENT

Operational support

The Estonian Police and Border Guard Board, which conducts criminal investigations in Estonia, conducted research in 2025 to explore using automated AI-based tools to deter crime on social media platforms.

Data review and analysis

The Estonian Police and Border Guard Board uses automated cameras to **detect vehicle licence plates** and use this information to aid investigative processes. In 2025, during public discourse about the legality of such cameras, the Director General of the Police and Border Guard Board noted that the aim would be to use the entire network of public cameras in conjunction with AI so that the system can automatically detect violations and respond before anything serious happens. As at September 2025, there is no public information regarding the exact plans to deploy such an AI-based system.

In 2017 and 2018, the Police and Border Guard deployed security cameras equipped with **facial recognition abilities**. The software enabled users to create watchlists of specific individuals (such as suspects or wanted persons), triggering alerts when those individuals were detected. However, the system proved ineffective, as it did not lead to the identification of any listed

individuals, lacking sufficient accuracy. With the enforcement of the GDPR (see below) in 2018, the use of such technologies became subject to stricter compliance requirements. The technology was used again in January 2024, when the Ukrainian president visited Estonia. To ensure compliance with the GDPR, the facial recognition tool was not used in public spaces, but in a defined area. However, the Police and Border Guard Board has not noted any further plans to use the technology in 2025.

PROSECUTORS

Evidence review and analysis

Estonia has been testing the use of **virtual autopsies**, employing CT (Computed Tomography) and MRI (Magnetic Resonance Imaging) scans to determine causes of death without the need for invasive procedures. Digital imaging is used to identify all major internal injuries, although some finer details may not be as clearly visible. For this reason, cases are selected where such details are not critical to the investigation. This approach offers a more compassionate option for families and can help lower associated costs.

COURTS

Estonia, while advanced in digitisation of the judiciary, remains cautious about AI use in core judicial functions. As at September 2025, **AI is mainly used for support tasks** such as transcription and translation, with a growing use of AI in decision-making support.

> "It cannot be ruled out that artificial intelligence can solve some issues from beginning to end, at least in standard matters precluding discretionary rights, where the human dimension only comes into play in disputes or appeals."
>
> *Dr Villu Kõve, Chief Justice of the Supreme Court, 2020.*

Case management

Estonian courts use 'Salme', a nationwide AI-powered speech recognition assistant that transcribes court proceedings. reducing the time required for manual transcription. The speech-recognition software, based on natural-language technology, helps to record court hearings and, simultaneously with the audio recording of the session, create a transcript of the session. During a court session, *Salme* generates a transcript of the proceedings with only a few seconds' delay. While the system operates almost entirely automatically, some human input is required beforehand. This involves identifying the attendees prior to the session, enabling *Salme* to recognise individual voices during the hearing. The Salme system has a reported accuracy of approximately 92%, but it is subject to further human oversight, with clerks reviewing and correcting the prepared text where necessary.

'Krat' is an anonymisation software which removes participants' personal data from court judgments. In the initial stages of deployment, it was reported that the program mistook names, personal identification numbers, and addresses, leading to the necessity of additional review by court staff. The tool struggled to recognise contextual hints and references to identifiable individuals. However, the error rate decreased as the system learned.

A **text analytics tool** created by Texta OÜ is also reportedly being used by several government institutions to optimise work processes and streamline routine activities. For example, the Ministry of Justice (in collaboration with the Centre of Registers and Information Systems) used the system to remove personal data from nearly 80,000 court decisions involving outdated court sentences and republished the decisions in the Court Information System.

Legal research, analysis and drafting support

The Estonian judiciary has introduced a pilot project aimed at enhancing the analysis of court documents, by introducing **automated data labelling**. The automation possibilities being explored are:

Automatic extraction	Systems can read crime reports and pull out the key facts automatically: including who was involved, where it happened, what was stolen or damaged, and how much the loss was.
Indexing procedural documents	Documents can be searched with labels/categories (rather than specific words); automatic summarisation, simplification, and anonymisation.
Natural language queries	Users can ask questions in natural (non-legal) language to get information from justice databases. For example: 'what is the average amount for civil claims in 2023?'

