Legal 500
Country Comparative Guides 2025

Ireland
Artificial Intelligence

Contributor

Maples Group

Claire Morrisey

Partner and head of Data, Commercial and Technology **|** claire.morrissey@maples.com

Sarah Lydon

Data, Commercial and Technology Associate **|** sarah.lydon@maples.com

Emily Harrington

Data, Commercial and Technology Associate **|** emily.harrington@maples.com

This country-specific Q&A provides an overview of artificial intelligence laws and regulations applicable in Ireland.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Ireland: Artificial Intelligence

1. What are your countries legal definitions of "artificial intelligence"?

There is no legal definition of "artificial intelligence" ("AI") under Irish law currently. As Ireland is a member of the European Union ("EU") the EU's AI Act 2024 ("AI Act") is directly applicable in Ireland. The AI Act does not define "artificial intelligence" exactly but does define an 'AI System' as: *'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'*.

2. Has your country developed a national strategy for artificial intelligence? If so, has there been any progress in its implementation? Are there plans for updates or revisions?

In November 2024, the Irish government published a refresh of its national AI strategy titled "*Ireland's National AI Strategy: AI – Here for Good*" ("Strategy") which was originally published in 2021. This refresh takes into account recent developments in AI technology and regulation since the original strategy was published.

The Strategy aims to "*emphasise the importance of trustworthy, person-centred AI development and use, while positioning Ireland as a leader in seizing AI's economic and societal benefits*".

Ireland's national AI strategy is based on the following seven strands:

- **AI and Society:** The aim is to build public trust in, and understanding of, AI in Ireland. Key strategic actions include supporting the Irish AI Advisory Council, raising awareness about guardrails for trustworthy AI and make AI literacy an integral component of Ireland's Literacy, Numeracy and Digital Literacy Strategy 2024-2033.
- **Governance for Trustworthy AI:** The AI Act will be the primary legislation regulating AI in Ireland. Key strategic actions include Ireland's participation through EU working groups on the effective implementation of the AI Act, implementing the National Standard Authority of Ireland's Roadmap for AI Standards and Assurance, developing campaigns to raise awareness of the implications of the AI Act and ensuring Ireland's voice is heard in international fora on the governance of AI.
- **Driving AI in Irish Enterprise:** The Irish government recognises that it can be difficult for businesses to navigate rapid developments in technology and to identify the opportunities and risks associated with these developments. Key strategic actions include providing target support, training and advice to businesses on AI, looking to leadership and expertise of multinational corporations to support local enterprises, incentivising private investment in AI and establishing an AI regulatory sandbox.
- **AI Serving the Public:** AI can help to improve the delivery of public services (such as research, automated document handling, weather forecasting, prediction of disease outbreaks). Strategic actions include publishing guidelines on use of AI (published May 2025), identifying and sharing examples of best practice, raising awareness in the public sector on available supports and providing reskilling and upskilling opportunities to public sector staff.
- **A Strong AI Research and Innovation Ecosystem:** The Irish government wants to strengthen its research and innovation ecosystem. Strategic actions include creating a National AI Research Nexus (allowing for collaboration agreements and strategic partnerships), promoting Irish participation in the EU AI Innovation package measures and providing funding for AI research.
- **AI Education, Skills and Talent:** The Irish government is closely monitoring the potential impacts of AI on employment and has asked the AI Advisory Council to examine this. Strategic actions include participating in the OECD study on the impact of generative AI on skills needs of SMEs, developing guidelines on the use of AI for teachers, consideration of the integration of AI in curricula, funding AI PhD graduates and expanding upskilling and reskilling initiatives.
- **Infrastructure for AI:** The Irish government recognises the issue of the compute capacity of AI systems, the importance of quality data sets, the cybersecurity risks and the demand on the energy infrastructure. Key strategic actions include a review of high-performance computing services, maximising the value of grid and energy investment and assessing cybersecurity risks arising from greater use of AI

systems.

