

The Law Relating to AI and Related Aspects of Digital Technologies in the UK

Jessica Alder, Bhumika Billa and Simon Deakin

Centre for Business Research, University of Cambridge

Draft of 29 January 2026

1. Introduction

This paper reviews the state of the law relating to AI and related aspects of digital technologies in the UK. The UK has no general AI-related law which could be compared, for example, to the EU's Artificial Intelligence Act. UK policy makers have sought to avoid addressing AI-related issues through a horizontal measure of this kind. Instead, AI-related governance has been largely delegated to existing regulatory bodies. At the same time, the British government has sought to provide general guidance to regulators, through which the elements of an AI policy or strategy have begun to emerge. This approach can be characterised as promoting the development of AI-related technologies while seeking to build trust in their use. The current government has not ruled out legislating for generic AI-related risks should this prove necessary.

As a result of this orientation of UK policy towards AI, an account of the UK law relating to AI needs to address the distinct areas in which AI-related issues have so arisen. Section 2 below sets out the evolution of the overall approach of UK policy makers to AI. Section 3 takes a closer look at the interface of data protection law and AI. In section 4 we consider the impact of AI on intellectual property law, with specific reference to the implications for copyright of data scraping. Section 5 examines product safety, section 6 employment law, and section 7 competition law and market concentration. In section 8 we examine the use of AI in legal services and the administration of justice. Section 9 provides an assessment and section 10 concludes. The law is stated as it stood at the end of November 2025.

2. General law and policy with respect to AI-related risks

2.1 Evolution of UK AI Policy

The UK's approach to artificial intelligence (AI) has been to promote its use and adoption within the economy and across society, while seeking to address emerging risks and build public trust. It has avoided enacting a 'horizontal' or generally applicable regulatory measure along the lines of the EU's AI Act, choosing instead to retain existing sector-specific regulation. This approach has been consistent across recent governments of different political composition (the current Labour government replaced the previous Conservative one in the summer of 2024). Figure 1 below shows the evolution of the policy in the form of a flow chart linking the principal initiatives since 2015.