Decision-making support

In the context of civil proceedings, Estonia has introduced a semi-automated procedure for small claims, in which **computer-generated payment orders** are <u>automatically</u> issued based on information supplied by the parties. These payment orders have the legal status of judgments for enforcement purposes. The process applies to monetary claims of up to EUR 8,000. Applications must be <u>submitted</u> exclusively through the national e-File system and are handled by the dedicated Payment Order Department of the Pärnu County Court. The system relies on <u>algorithms</u> to prepare the orders, and human oversight is retained for specific functions such as determining jurisdiction and ensuring the proper service of documents. While parties are notified that their case is handled through this expedited procedure, the official description does not expressly <u>inform</u> them that the initial decision is produced semi-automatically.

DEFENCE

> "At the moment, nobody really knows how legal professionals are using general, freely available AI tools. Whatever they do with them, it isn't transparent, so we don't have a clear picture. As for tailor-made AI solutions, we are still at the very early stages.
>
> *Dr Viljar Peep, Project manager for judicial reform, Ministry of Justice and Digital Affairs, July 2025*

Administrative support

Inmates in Estonia often require regular access to their personal information and court documents, but the current process of filing appeals and other legal actions typically relies on paper-based systems. To streamline these procedures and enhance efficiency, correctional facilities have implemented digital devices equipped with **facial recognition** technology, allowing prisoners to securely access essential legal services and documentation more efficiently.

TRAINING

There is **not yet a fully developed, Estonia-specific training programme for judges,** prosecutors or defence counsel that focuses exclusively on AI. But AI-related topics have been addressed by Estonian professional associations in their training efforts. For example, the Estonian Bar Association has organised training sessions for its members that cover the general opportunities and risks of using AI in legal practice. In the private sector, larger law firms in Estonia have begun to integrate AI into their internal workflows and, in doing so, organise in-house seminars and workshops to familiarise lawyers with both the potential and the risks of these tools.

REGULATION

Under Estonian law, there are **currently no binding domestic statutes, judicial protocols, or bar association rules** that expressly regulate the use of AI in the courts or in criminal proceedings. There are no reported instances of judges informally using AI to draft judgments, nor of parties employing AI tools in criminal proceedings in a way that would significantly impact the justice process.

At the international level, Estonia is bound by all directly applicable EU acts. Several apply to the use of AI in courts, including the *Artificial Intelligence Act (EU AI Act)* and the *General Data Protection Regulation (GDPR)*.

AI REGULATIONS

In Estonia, the regulation of AI is governed not by a standalone national law, but by the *EU AI Act,* which entered into force on 1 August 2024 and is being phased in between 2025 and 2030. Estonia is obliged to implement and comply with the provisions of the Act, which set out a harmonised legal framework for 'the development, the placing on the market, the putting into service, and the use' AI systems across the EU.

The *EU AI Act* adopts a risk-based approach, categorising AI systems into four levels of risk, including systems that pose an 'unacceptable risk' to fundamental rights and are banned outright, and high-risk systems, which are subject to strict obligations. 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 Act expressly refers to AI systems related to the administration of justice and criminal proceedings, which are mainly classified as high-risk and, in some instances, fall into the 'unacceptable risk' category.

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.

GUIDELINES FOR PRACTITIONERS

Bar Association Act and Code of Conduct

The Estonian Bar Association, governed by the *Bar Association Act*, plays a central role in regulating the legal profession's use of technology. The Act mandates the Bar to oversee the professional ethics of attorneys, organise continuing legal education, and ensure the lawful provision of legal services. Attorneys are expected to follow the existing *Code of Conduct* and ethical guidelines when using AI or other digital tools in their practice.

AI Guide for Lawyers

In addition, the Estonian Bar Association has developed a comprehensive *AI Guide for Lawyers*, which provides a structured framework for the responsible use of AI in legal practice in general. The guide is advisory in nature. It emphasises that while AI can be a powerful tool for processing large datasets, researching foreign laws, or gaining initial insights into new areas, ultimate responsibility for legal advice remains with the lawyer.

The document sets out principles for ensuring quality of service, independence, confidentiality, and cybersecurity, noting that lawyers must always verify AI outputs, avoid overreliance on AI, and prevent the disclosure of client-sensitive or personal data when using generative AI systems.

