The Gavel and the Algorithm: The Role of the Courts in a Data-Driven World

Delivered by Ms. Justice Iseult O'Malley at the international symposium in Dublin City University on 22 January 2026

1. I am honoured to have been invited to contribute to your discussion on this extremely important topic. I need to make it clear from the start, however, that I am speaking without any expertise whatsoever as far as technology goes, and have no idea what it may be capable of in the coming years. My role here, as I see it, is to give some indication, from the perspective of a non-technophile judge, of what I think are possible significant challenges for the courts arising out of the widespread use of artificial intelligence and to tell you what tools may be available to a judge in dealing with them. Of necessity, given the vast scale of potential issues, what I have to say will be merely an overview of certain issues and I will inevitably omit matters that are of real concern or importance.

2. I start with certain basic principles. This State, and the institutions of the State, are obliged to uphold human rights. That means that, where necessary, the government and the legislature should put in place laws for the protection of rights and the courts should provide remedies for breach of rights. Modern liberal democracies in the current era tend to have highly developed systems for the protection of human rights – I will not claim that any of them are perfect or that they do not have gaps, but it is necessary to understand that issues around technological developments are arising in a legal landscape that is not entirely barren.

3. In Ireland, every new judge makes a declaration in open court that they

will uphold the Constitution and the laws. The Constitution is the source of most of the fundamental rights that can be relied upon by citizens and by others who are within the jurisdiction of the Irish courts. Under Article 40.3 the State guarantees in its laws to respect and, as far as practicable, to defend and vindicate personal rights. In particular it must protect as best it may from unjust attack, and in the case of injustice done, vindicate the life, person, good name and property rights of individuals. Some personal rights are expressly set out in the text of the Constitution, while others (including the right to privacy) have been derived from the text. This difference does not have any consequence in terms of the constitutional duty of the courts to protect any constitutional right.

4. Importantly, the Irish Supreme Court has from an early stage of the development of its constitutional jurisprudence seen the Constitution as a "living document" – on issues concerning human rights, judges do not feel bound to ask what the drafters of the text thought in 1937, but can adapt to developing concepts and values such as human dignity.[1]

5. One significant principle that has been applied in the development of our constitutional jurisprudence is that there must be a remedy for any violation of a constitutional right. If a remedy is not provided by legislation (such as legislation dealing with privacy in relation to data or the protection of one's good name through an action for defamation), or by the existing range of common law torts, then the courts must devise an appropriate solution. Where the defendant is the State, it will sometimes be sufficient to simply make a declaration that a breach has occurred – the relationship between the judicial executive and legislative branches of government is such that a declaration will in general be enough to ensure that the wrong will be rectified. Where the violation of rights occurs through legislation, the legislation may be found to be

[1] ***McGee v. Attorney General*** [1974] I.R. 284, ***NVH v. Minister for Justice*** [2017] IESC 35.

repugnant to the Constitution and accordingly invalid.

6. In other cases, an award of damages will be appropriate. So, for example, in the 1980s the Supreme Court held that the constitutional right to privacy of two journalists had been breached by the State when the Minister for Justice directed the Gardaí (the Irish police force) to tap their telephones for purely political reasons. A large award of damages was made and subsequently legislation was introduced to regulate the powers of the gardai to take such actions.[2] Actions for a breach of constitutional rights against non-State actors are less frequent but not unheard of. In such cases an award of damages, coupled perhaps with some form of injunction, may be the more likely remedy.

7. Since Ireland joined what were at the time the three European Community institutions in 1972, the Constitution has provided that nothing in it can be relied upon for the purpose of invalidating any legislation or measures adopted by the Irish State that are necessitated by membership, or to prevent any European legislation or measure from having force in the State. We accept, therefore, the supremacy of European Union measures in areas within its rightful scope. That means that individuals may be able to rely on rights derived from EU law, including the judgments of the Court of Justice of the European Union and the Charter of Fundamental Rights in areas where that law applies.

8. For today's purposes, a crucial development in EU law is the introduction of the AI Act in Regulation (EU) 2024/1689 – this is going to be a major feature of our legal landscape in coming years. (Bear in mind that regulations are directly effective in Member States and do not require national legislation to be enforceable.) It is a complex and ambitious measure that lays down harmonised rules for the placing on the market, the putting into service, and the use of artificial intelligence within the

[2] ***Kennedy v. Ireland*** [1987] I.R. 587.