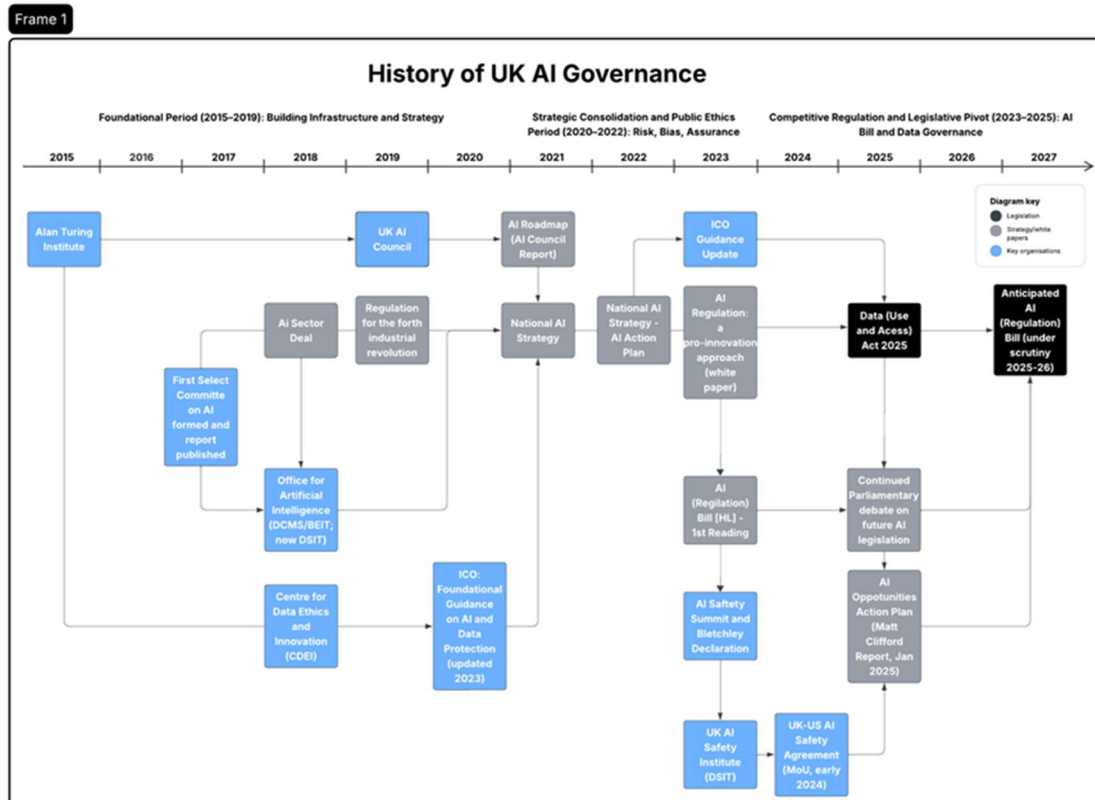


Figure 1. History of UK AI Governance

The beginnings of current UK policy on AI can be dated to the [2017 Industrial Strategy, Building a Britain Fit for the Future](#), which ‘set out the government’s vision to make the UK a global centre for AI innovation’. In 2018 the government announced an [AI Sector Deal](#) amounting to £1 billion of co-investment with companies in the UK AI ‘ecosystem’, and in 2019 it set up the [AI Council](#), a non-statutory expert body, to provide advice on AI policy. In 2021 the government adopted a [National AI Strategy](#), a ten-year vision to realise ‘a step change for AI in the UK, recognising the power of AI to increase resilience, productivity, growth and innovation across the private and public sectors’.

The UK’s sector-led regulatory model for AI has been expressly developed as an alternative to the EU’s horizontally applicable AI Act. In March 2023 the then Conservative government published a White Paper on AI regulation, [A Pro-Innovation Approach to AI Regulation](#), setting out the case for a flexible, sector-based model rather than a single overarching law. The premise of the White Paper was that the pace of AI development made it vital for the UK to act quickly to secure its position as a hub for AI companies, while avoiding overly strict prescription that could stifle innovation. This remains the basis for UK policy on AI under the Labour administration which took office in the summer of 2024.

The White Paper proposed that existing sector-specific regulators, including the Information Commissioner’s Office (ICO), the Competition and Markets Authority (CMA), the Office of Communications (Ofcom), the Medical and Healthcare Products Regulatory Agency (MHRA) and the Financial Conduct Authority (FCA), should address emerging AI risks according to five common principles of ‘safety’, ‘transparency’, ‘fairness’, ‘accountability’ and ‘contestability’, within their respective remits.

To coordinate its overall strategy, the government committed in the White Paper to setting up a central function responsible for horizon scanning, cross sector risk assessment and ensuring coherence across regulator activities. The White Paper also envisaged the launch of a multi regulator sandbox where businesses could trial AI products under regulatory supervision. The White Paper also made it clear that the government would introduce no new AI specific legislation at the outset, preferring to use existing regulatory powers unless future risks demanded statutory intervention.

Following publication of the 2023 White Paper, the government invited the views of stakeholders, and published a [response](#) in April 2024. This reaffirmed the approach taken in the White Paper. The response concluded that stakeholders had broadly endorsed the five principles and the idea of a central coordinating function. Regulators were instructed to publish their own AI strategies by 30 April 2024, setting out how they would integrate the principles and manage sector specific risks ([Mayer Brown](#)). The government signalled that binding legal duties, requiring regulators to give due regard to the principles, could follow if voluntary alignment proved insufficient ([Deloitte](#)). While maintaining a pro-innovation emphasis, the government response left open the possibility of future legislation, particularly for high risk areas such as foundation or frontier AI ([Eversheds Sutherland](#)).