3. Has your country implemented rules or guidelines (including voluntary standards and ethical principles) on artificial intelligence? If so, please provide a brief overview of said rules or guidelines. If no rules on artificial intelligence are in force in your jurisdiction, please (i) provide a short overview of the existing laws that potentially could be applied to artificial intelligence and the use of artificial intelligence, (ii) briefly outline the main difficulties in interpreting such existing laws to suit the peculiarities of artificial intelligence, and (iii) summarize any draft laws, or legislative initiatives, on artificial intelligence.

As noted in question 1, the AI Act is directly applicable in Ireland. The AI Act is designed to establish a comprehensive legal framework governing the development and deployment of AI within the EU, placing a particular emphasis on ensuring that emerging AI technologies align with core EU legal principles relating to human rights, consumer protection, and data privacy. It classifies various forms of AI according to levels of risk, ranging from minimal to unacceptable. The AI Act also sets forth mandatory requirements for high-risk AI systems, such as those related to biometric identification or essential public services, including strict obligations for transparency, accountability, and oversight.

The AI Act also requires codes of practice to be developed by the EU AI Office including a code relating to General Purpose AI Models ("GPAI Models"). This GPAI Model code and accompanying guidelines were published by the AI Office in July 2025. Whilst the GPAI Model code and any others published by the AI Office are non-binding, they are indicative of the standards which regulators expect in terms of compliance with the AI Act.

The Irish Government's Spring 2025 Legislation Programme published in February 2025 includes a proposal for new Irish legislation titled "Regulation of Artificial Intelligence Bill" which will give effect to the AI Act, designate the national competent authorities responsible for implementing and enforcing the AI Act and provide for penalties for non-compliance with the AI Act. The heads of this bill are currently in preparation with little detail published on its contents as of yet.

The Irish government recently published 'Guidelines for the Responsible Use of AI in the Public Service' to set out principles for the use of AI by Irish public bodies.

4. Which rules apply to defective artificial intelligence systems, i.e. artificial intelligence systems that do not provide the safety that the public at large is entitled to expect?

Save for the AI Act, Ireland does not have an overarching AI legislative framework, including for defective AI systems. In the absence of specific AI liability legislation, rules for defective AI systems are covered under other legal regimes such as:

- **Product Liability:** The EU's new Product Liability Directive entered into force on 8 December 2024, but EU member states have until 9 December 2026 to transpose this into national law. The new Product Liability Directive extends the definition of a product to include software and AI integrated products. Manufacturers can be liable for damages which arise as a result of the lack of software updates or upgrades to maintain safety, including cybersecurity. With respect to claims for damages, compensation can be sought for death or personal injury, damage to or destruction of property and destruction or corruption of data that are not used for professional purposes. Products placed on the market post 9 December 2026 will be subject to the new Product Liability Directive and products placed on the market prior to this will be subject to the existing Product Liability Directive. In Ireland, the provisions of the EU's existing Product Liability Directive are currently in force under the Liability for Defective Products Act 1991 which does not specifically refer to software or AI and focuses on tangible products. Therefore, under the current legal regime in Ireland, AI will need to form part of a tangible product in order for the Liability for Defective Products Act 1991 to apply.
- **Negligence:** The common law tort of negligence also applies in respect of liability for defective AI systems. To establish negligence, a claimant must prove a duty of care, a breach of the duty of care, loss or damage and a causal link between the breach of the duty of care and the loss or damage suffered.
- **Data Protection:** Defects in AI systems may result in breaches of the GDPR and the Irish Data Protection Act 1988-2018 which may lead to penalties from the Irish Data Protection Commission ("DPC") and/or claims from data subjects.
- **Equality:** Where an AI system generates outcomes that are discriminatory in nature, individuals may take a claim under the Irish Employment Equality Act 1998 (as amended) or the Equal Status Act 2000 (as

amended).

The EU's proposed AI Liability Directive was intended to introduce liability rules for AI risks and to help to simplify the process for seeking compensation for damages caused by AI systems. However, the proposed directive was withdrawn by the European Commission in February 2025.