Union. The stated aim is to promote innovation in and the uptake of AI through a "human-centric" approach, and to make the EU a global leader in the development of "secure, trustworthy and ethical" AI.[3] At the same time, it seeks to ensure a high level of protection of health, safety and fundamental rights in the Union, including democracy and the rule of law. The Regulation is coming into force in phases. In the first phase, a prohibition on unacceptable uses of AI has been in place for a year now, and I'll come back shortly to describe some of those. I will also very briefly mention the "high risk" category set out in the AI Act.

9. At a more mundane, day-to-day level, note that EU law provides for a simplified, uniform procedure whereby individuals or companies in one member State of the EU can sue individuals or companies in another.

10. Another important source of rights is the European Convention on Human Rights. Ireland was a party to the Convention from the start, and one of the first to accept the right of individual petition, although it was only in 2003 that the Convention and the case-law of the European Court of Human Rights became directly relevant to cases decided in the Irish Courts. There is of course an overlap between the rights protected by the Constitution and the Convention, but it is essential to note that, additionally, Contracting States may be held liable for a breach if they fail to protect and vindicate the rights of an individual. That can include failing to criminalise conduct that violates rights.

11. The Convention is implemented in Irish law through the provisions of the European Convention on Human Rights Act 2003 as amended. For present purposes, there are some significant features of the Act – State organs must perform their functions in a manner compatible with the State's obligations under the Convention. Judges must, so far as is

[3] European Commission, 'AI Act'. See link here; EU parliament, 'EU AI Act: first regulation on artificial intelligence' (2023). See link here.

possible and subject to rules of law about statutory interpretation, interpret laws in a manner compatible with Convention obligations. Judges must also take judicial notice of decisions, declarations and advisory opinions of the Court of Human Rights, the European Commission on Human Rights and the Committee of Ministers. Where no other legal remedy is available, a declaration can be granted to the effect that a statutory provision is incompatible with the State's obligations. Such a declaration is not the same as a declaration that legislation is repugnant to the Constitution – it does not invalidate the law – but it is a considered finding by the courts that the State is in breach of its international obligations.

12. Finally, it is of course open to the Oireachtas, the Irish legislature, to provide for additional protections for rights through its legislation and it may create new criminal offences to deal with new forms of harm to society and to individuals.

Protection of Human Rights and AI

13. The rights that have been most focussed upon in public discussion of AI seem to be the rights to privacy and freedom of expression. This may be because of the clear differences between views on the relative importance of these rights in differing contexts on the two sides of the Atlantic. It is clear that the Member States of the EU, and certainly the Court of Justice, are inclined to place a very high value on personal privacy and individual dignity, while the USA tends to promote freedom of expression to a greater extent.

14. The debate on the proper balance to be struck between these two deeply entrenched rights will no doubt continue for the foreseeable future. It should not, however, be allowed to obscure the fact that other rights can be engaged by the use of AI. In some circumstances, even the rights to life and to bodily integrity can be endangered – I am thinking here of the

use of deepfake pornography to target individuals (mostly women) or to facilitate the spread of child sexual abuse material on the internet. Children and vulnerable adults can be harmed by AI systems that respond to them in inappropriate ways, through, for example, chatbots intended to be companionable. Property rights can be engaged, since an individual's work (their intellectual property) may be taken without acknowledgement and added to the data used to train Large Language Models. The right to work (a recognised constitutional right in this jurisdiction) is manifestly affected, even in occupations once thought of as providing an entirely secure career.

15. AI may also affect the core work of the courts in the administration of justice. In some jurisdictions,[4] the use of AI systems for the determination of disputes between individuals is being pioneered. There are, of course, differing views on this development. Proponents say that it provides for a swifter, more consistent method of dispute resolution and that many people would prefer it to the possibly biased judgment of a human being. Others say that human judgment is central to the concept of the administration of justice, and point out that AI can be infected by bias fed into the model.