Alongside its sector-specific approach to the governance of AI-risk, the UK has sought to position itself as a global leader in AI safety. It established the AI Safety Institute, now the [AI Security Institute](#) (AISI), to evaluate advanced models and develop safety science, with an international footprint now extending to Silicon Valley. The UK hosted the Bletchley Summit in November 2023, producing the Bletchley Declaration on frontier AI safety, and co-hosted the AI Seoul Summit in May 2024, at which governments and companies agreed on commitments and built a global network of safety institutes.

In a related development, UK policy is to treat compute capacity as critical infrastructure. Following the [Future of Compute Review \(2023\)](#), the government invested in the National AI Research Resource (AIRR) and in exascale-class facilities. A flagship development, the Isambard-AI supercomputer in Bristol, came online in July 2025, providing UK researchers and startups with access to world-class compute.

To drive adoption, Innovate UK, a public funding agency, has launched [BridgeAI](#), a £100m+ programme targeting sectors with high economic potential but lower AI maturity, such as agriculture, construction, creative industries and logistics. In parallel, UK Research & Innovation (UKRI), the umbrella body for the UK's publicly funded research councils, and the Alan Turing Institute, the UK's national research institute for AI and data science, have run the long-standing [AI for Science & Government \(ASG\)](#) programme, seeking to embed AI in health, environment, engineering and public-sector missions. In the health sector, the [NHS AI Lab](#) (2019–2025) has served as a testbed for deploying AI safely in healthcare.

In 2025 the government published an [AI Opportunities Action Plan](#) setting out 50 recommendations drafted by the tech entrepreneur Matt Clifford, aimed at 'ramping up AI adoption across the UK to boost economic growth, provide jobs for the future and improve people's everyday lives'. The Action Plan envisages AI playing a major role in the current government's 'pro-growth' agenda.

Together, these elements constitute the UK's strategy for AI: invest in inputs (compute, R&D, talent); de-risk adoption ([BridgeAI](#), [NHS AI Lab](#)); and govern through sector regulators applying common principles, rather than a single law. At the same time, the UK is seeking to build a strong international brand around AI safety. In 2025, the government's position is that this strategy is maturing: compute resources are operational, regulators have published their AI plans, and the UK is consolidating its place in the global AI-safety architecture. British AI companies are estimated to contribute £11.8 billion to the UK economy, double the amount in 2023. The government is

currently aiming to stimulate the AI sector further through deregulation ('[slashing red tape](#)'). In the medium term, a [Frontier AI Act](#) aimed at risks arising from the more advanced models and putting into statutory form currently voluntary undertakings on AI safety is a possibility, but is [not currently government policy](#).

2.2 Defining AI

One of the notable features of the 2023 White Paper was that it deliberately avoided a rigid statutory definition of AI or AI system, again in contrast to the more prescriptive EU AI Act ([Mayer Brown](#)). The UK government argues that this flexibility will make the framework for AI more resilient as technologies evolve. For some purposes, however, an AI definition is seen as useful. In February 2024 the ministry with responsibility for AI, the Department for Science, Innovation and Technology (DSIT), issued [guidance for regulators on implementing the UK's AI principles](#). This guidance defined AI systems broadly as including any product or service that is both adaptable and autonomous, encompassing everything from narrow AI tools to advanced frontier models. It defined AI agents as autonomous systems capable of completing multi step tasks like web browsing or equipment control, and mapped the AI lifecycle from research and training through deployment, maintenance and decommissioning. It also clarified the roles of developers, who design, train and adapt AI models, deployers, who supply or integrate AI into products or services, and end users, who ultimately use or benefit from AI outputs. The DSIT guidance also distinguished between narrow AI, designed for single purpose tasks such as sentiment analysis, and frontier AI, referring to advanced models capable of a wide range of functions at or beyond the level of today's most powerful systems. The guidance is intended to give regulators a practical taxonomy for applying the five principles in their respective sectors, while retaining the agility to adapt as AI technologies continue to advance.

2.3 AI-related Law: Overview

Although the UK does not have a single AI Act or equivalent measure, an emergent AI law exists in the form of international commitments, domestic legislation which predates the appearance of AI, and emerging proposals.