5. Please describe any civil and criminal liability rules that may apply in case of damages caused by artificial intelligence systems. Have there been any court decisions or legislative developments clarifying liability frameworks applied to artificial intelligence?

As per question 4, civil liability for AI-caused damage in Ireland currently falls under general tort law (which is fault-based) and will be governed by the strict liability regime of the EU's Product Liability Directive once implemented in Ireland.

Criminal liability arising from AI systems is not specifically addressed in the AI Act or under national legislation. Existing principles will apply to any such damage, but attribution of liability for actions by autonomous AI remains unclear. There is no stand-alone corporate manslaughter legislation in Ireland which could address extreme cases of damage caused by AI systems.

No Irish court decisions or national legislation have yet clarified the liability framework for AI, but EU legislative developments are expected to shape future Irish law in this area. The EU had previously proposed the introduction of an AI Liability Directive to deal with non-contractual civil liability for damage caused by AI systems however, the European Commission abandoned this proposal in February 2025.

6. Who is responsible for any harm caused by an AI system? And how is the liability allocated between the developer, the deployer, the user and the victim?

The Product Liability Directive (as outlined above) sets out a broad pool of operators that can be liable for a defective AI system. This is primarily the manufacturer (or the developer) of the system. An exception to this is where an entity is not based in the EU in which case the importer, authorised representative or in limited cases the distributor can be held liable. A third party making substantial changes to the product or providing related

services, which may include the deployer, can also be liable. The burden is on the victim to prove the damage caused under such a claim.

Aside from the Product Liability Directive, determining responsibility for harm under existing Irish law is dependent on whether the harm is actual harm to a person or property or whether this is a tort. In a conventional tort law system, responsibility for damages is established by pinpointing which party's actions led to the harm. The blame can rest with the developer, the deployer, or any participant involved in the product's journey through the market. When multiple parties are implicated in causing the loss, each is accountable for the share of harm they caused. If it is not possible to accurately determine the extent of each party's fault, the principle of joint and several liability may be invoked. Additionally, if the victim is found to have contributed to the incident, or if an unforeseeable event (force majeure) occurs, the liable party's obligation may be reduced or eliminated.

In the case of harm to a person or property the liability will rest on the party whose actions or inactions led to the damage to the victim. This could be the developer, deployer or user of an AI system and this is most typically a negligence claim.

7. What burden of proof will have to be satisfied for the victim of the damage to obtain compensation?

Under civil law in Ireland the burden of proof is 'on a balance of probabilities' and typically the obligation is on the plaintiff (or alleged victim) to satisfy the burden of proof. A plaintiff would need to demonstrate that on review of the facts it seems their account is more than 50% likely to be true.

There are certain exceptions to this which may be relevant to an AI claim. For example, if a defendant in a defamation case wishes to rely on the defense of truth (i.e. that the statement they said about the plaintiff was true) the obligation is on the defendant to establish this truthfulness. This is relevant as Ireland has seen a case in its courts regarding defamation as a result of the outputs of generative AI – see further 17 below.

8. Is the use of artificial intelligence insured and/or insurable in your jurisdiction?

Yes. Certain insurance providers cover the use of AI, in particular through professional indemnity insurance.

Risks relating to AI may also be covered under business interruption, D&O, cybersecurity, product liability and employers' liability. However, bespoke AI cover is not yet market-standard in Ireland.

9. Can artificial intelligence be named an inventor in a patent application filed in your jurisdiction?

The Irish Patents Act 1992 (as amended) is silent on whether or not an inventor must be a natural person and the Intellectual Property Office of Ireland ("IPOI") has not made any statements or decisions on whether AI can be named an inventor in a patent application. A decision from the European Patent Office ("EPO") in 2019 held that an inventor must be a human being and EPO decisions are considered persuasive authority in Ireland. The EPO Guidelines for Examination in the EPO also state that an inventor must be a natural person and that it will verify this. US, German and UK courts have come to a similar conclusion to the EPO. It is likely that the IPOI and the Irish courts would adopt a similar approach to the EPO.