16. In the ordinary work of the courts, the use of AI by judges, lawyers, their clients or litigants representing themselves could create its own risks for the integrity of the process.[5]

The AI Act

17. The Regulation is based on the classification of AI systems according to risk. Article 5 prohibits the provision or deployment of systems that pose

[4] Lord Sales, 'The application of public law values and principles in automated governance' (Lecture, 7 August 2025).
[5] ***ProHealth Inc v Pro Health Solutions Ltd*** BL Number O/0559/25 (Decision date: 20 June 2025).The full decision can be found here.

unacceptable risks to fundamental rights and Union values – that is the topic I want to look at most closely, since it is the category that most engages the duty of the courts to uphold rights. The next category is high risk, then limited risk, then minimal risk. Differing levels of regulation apply to each of those three categories – at the lowest level, for example, if a person finds themselves dealing with a chatbot deployed by a government department to answer straightforward queries, all that might be necessary is to simply inform the person that they are not communicating with a human.

18. There are exceptions to the prohibitions, relating to matters such as systems used exclusively for military, defence or national security purposes, or for the sole purpose of scientific research and development. Also, the Regulation does not apply to a user who is a natural person using AI systems in the course of a "purely personal non-professional activity". The limits of this exclusion are not entirely clear to me. It seems clear that an influencer who is paid to promote goods or services and who uses a harmful system to do so may be subject to the Regulations, but what of the individual who deploys a manipulative or deceptive system for reasons other than gain? The Commission guideline does not go into great detail on this, but does state that criminal conduct cannot be considered to be "personal".

19. From a specifically Irish point of view, it is also important to note that this State is exempt in relation to certain of the prohibitions because of the effects of Protocol No. 21 (annexed to the Treaty on the European Union and the Treaty on the Functioning of the European Union). Ireland has what is generally referred to as an opt-out from measures enacted in the area of freedom, security and justice governing the forms of judicial cooperation in criminal matters or police cooperation and this is acknowledged in Recital 40 of the AI Act. The Recital states that Ireland is not bound by the rules laid down in Article 5(1)(g), which I will come to, to the extent it applies to the use of biometric categorisation systems

for activities in the field of police cooperation and judicial cooperation in criminal matters, or by Article 5(1)(d), to the extent it applies to the use of AI systems covered by that provision.

20. This exemption does not give Ireland free rein in respect of the use of biometric data. The State remains bound in this context by measures on data privacy such as the GDPR Directive and by the obligation to respect human rights.

21. The Regulation does not affect the applicability of existing Union law relating to the protection of personal data, privacy, the confidentiality of communications, consumer protection or product safety and nor do the exemptions. Therefore, a system that is not prohibited by the Regulation could still be unlawful because of a breach of rights in relation to, for example, data protection law or because of prohibited discrimination.

22. The prohibitions listed in Article 5 of the AI Act are set out in eight categories.

23. The first and second categories cover AI systems that deploy subliminal techniques beyond a person's consciousness, or purposefully manipulative or deceptive techniques, with the objective or with the effect of distorting behaviour by impairing the ability to make decisions, in a manner that causes or is likely to cause significant harm to the person making the decision or to others (Article 5(1)(a)) and harmful exploitation of vulnerabilities (Article 5(1)(b)). The Commission's Guideline says that the underlying rationale of these prohibitions is to protect individual autonomy and well-being from manipulative, deceptive, and exploitative AI practices that can subvert and impair an individual's autonomy, decision-making, and free choices.

24. The Guideline gives as an example of subliminal techniques a game played using a headset that detects brain activity in order to control the game. Such a system can leverage AI-enabled neuro technologies and machine-brain interfaces to train the user's brain surreptitiously and without their awareness, pushing them into behaviour and into decisions they would normally not have made in a manner that can cause them significant harm. The Commission says that the prohibition targets only cases of such significantly harmful subliminal manipulation and not machine-brain interface applications in general, when designed in a safe and secure manner that is respectful of privacy and individual autonomy.

25. An example of purposefully manipulative techniques is sensory manipulation where an AI system deploys background audio or images that lead to mood alterations, for example increasing anxiety and mental distress, that can influence users' behaviour to the point of creating significant harm. Another example is personalised manipulation where an AI system creates and tailors highly persuasive messages based on an individual's personal data or exploits their vulnerabilities to influence their behaviour or choices to a point of creating significant harm.