In September 2024 the UK signed the [Framework Convention on Artificial Intelligence](#), developed by the Council of Europe. This is the first international treaty of its kind and is legally binding. It commits signatory states to put in place measures that address risks to human rights, democracy and the rule of law arising from the use of AI. The UK will therefore be required to implement domestic measures to meet these obligations.

Domestically, there are already several statutes that apply to AI-driven activity. The [Online Safety Act 2023](#), although not AI specific, places legal duties on online platforms to tackle illegal and harmful content, particularly where algorithmic recommendation or moderation systems are involved. Data protection law, including the [UK GDPR](#) and the [Data Protection Act 2018](#), continues to govern the use of personal data in AI systems. The Equality Act 2010 applies where AI is used in ways that could lead to discriminatory outcomes. Consumer protection law, including the [Consumer Rights Act 2015](#), is relevant where AI products or services are offered to the public. Intellectual property law also applies: the UK courts have clarified that AI systems cannot be recognised as inventors for patent purposes ([King & Spalding](#)), and there is a continuing debate about the implications for copyright law of data scraping.

In terms of new legislation, there are important proposals under discussion. The Artificial Intelligence (Regulation) Bill ([Kennedys Law](#)) was reintroduced in March 2025 as a Private Member's

Bill. It would create a statutory AI Authority, require mandatory impact assessments for certain AI systems and move elements of the government's voluntary framework into binding law. Its future, however, is uncertain given its status as a backbench (Private Member's) Bill without government support.

The government announced in the 2024 King's Speech the government's intention to introduce a Bill to strengthen cyber-security requirements for critical infrastructure and digital services. While not written solely for AI, its provisions are intended to affect AI systems used in sensitive or high-risk environments. The [Cyber Security and Resilience \(Network and Information Systems\) Bill](#) was given its first reading in the House of Lords in November 2025.

Use of AI in criminal justice, risk assessment, digital-evidence triage, and pattern recognition, raise acute fairness and procedural-rights issues. The [EU AI Act](#) draws red lines and imposes safeguards. Notably, Article 5 prohibits certain practices outright, including using AI to make risk assessments of natural persons to predict the risk of committing a criminal offence based solely on profiling or personality traits; any supportive use must be anchored in objective, verifiable facts and accompanied by human assessment. These prohibitions started to apply in early 2025, with further safeguards phasing in across 2025-2027. Practitioner and official summaries emphasise the staged nature of these bans and the associated governance duties. Consistently with its general position of avoiding a horizontal AI measure akin to the AI Act, the UK has not enacted a criminal-justice-specific AI law. Instead, its regulatory programme assigns sector regulators to manage risks such as discrimination, contestability and explainability using existing powers, with central coordination via the AI principles. This is reflected in the 2024 government response and subsequent regulator workplans ([A Pro-Innovation Approach to AI Regulation](#)). However, the practical upshot may not be so different: systems affecting liberty or rights in the context of criminal justice must preserve meaningful human discretion and be contestable with evidence trails, even if the UK relies on guidance and sectoral enforcement rather than a single statute.

2.4 The Trusted Third-party AI Assurance Roadmap

Part of UK AI policy is to build confidence in AI systems, drive innovation, and boost economic growth through support for the UK's [AI assurance market](#), currently valued at £1.01 billion gross value added (GVA) in 2024 with potential to reach over £18.8 billion GVA by 2035. This is an area in which the UK is seen as having a 'unique opportunity to be a world-leader.' AI assurance is deemed 'crucial to ensure that AI systems are developed and deployed responsibly and in compliance with the law.' This approach is intended to foster trust, which in turn should support wider AI adoption and economic growth. The UK is seen as possessing strengths in professional services and technology, positioning it to become a 'world-leader in AI assurance services.' The market is 'nascent but growing,' with significant potential for GVA growth. Third-party providers are highlighted for their 'particularly important role... in independently verifying the quality and trustworthiness of AI systems and providing bespoke, high-quality services to firms who may lack this capability inhouse.' Public confidence in the assuring organisation is seen as just as vital as the assurance process itself.