10. Do images generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to?

Images generated by and/or with artificial intelligence can benefit from copyright protection in Ireland provided, pursuant to the Irish Copyright and Related Rights Act 2000 (the "CRRA"), they are both "artistic works" and original. The definition of "artistic work" is very broad and applies irrespective of 'artistic quality'.

The CRRA defines the "Author" as the person who creates the work and expressly states that *"in the case of a work which is computer-generated, the person by whom the arrangements necessary for the creation of the work are undertaken".* In the case of AI generated works this means that authorship is attributed to the person undertaking the AI image generation.

11. What are the main issues to consider when using artificial intelligence systems in the workplace? Have any new regulations been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

The main issues to consider when using AI systems in the workplace are:

- **Discrimination and Bias**: AI systems can unintentionally perpetuate or amplify existing biases, leading to unfair treatment of certain groups in workplace decisions;
- **Data Privacy and Security**: The use of AI in the workplace may involve processing large amounts of personal data including special category personal data, raising concerns about how this information is protected and used. Businesses need to consider the risk of cyberattacks on the AI infrastructure;
- **Job Displacement**: Automation through AI may replace certain roles, potentially leading to job losses and requiring businesses to manage workforce transitions;
- **Transparency**: Businesses need to ensure that employees understand when AI systems are used to make decisions about them or when they are interacting with AI systems. Furthermore, businesses should be transparent with employees about when employees can use AI tools as part of their work and adopt clear policies on such use; and
- **Skills and AI Literacy**: Employees may need new skills and a better understanding of AI to work effectively alongside these systems and adapt to changing job requirements. Businesses will need to ensure that sufficient training and support is provided to employees to allow them to adapt to the changing work environment.

Ireland has not yet introduced any new regulations regarding AI-driven hiring, performance assessment or employee monitoring. However, the AI Act contains a number of provisions that relate specifically to the workplace.

Under the AI Act, the following types of AI systems are prohibited:

- AI systems that infer emotions of an individual in the workplace unless this is for medical or safety reasons; and
- biometric categorisation systems that categorise individuals based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation.

The AI Act also classifies the following AI systems as high-risk AI:

- AI systems intended to be used for the recruitment and selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications and to evaluate candidates; and
- AI systems intended to be used to make decisions

affecting terms of work-related relationships, the promotion or termination of work-related contractual relationships, to allocate tasks based on individual behaviour or personal traits or characteristics or to monitor and evaluate the performance and behaviour of persons in such relationships.

12. What privacy issues arise from the development (including training) and use of artificial intelligence?

There are several privacy issues that arise from the development and use of AI particularly the interplay between the AI Act and the EU's General Data Protection Regulation ("GDPR"). The primary concerns are:

- **Lawful Basis for Processing:** AI systems often require large datasets, which may include personal data. Under the GDPR, organisations must have a lawful basis for processing such data (e.g., consent, legitimate interests, contractual necessity). Determining and documenting the appropriate basis can be challenging, especially when data is repurposed for AI training.
- **Transparency and Explainability:** GDPR mandates that data subjects are informed about how their data is used. AI, particularly generative models, can be complex, making it difficult to provide clear explanations about data processing, decision-making logic, and potential outcomes. This lack of transparency can hinder compliance with Articles 13 and 14 of the GDPR (information to be provided to data subjects).
- **Data Minimisation and Purpose Limitation:** GDPR requires that only data necessary for a specific, explicit purpose is collected and processed. There is a risk of collecting excessive data or using it for purposes beyond the original intent, which would breach the principles of data minimisation and purpose limitation.
- **Data Subject Rights:** The GDPR grants individuals rights such as access, rectification, erasure, restriction of processing, and data portability. Fulfilling these rights can be problematic with AI systems, especially if personal data is embedded in training data or if outputs are generated in a way that makes it difficult to trace or delete specific data points.
- **Automated Decision-Making and Profiling:** Article 22 of the GDPR gives individuals the right not to be subject to decisions based solely on automated processing, including profiling, which significantly affects them. Many AI systems, including generative AI, may make or inform such decisions in a completely automated way, raising concerns about fairness, bias,