Furthermore, it recommends using only trustworthy providers, consulting IT and cybersecurity specialists before adoption, and negotiating clear terms with vendors regarding data security and liability. The guide also includes a practical 'AI User's Checklist' for lawyers and refers to a broader state-backed <u>risk assessment study by the Estonian Information System Authority (RIA) and Cybernetica</u>, which analyses risks of AI and machine learning technologies and methods for mitigating them.

CRIMINAL PROCEDURE RULES

Code of Criminal Procedure

The rules in Estonia's *Code of Criminal Procedure* set clear conditions for how evidence must be collected, and these standards would equally apply to AI-generated or AI-analysed material. According to section 64 of the *Code of Criminal Procedure*, evidence may only be gathered in a way that respects the dignity, life, and health of the individuals involved, and it is strictly prohibited to obtain evidence through torture, violence, methods that impair memory, or techniques that degrade human dignity. The provision further requires transparency when technical means are used in evidence collection: participants must be informed in advance and told the purpose of the technology, which would cover any use of AI-based tools. Estonian law therefore emphasises both fairness and procedural integrity, ensuring that any evidence—whether traditional or technologically assisted—cannot be admitted if obtained in violation of these safeguards.

DATA PROTECTION LEGISLATION

Estonia is bound by the European Union's *General Data Protection Regulation* (GDPR), which covers personal data processing matters, including processing information on criminal convictions. The GDPR is further implemented by the national *Personal Data Protection Act*. In addition, Estonia has transposed the *Law Enforcement Directive* into Estonian law through the *Personal Data Protection Act*, which specifically regulates the processing of personal data by law enforcement authorities for the purposes of preventing, investigating, detecting or prosecuting criminal offences. Section 21 of the *Personal Data Protection Act* establishes a general prohibition on decisions based solely on automated processing, including profiling, where such decisions produce adverse legal effects or otherwise significantly affect individuals. Effectively, this means that AI systems are prohibited from taking binding legal decisions in criminal proceedings without meaningful human involvement or oversight.

HUMAN RIGHTS

Section 146 of the *Constitution of the Republic of Estonia*, together with article 6 of the *European Convention on Human Rights,* guarantees fair trial rights that constrain the use of AI in criminal proceedings. Section 146 of the Constitution provides that justice shall be administered solely by the courts, which are independent in their activities and must act in accordance with the Constitution and laws. Article 6 of the European Convention guarantees the right to 'a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law', and this applies comprehensively to all stages of criminal cases. Taken together, these provisions should ensure that the introduction of AI tools cannot undermine judicial independence or the fundamental right to a fair trial. Guarantees of the right to privacy in section 26 of the Estonian Constitution and article 8 of the European Convention may also be relevant.

Some additional international guidance is offered by the *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. It sets out general principles on the use of AI, including that their design and implementation must be 'compatible with

fundamental rights'; that the 'development or intensification of any discrimination between individuals or groups of individuals' must be prevented; that 'certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment' must be used for the 'processing of judicial decisions and data'; that 'data processing methods' must be 'accessible and understandable' and external audits authorised; and finally, that users must be 'informed actors and in control of their choices'.

The EU has signed the *Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law.* The treaty, which as at September 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 Estonia 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.

OUTLOOK

While Estonia is a leader in digital public administration, its judiciary has not yet fully embraced AI, partially due to concerns about transparency, accountability, and the potential erosion of judicial discretion. Estonia's *Artificial Intelligence Action Plan 2024-2026* mentions the need for legal frameworks to ensure ethical AI use while the *Judicial Development Plan 2024-2030* envisions the gradual integration of AI into the judicial process as an aid to enhancing efficiency, improving case management, supporting legal research, and assisting judges. There is no domestic record yet of enforcement actions concerning the use of AI in criminal proceedings. But enforcement has begun under the *EU AI Act*, which is being phased in gradually (see above). This means that the scope and intensity of enforcement in Estonia continues to depend on how quickly national monitoring structures are put in place in line with the gradual entry into force of the different provisions of the Act. Estonia continues to

seek to address some of the concerns and foster trustworthy and non-discriminatory AI through initiatives like the 2024 Equitech cooperation project involving the Ministry of Justice and others. The project seeks to evaluate the fairness of automated decision-making by public authorities and explore ways to prevent bias and discrimination.

CASES

As at September 2025, Estonia has not reported any cases in which AI systems used in courts or in criminal justice have been formally reviewed or sanctions have been imposed for violations.