2.5 Discussion of the UK Government's Approach

Independent policy institutes argue that the UK's approach leaves notable safety and accountability gaps. The Ada Lovelace Institute warns that, as things stand, no UK regulator is explicitly empowered to inspect internal AI safety policies, judge their adequacy or mandate fixes for unsafe systems, leaving the public reliant on private actors' self-assessment. Their take on a mooted UK AI Bill highlights the absence of general powers to halt or withdraw unsafe foundation models and the lack of a single authority for general-purpose AI. Public opinion data point in the same direction: a

nationally representative survey by the Ada Lovelace Institute and the Alan Turing Institute reports that 72% of the UK public would feel more comfortable with AI if there were stronger laws and regulation, up from 62% in 2023 ([Ada Lovelace Institute](#); [Alan Turing Institute](#)).

On legislative trajectory and timing, law firm Kennedys' walkthrough of the Private Member's Artificial Intelligence (Regulation) Bill [HL] explains how peers have sought to fill the vacuum with risk-classification and coordination powers, even though the government's own programme continues to favour a light-touch, sector-led approach grounded in the five principles from the 2023 White Paper of safety, transparency, fairness, accountability and contestability ([Kennedys Law](#)). The King & Spalding July 2025 round-up ([King & Spalding](#)) noted that the government had declined to use the new [Data \(Use and Access\) Act 2025](#) (DUAA) to legislate on the AI-copyright issue, instead committing to produce by-deadline reports and impact assessments on options ranging from 'no change' to a commercial text-and-data-mining exception. Against the backdrop of government inaction, the data protection regulator, the ICO, has seemed ready to fill the gap, signalling that it will develop a statutory code of practice on AI and automated decision-making, moving some of its current guidance onto a binding footing ([King & Spalding](#)). Meanwhile, the government is pushing ahead with adopting AI across the public sector. This is being led by the [AI Playbook](#), which sets expectations for safe adoption across departments and arm's-length bodies and updates the earlier Generative AI framework.

On growth and infrastructure, the law firm Clifford Chance's analysis stresses both the opportunity narrative and the tension that the government's approach creates for sector regulators, who must promote innovation while enforcing existing mandates; it also notes early market investigations touching AI services, underscoring that competition and consumer law will be active levers even in the absence of an AI Act. Pinsent Masons reads the government's Action Plan as a conditional nudge: if sector regulators cannot demonstrably enable innovation within their remits, a shift to a more centralised model is on the table ([Pinsent Masons](#)).

Some stakeholders are treating 'no single AI law yet' as 'regulate via many.' A&O Shearman's briefings crystallise the point: the UK is letting expert regulators like the ICO, CMA, Ofcom and the FCA lead through guidance, supervision and sandboxing ([A&O Shearman](#)). The regulator-first posture is echoed in sector updates, such as FCA's AI Sprint summary and Treasury Committee calls for evidence on AI in financial services ([A&O Shearman](#)).

In short, the UK is trying to square growth and safety by empowering existing regulators, equipping the public sector with operational guidance, investing in compute and assurance markets, and delaying horizontal AI legislation until it can target 'frontier' risks and settle the copyright-training debate. Independent analysis is supportive of agility but sceptical about enforcement powers and system-level risk control. In the absence of an overarching legal instrument for AI, the expectation is that policy will evolve via individual regulators' statutory tools, cross-regulator coordination and focused consultations, with timelines shaped by DUAA reporting duties and the ICO's planned code of practice ([Ada Lovelace Institute](#); [King & Spalding](#)).

3. Data protection Law

3.1 ICO Guidance

The UK's data protection regulator, the Information Commissioner (ICO), has issued a set of guidance documents to help regulators and organisations manage the risks of AI while staying aligned with data protection law. These documents sit alongside the government's pro-innovation AI

regulatory principles and are intended to show how regulators should interpret and apply them in practice.