and the ability to contest or understand these decisions.
- **Data Security:** AI systems can be vulnerable to data breaches, model inversion attacks, or unintended data leakage, especially if generative models inadvertently reproduce personal data from their training sets. Ensuring robust security measures is essential to protect personal data from unauthorised access or disclosure.
- **Data Anonymisation and Re-identification Risks:** While anonymisation is a common strategy to mitigate privacy risks, AI models can sometimes "memorise" and regenerate personal data, undermining anonymisation efforts. There is a risk that outputs from generative AI could inadvertently reveal information about individuals, leading to potential re-identification.
- **International Data Transfers:** AI development often involves cross-border data flows. The GDPR imposes strict requirements on transferring personal data outside the European Economic Area ("EEA"), and ensuring compliance with these rules can be complex, particularly when using cloud-based AI services or collaborating with international partners.

13. How is data scraping regulated in your jurisdiction from an IP, privacy and competition point of view? Are there any recent precedents addressing the legality of data scraping for AI training?

IP Perspective: Irish and EU laws on IP protection apply to material being scraped and the parties doing the data scraping. The European Union (Copyright and Related Rights in the Digital Single Market) Regulations 2021 (S.I. No. 567/2021) gives an exemption to copyright for text and data mining, which would include data scraping, provided that the owner of the copyright has not reserved their rights in an 'appropriate manner'.

The AI act requires providers of General Purpose AI systems (e.g. ChatGPT or similar large models) to comply with copyright laws including reservations of rights by authors. Such providers are also required to keep sufficiently detailed records of the materials they use to train their AI models. This will allow for review to determine if copyright has been breached.

There is an ongoing case awaiting hearing in the Courts of Justice of the European Union (CJEU) (*Like Company v Google Ireland C-250/25*) which will determine the legality of Google scraping copyrighted articles to train its Gemini AI system which, when prompted, produced

wording very similar to that of the original article published by Like Company. This case will be a key development in how scraping is treated from an IP perspective.

GDPR Perspective: Data scraping is subject to the data processing obligations as set out in the GDPR and the Irish Data Protection Acts 1988-2018. These include the requirement for consent of the data subject, having a lawful basis for the processing and compliance with the principles for data processing set out in the GDPR such as transparency, accuracy and storage limitation.

In April 2025 the DPC launched an inquiry into the legality of 'X' (formerly Twitter) scraping its users publicly accessible posts to train its Grok AI system. The ongoing inquiry will determine whether the processing of personal data in this way is lawful under the GDPR and will give insight into the regulators' approach to data scraping.

Competition Perspective: The Irish Competition Act 2002 (as amended) and Articles 101-106 TFEU apply to such activities.

14. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

In order for prohibitions on data scraping contained in website terms to be enforceable in Ireland the prohibition must be clear and form part of legally binding terms entered into between the parties which were accepted by the user including via a click-wrap or browse-wrap mechanism. This has been reflected at an EU level and also at a national level in a series of cases taken by Ryanair (*Ryanair Ltd v Bravofly and Travelfusion Ltd, Ryanair Ltd v Billigfluege and Ryanair Ltd v SC Vola.Ro Srl*) in which the High Court enforced provisions of the Ryanair website terms prohibiting data scraping of their website.