26. 'Deceptive techniques' deployed by AI systems involve presenting false or misleading information with the objective or the effect of deceiving individuals and influencing their behaviour in a manner that undermines their autonomy, decision-making and free choices. The Commission cites as an example of deceptive techniques that may be deployed a chatbot that impersonates a person's friend or relative using a synthetic voice. Another, very striking, example is an AI system that learns how to recognise that it is under evaluation and will temporarily stop any undesired behaviour, only to resume such behaviour once the evaluation period is over.

27. The prohibition on harmful exploitation targets systems that exploit

vulnerabilities due to age, disability, or a specific social or economic situation, with the objective or with the effect of distorting behaviour, causing or reasonably likely to cause significant harm. It is assumed that persons within the specified categories are less likely to recognise, and may be particularly vulnerable to, manipulative and exploitative practices. "Vulnerability" is understood to encompass cognitive, emotional, physical, and other forms of susceptibility that can affect the ability of an individual or a group of persons to make informed decisions or otherwise influence their behaviour. "Exploitation" is seen as making use of such vulnerabilities in a manner that is harmful for the exploited person(s). Examples given include children's games that can analyse a child's individual behaviour for the purpose of offering them rewards in a way that renders the game addictive; systems that target older persons who may have reduced cognitive abilities with deceptive personalised offers that may expose them to financial loss; therapeutic chatbots intended to support persons with disabilities that influence them to buy expensive medical products; systems that identify young women and girls with disabilities online and target them with grooming practices; and systems that target people who live in low-income areas with predatory financial products.

28. The next prohibition applies to "social scoring", where AI systems evaluate or classify natural persons based on social behaviour or on personal or personality characteristics, with the social score leading to detrimental or unfavourable treatment. The data leading to that treatment may come from an unrelated social context, and the treatment may be unjustified or disproportionate to the social behaviour.

29. The prohibition in Article 5(1) (d) is potentially directly relevant to the courts, and it is not yet clear to what extent Ireland intends to be bound by it. It forbids the use of AI systems that assess or predict the risk of a natural person committing a criminal offence based solely on profiling, or on assessing personality traits and characteristics. The prohibition does

not apply if the AI system is used to support a human assessment, based on objective and verifiable facts, of the involvement of a person in a criminal activity. Where that is the case, however, the systems used, while not prohibited, will still be classified as "high risk" and thus subject to stringent regulation. The rationale for the prohibition is that natural persons should be judged on their actual behaviour and not on AI-predicted behaviour.

30. The examples given by the Commission include the following:

- A law enforcement authority uses an AI system to predict criminal behaviour for crimes such as terrorism solely based on individuals' age, nationality, address, type of car, and marital status. With that system, individuals are deemed more likely to commit future offences that they have not yet committed solely based on their personal characteristics. Such a system may be assumed to be prohibited under Article 5(1)(d) AI Act.

- National tax authorities use an AI predictive tool to review all taxpayers' tax returns to predict potential criminal tax offences to identify cases requiring further investigation. This is done solely on the basis of the profile built by the AI system, which uses for its assessment personality traits, such as double nationality, place of birth, number of children, and opaque variables, especially inferred information that is predictive and therefore non-objective and hard to verify. Such a system will normally fall under the prohibition of Article 5(1)(d) AI Act, since there is no reasonable suspicion of the involvement of a particular person in a criminal activity or other objective and verifiable facts linking that to that criminal activity. This is also an example that falls within the scope of social scoring prohibited under Article 5(1)(c) AI Act involving unfavourable treatment with data from unrelated social contexts.

- A police department uses an AI-based risk assessment tool to assess the risk of young children and adolescents being involved in 'future violent and property offending'. The system assesses children based on their relationships with other people and their supposed risk levels, meaning

that children may be deemed at a higher risk of offending simply by being linked to another individual with a high-risk assessment, such as a sibling or a friend. The parents' risk levels may also impact a child's risk level. The risk assessments result in police 'registering' these children in their systems, monitoring them with additional inspections, and referring them to youth 'care' services. Such a system is also likely to fall under the prohibition of Article 5(1)(d) AI Act.