The government Policy Paper, [Implementing the UK's AI Regulatory Principles: Initial Guidance for Regulators](#), published in February 2024, consists of guidance explaining how regulators should operationalise the five White Paper principles of safety, transparency, fairness, accountability and contestability. It stresses that the principles are not prescriptive but should be interpreted flexibly according to each regulator's remit and maturity. Regulators are encouraged to draw on technical standards such as ISO/IEC 42001 on AI management systems and ISO/IEC 22989 on AI concepts, but without mandating their use. The ICO also advises regulators to produce outcome-based or sector-specific guidance and, where possible, to collaborate across sectors to avoid duplication. The guidance identifies a central function within the Department for Science, Innovation and Technology (DSIT) as a resource for sharing risk analysis, best practice and coordination. The publication is described as the first phase of a three-stage process, with further detail and collaborative tools to follow in later phases. Building on the Policy Paper, in April 2024 the ICO released [Regulating AI: The ICO's Strategic Approach](#). This strategy document sets out how the ICO sees its own role in relation to AI. It positions the ICO as a de facto AI regulator on the premise that personal data flows through the entire AI lifecycle, from development and training to deployment. The approach is explicitly risk-based: the ICO expects organisations to identify and mitigate risks, but not to eliminate them entirely. The document maps existing data protection principles directly onto the government's AI principles, showing that much of the AI agenda can be delivered under existing law. It also highlights the ICO's practical support for existing initiatives, such as the [AI and Data Protection Risk Toolkit](#) and its Innovation Hub and Regulatory Sandbox, which help innovators test systems in a controlled environment. The ICO makes clear, however, that it will take enforcement action where risks to privacy are serious, for example in the use of biometric data or children's information.

Alongside these strategic documents, the ICO maintains detailed [Guidance on AI and Data Protection](#), first published in March 2023 and now under review in light of the legislative changes contained in the [Data \(Use and Access\) Act 2025](#). This guidance is structured around the core data protection principles, translated into AI contexts. It includes dedicated sections on accountability, transparency, lawfulness, fairness, accuracy, security and individual rights. It offers practical explanations, for example on how to explain AI-based decisions to individuals, how to handle bias and discrimination risks, and how to ensure statistical accuracy. It also contains a glossary and a toolkit that organisations can use to assess and manage AI-related risks.

In June 2025 the ICO launched an [AI and Biometrics Strategy \(A&O Shearman\)](#) that promises a proactive agenda for high-risk applications, including a statutory code of practice for AI, audits of police facial recognition and guidance on using personal data to train generative models, framed explicitly as a trust-building programme.

3.2 Reform of the UK GDPR

The [Data \(Use and Access\) Act 2025](#) (DUAA) amends the UK GDPR, the Data Protection Act 2018, and [Privacy and Electronic Communications Regulations 2003 \(PECR\)](#), with the stated aims of economic growth, service improvement and practical simplification. Changes include recognition of certain 'compatible' re-uses, a new list of recognised legitimate interests as a lawful basis, and relaxed conditions for automated decision-making, alongside significantly increased PECR fines aligned with UK GDPR maxima (up to £17.5m or 4% of global turnover) for cookies and electronic-marketing breaches ([Law Society](#)). These reforms aim to shape both in-house AI deployments and the compliance perimeter for any scraping that touches personal data.

The government's overview groups DUAA's data-protection measures into nine themes. Three are expected to have the most impact on day-to-day practice:

- Automated decision-making (ADM): the UK GDPR becomes more permissive about decisions based solely on automated processing that produce legal or similarly significant effects but with codified safeguards (information, the ability to challenge, and meaningful human intervention). The [Guidance](#) and [Explanatory Notes](#) also define what counts as 'entirely automated' and create powers to clarify the circumstances and safeguards.
- Subject access (DSARs): the DUAA introduces a 'stop-the-clock' mechanism (deadlines can be paused while awaiting required clarifications) and confirms that organisations must make reasonable and proportionate searches. The Notes spell out the pausing/extension mechanics ([Explanatory Notes](#)).
- Recognised legitimate interests (RLI): a new lawful basis under Article 6(1)(ea) for certain defined activities listed in a new Annex 1, with regulation-making powers to update that list; the right to object still applies and public authorities cannot rely on RLI for their public tasks. The ICO's DUAA hub explains the intent and initial scope ([Explanatory Notes](#); [ICO Guidance](#)).