15. Have the privacy authorities of your jurisdiction issued guidelines on artificial intelligence?

The DPC has not yet issued any substantive guidelines on AI. In July 2024, the DPC published a blog on its website titled "AI, Large Language Models and Data Protection" which sets out some data protection considerations for organisations. In this blog, the DPC noted the following key points for organisations to consider:

- where creating an AI model using personal data already collected, organisations should consider if the new processing is within the scope of the existing legal basis;
- consider all the risks involved in the AI model or product design, creation and its onward usage and consider whether a data protection impact assessment is required;
- determine how the principle of storage limitation can be met;
- consider the risks associated with inaccurate or biased information and if those inputs are relied upon without human analysis or intervention;
- determine how to secure and protect the personal data within the AI models, in particular where the personal data will be held by a third party;
- consider how to comply with data subject rights such as access and erasure; and
- organisations should have appropriate data governance, design, policy and decision-making controls in place.

The European Data Protection Board ("EDPB") published its "*Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*" on 18 December 2024. While the opinion is not legally binding, it is indicative of the view a European data protection supervisory authority, including the DPC, would take. The key points in the opinion are as follows:

- **Anonymity:** The opinion provides an overview of how data protection supervisory authorities should assess the anonymity of an AI model. AI models will only be considered anonymous after a thorough evaluation where it can be concluded, after using reasonable means that the likelihood of obtaining or extracting personal data is insignificant. There should also be adequate documentation of processing operations at development and deployment stages to ensure accountability obligations under the GDPR were complied with;
- **Legitimate interest:** Legitimate interest can be used as a legal basis for processing for AI models provided that the three cumulative conditions are met; (i) pursuit of legitimate interest by controller or third party, (ii) processing is necessary to pursue the legitimate interest and (iii) legitimate interest is not overridden by interests and fundamental rights and freedoms of the data subjects. It is important to consider if there are less intrusive means of achieving the legitimate interest relied upon and the EDPB noted that mitigating measures can be adopted to address any identified negative impacts on data subjects' fundamental rights and freedoms; and
- **Unlawful processing:** The EDPB further clarifies that

unlawful processing that occurs in the initial stages prior to deployment can impact the lawfulness of subsequent processing that takes place. In the event there are separate controllers involved at different stages of processing, the data protection supervisory authority will consider the due diligence conducted by each controller. Where an AI model is considered effectively anonymised, the GDPR will not apply to subsequent processing.

16. Have the privacy authorities of your jurisdiction discussed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

The DPC has not yet published any decisions involving AI. However, in September 2024, proceedings initiated by the Irish DPC against X were struck-out on the basis of X's agreement to continue to adhere to the terms of an undertaking to suspend the processing on a permanent basis. The DPC had made an application under section 134 of the Irish Data Protection Act 1988 – 2018 which allows for an application to be made to the Irish High Court to suspend or restrict the processing of personal data where there is an urgent need to act to protect the rights and freedoms of data subjects. The DPC had concerns about the impact of the processing of personal data from publicly accessible posts posted on X to train X's Grok large language models.

Following on from the Irish High Court proceedings, in April 2025, the DPC announced an inquiry into X's processing of personal data from publicly accessible posts posted on X by EU/EEA users for the purposes of training its Grok large language models. According to the DPC, the inquiry will examine compliance with a range of GDPR provisions including lawfulness and transparency of processing.

17. Have your national courts already managed cases involving artificial intelligence? If yes, what are the key takeaways from these cases?

There have been no seminal Irish cases on AI as of yet. However, in addition to the DPC's ongoing inquiry into X mentioned above, some other recent cases have touched upon the use of AI.

- The case of *Reddan v An Bord Pleanála* [2025] IEHC 172 is a cautionary tale on the use of AI in legal proceedings. In this case, the applicant (a lay litigant) was seeking leave to bring judicial review proceedings. In one of the grounds for judicial review,

the applicant had used the phrase "subordination to perjury" which is not a legal phrase in Irish jurisprudence. The judge noted that this likely came from AI and "*has all the hallmarks of ChatGPT, or some similar AI tool*".
- In *Coulston & Others v Elliott & Elliott* [2024] IEHC 697, the defendants, who were also lay litigants, raised a new legal claim but could not explain it in court. The judge suggested that the defendants may have used AI in preparing the submissions and cautioned against the use of AI for submissions stating "*[t]he general public should be warned against the use of generative AI devices and programs in matters of law.*" In this case, the judge stated that the argument in this case was "*fatally flawed*" which is a risk that arises from use of AI.