31. I note here that in the USA the deployment of risk-prediction tools has been highly controversial for many years because of the perception that they embed pre-existing biases. The problem arises from the fact that crime-prediction systems generally use historical data about crime, analyse it for indicators and generate risk-scores as predictions. They may be of value to law enforcement agencies in, for example, making policing plans but the use of data about crimes committed in the past in order to predict the future behaviour of other individuals may perpetuate or even reinforce biases – it may be that certain groups of people are more likely to be arrested and more likely to be convicted of some kinds of crime than others. It may also be the case that relevant individual circumstances of previous offenders or of the person who is the subject of a decision are not taken into account in whatever AI model is used.

32. Article 5(1)(e) prohibits "untargeted scraping" of the internet or of closed-circuit TV for the purpose of developing facial recognition databases.

33. Article 5(1)(f) prohibits emotion recognition – that is, AI systems that infer emotion – in the workplace or in educational establishments, except for health or safety reasons.

34. Paragraphs (g) and (h) of Article 5(1) are about biometric data. Paragraph (g) prohibits biometric categorisation – AI systems that

categorise people 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, apart from the labelling or categorisation of lawfully acquired biometric datasets, including in the area of law enforcement. Paragraph (h) prohibits the use of real-time remote biometric identification in publicly accessible spaces for the purposes of law enforcement, except where necessary in a targeted search for specific victims of crime, the prevention of specific threats including terrorist attacks, and the search for specific suspects in relation to specific offences.

Penalties

35. The AI Act follows a tiered approach in setting the penalties for non-compliance with its various provisions, depending on the seriousness of the infringement. Breaches of the prohibitions in Article 5 are subject to the highest fine. Providers and deployers engaging in prohibited AI practices may be fined up to 35 million euros or, if the offender is an undertaking, up to 7% of its total worldwide annual turnover for the preceding financial year, whichever is higher. EU institutions, bodies and agencies that violate the prohibitions may be subject to administrative fines of up to 1 500 000 euros.

High Risk AI systems

36. "High-risk" systems are systems that pose a significant risk to the health, safety or fundamental rights of individuals. As listed in Annex III of the Regulation they include systems used to determine access to educational institutions, employment recruitment, access to essential public and private services and migration control. They also include AI systems intended to be used by a judicial authority or on their behalf in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution.

37. Categorisation of a system as high risk means that it is subject to rigorous regulation.

National implementation measures

38. At national level, the Government has nominated nine statutory bodies as Competent Authorities, upon whom additional powers will be conferred under the AI Act in August of this year. They include An Coimisiún Toghcháin (the Electoral Commission), Data Protection Commission, Irish Human Rights & Equality Commission and the various Ombudsmen.

39. According to the Government, these authorities will not be given additional tasks but will have additional powers to facilitate them in carrying out their current responsibilities for protecting fundamental rights, in circumstances where use of AI poses a high risk to those rights. The Government has also said that by August 2026 it will establish a new "AI Office of Ireland"[6] as a central and coordinating authority for the implementation of the AI Act in Ireland. Its purpose will be to provide a focal point for the promotion and adoption of transparent and safe AI in Ireland. The AI Office is intended to co-ordinate Competent Authority activities to ensure consistent implementation of the AI Act and serve as a single focal point.

40. In early 2024 the Irish Government made a commitment that Artificial Intelligence (AI) tools used in the public service must comply with seven key principles for Trustworthy AI. It has produced a guideline for the use of AI in the public service based on principles developed by the European Commission's High-Level Expert Group. The guideline emphasises the need for human agency and oversight of AI systems, technical robustness and safety, privacy and data governance, transparency, diversity, non-

[6] Government of Ireland, 'Ireland leads the way in EU AI regulation' (16th September 2025). See link here.

discrimination and fairness, societal and environmental well-being and accountability.

Conclusion

41. I stressed earlier that developments in AI were not taking place in a barren legal landscape. That is so, but it may well turn out that there are bare patches in the landscape. We will no doubt learn as we go along, and further legislative intervention may be required. In the meantime, the task of the courts must remain as it has been – to uphold the Constitution and the laws.