Both of these cases highlight the risks associated with using AI in legal proceedings as AI has a tendency to hallucinate, or it fails to recognise the nuances between the laws of different jurisdictions, and this could ultimately lead to an individual being unsuccessful in legal proceedings.

In *Ryanair DAC v Flightbox SP ZOO* [2023] IEHC 689, Ryanair sought to obtain an injunction to prevent Flightbox from screen scraping Ryanair's website on the basis that it was in breach of Ryanair's terms of use which prohibit use of automated systems or software to extract data from its website for commercial purposes. It is worth noting that this was a judgement in default of an appearance. This case is one of a series of cases Ryanair has taken in Ireland and the EU in respect of data scraping and these cases may inform other cases in the future where AI is used for data scraping.

In 2024, an applicant issued a defamation claim in the Irish High Court alleging that his photo was incorrectly included in an article concerning a sexual misconduct trial. Lawyers for the applicant have stated that it is suspected that AI was used to aggregate news articles. No judgment has been issued in this case as of yet, however, this case demonstrates how the use of AI can be relevant in a wide variety of legal proceedings.

18. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence?

Ireland does not have a dedicated AI regulator or authority but the government of Ireland has recently appointed the Minister for Enterprise, Trade and Employment to act as a 'competent authority' to co-ordinate enforcement. Ireland has also appointed eight

public authorities to act as 'competent authorities' responsible for the implementation and enforcement of the AI Act in Ireland. The competent authorities in Ireland are:

- Central Bank of Ireland
- Commission for Communications Regulation
- Commission for Railway Regulation
- Competition and Consumer Protection Commission
- Data Protection Commission
- Health and Safety Authority
- Health Products Regulatory Authority
- Marine Survey Office of the Department of Transport

In addition, Article 77 of the AI Act requires member states to appoint public authorities or bodies to supervise and enforce EU laws on the protection of fundamental rights in respect of the AI Act. The Irish government has appointed the following entities to act in this role:

- An Coimisiún Toghcháin (the Electoral Commission)
- Coimisiún na Meán (the Media Commission)
- Data Protection Commission
- Environmental Protection Authority
- Financial Services and Pensions Ombudsman
- Irish Human Rights and Equality Commission
- Office of the Ombudsman (general public sector Ombudsman)
- Ombudsman for Children's Office
- Ombudsman for the Defence Forces

19. How would you define the use of artificial intelligence by businesses in your jurisdiction? Is it widespread or limited? Which sectors have seen the most rapid adoption of AI technologies?

According to the Irish Central Statistics Office ("CSO") in February 2025, the number of Irish businesses using AI increased from 8% in 2023 to 15% in 2024. The most common use of AI is for automating workflows or assisting in decision-making and data mining. Language generation, speech recognition and image recognition were also identified by the CSO in its report. A recent report from AWS titled *Unlocking Ireland's AI Potential 2025* also highlighted that 63% of Irish startups have already adopted AI which is significantly higher than the European average at 29%.

The sectors that have seen the most rapid adoption of AI technologies are the technology, science and media sectors according to a 2024 report by Microsoft Ireland and Trinity College Dublin. AI has also been increasingly used in the Irish manufacturing sector (for process automation, predictive maintenance and optimisation of production processes), financial services sector (for fraud detection, AML, risk management and customer analytics) and the retail and marketing sector (for customer insights, personalized marketing and sales optimisation).

20. Is artificial intelligence being used in the legal sector, by lawyers and/or in-house counsels? If so, how? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns surrounding them?

The use of AI in the legal sector has surged in recent years with many Irish law firms adopting GenAI and AI powered assistants. There are no definitive statistics to establish the level of this use, but anecdotal evidence suggests use of AI tools is widespread among large commercial law firms. A recent survey completed by Irish Tech General Counsel found that 60% of in-house counsel in Ireland are using AI tools in the completion of their work.

The regulatory concerns regarding the use of AI tools in the legal sector are similar to those discussed elsewhere in this guide surrounding privacy and particularly the concern that a client's confidential information will be used to train AI models and may be reproduced in a way that is inconsistent with the confidentiality obligations of lawyers in Ireland. There are also concerns that the output of an AI tool may be incorrect or in some cases made up (referred to as a 'hallucination') which makes the entire AI tool unreliable for use in a legal setting.

21. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

Key Challenges:

- **Ethical and Professional Responsibility:** AI introduces complex ethical questions, such as ensuring client confidentiality, maintaining privilege and avoiding bias in automated decision-making. Lawyers must ensure that the use of AI complies with the relevant legislation, Law Society guidance and broader ethical standards.
- **Data Privacy and Security:** AI systems often require access to large volumes of sensitive data. Ensuring compliance with the GDPR and Irish data protection law is a significant challenge, particularly in safeguarding client information from breaches or misuse.

- **Regulatory Uncertainty:** The legal and regulatory framework for AI is still evolving in Ireland and across the EU. Lawyers must navigate uncertain territory regarding liability and accountability.
- **Skills Gap and Training:** Many lawyers may lack the technical expertise to understand, implement or supervise AI tools effectively. Bridging this skills gap requires ongoing education and training, which can be resource intensive.
- **Impact on Employment and Traditional Roles:** AI has the potential to automate routine legal tasks, which may lead to concerns about job displacement or the changing nature of legal work. Lawyers must adapt to new roles that focus on higher-value, strategic tasks.

Key Opportunities:

- **Increased Efficiency and Productivity:** AI can automate time-consuming tasks such as document review, legal research and contract analysis, allowing lawyers to focus on more complex and strategic work.
- **Enhanced Access to Justice:** AI-powered tools can help make legal services more affordable and accessible, particularly for individuals and small businesses who may otherwise struggle to obtain legal advice.
- **Improved Accuracy and Consistency:** AI systems can reduce human error and provide consistent results in tasks such as due diligence, risk assessment and compliance checks, enhancing the quality of legal services.
- **Data-Driven Insights:** AI can analyse vast amounts of legal data to identify trends, predict outcomes and support decision-making, giving lawyers a competitive edge in litigation, negotiation and advisory work.
- **Innovation in Legal Services:** The adoption of AI encourages law firms to develop new business models and service offerings, such as online legal platforms, virtual assistants and automated contract generation, helping them to remain competitive in a rapidly changing market.

22. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

The phased implementation of the AI Act will be the most significant legal development in Ireland over the next 12 months. As noted in 3 above, the Irish Government's Spring 2025 Legislation Programme published in February 2025 includes a proposal for new Irish legislation titled "Regulation of Artificial Intelligence Bill" which will give effect to the AI Act, designate the national competent authorities responsible for implementing and enforcing the AI Act and provide for penalties for non-compliance with the AI Act. The heads of this bill are currently in preparation with little detail published on its contents as of yet.

In April 2025, the Protection of Voice and Image Bill was introduced into the Irish legislative process. The aim of the bill is to address the issue of deepfakes and misuse of individuals' data and seeks to make it a criminal offence to knowingly misuse an individual's name, photo, voice or likeness for the purposes such as advertising products, events, political activities and fundraising. It is worth noting that this is a private members' bill, and the likelihood of this becoming law is slim. However, private members' bills tend to bring focus to an issue which may cause the government to take action.

Contributors

Claire Morrisey
Partner and head of Data, Commercial and Technology

claire.morrissey@maples.com

Sarah Lydon
Data, Commercial and Technology Associate

sarah.lydon@maples.com

Emily Harrington
Data, Commercial and Technology Associate

emily.harrington@maples.com