Also flagged up in the new law are the following issues: children's data protections for online services likely to be accessed by children; clarifications for scientific research (including commercial research); international transfers simplifications; complaints handling requirements; and tweaks to cookies/other storage & access technologies for certain low-risk uses. PECR remains in force alongside the UK GDPR ([Explanatory Notes](#); [ICO Guidance](#)).

The ICO has started to operationalise the new DUAA through guidance updates and public consultations. On 21 August 2025 it opened consultations on recognised legitimate interests (draft guidance) and complaints handling; the consultation page confirms the scope and timetable. Further guidance waves are expected as commencement regulations land ([ICO Consultation](#)). The European Commission, as part of its remit to review data flows between the UK and EU, is conducting a review of the UK's updated framework and has launched the process to adopt renewed adequacy decisions ([European Commission Adequacy Decisions](#)).

3.3 Data Protection Law Relating to Data Scraping, Cleaning, and Training-Data Transparency

A core compliance issue for AI model builders is establishing a lawful basis for, and ensuring transparency in relation to, training on web-scraped personal data. In the UK, the Information Commissioner's Office (ICO) has affirmed through its generative AI consultation that 'legitimate interests' is effectively the only viable lawful basis for large-scale scraping of personal data to train models (outside very narrow contexts). However, relying on the 'legitimate interests' defence requires passing a rigorous three-part test: a valid purpose, necessity of using personal data (that is, there is no less intrusive alternative), and a balancing of interests that does not override data subjects' rights. The ICO stresses that the onus is on developers to demonstrate necessity, for example, by showing why methods other than indiscriminate web scraping (such as using non-personal or licensed data) are not suitable. The solicitors' professional body, the [Law Society](#), has reinforced the ICO's stance, warning that users must invest in governance and transparency in order to pass the legal balancing test. In practice, there is a tension between the government's innovation-first rhetoric and regulators' insistence on compliance and accountability.

According to the [ICO](#), AI developers must implement strong transparency measures and opt-out mechanisms; otherwise, they will likely fail the balancing test due to the 'high-risk, invisible' nature of covert scraping. The ICO warns that lack of transparency (and the consequent inability of people to exercise their rights) means developers will struggle to justify scraping on legitimate interest

grounds. To mitigate this, developers are expected to provide accessible notices about the data being collected (such as public privacy notices listing data sources/types) and avenues for individuals to request removal. This aligns with UK GDPR Article 14 obligations and the ICO's guidance to the effect that where direct notice to each person is impracticable, organisations should publish clear, accessible information about the data collected, the purposes and legal basis, and how people can exercise opt-out or deletion rights.

Continental European regulators are converging on similar principles. France's data protection authority, CNIL, has issued detailed AI guidance emphasising necessity, proportionality, and risk controls across the data lifecycle, from collection and cleaning of data, through annotation and training, to evaluation and deployment. CNIL's guidance on using legitimate interest as a legal basis echoes the UK ICO's: the interest pursued must be specific and lawful, the processing must be necessary (no less intrusive means available), and impacts on individuals' rights must be balanced and mitigated ([Hogan Lovells](#)).

CNIL explicitly notes that a controller should assess alternatives and 'encourages the use of technologies that allow model training with less reliance on personal data', underscoring data-use minimisation. It also provides criteria for the balancing test (including the nature of data, reasonable expectations of data subjects, and potential impacts) and highlights the need for measures to reduce risks including bias or privacy breaches during both development and deployment. Across the EU, there is a clear message that 'publicly available' does not equate to 'freely usable' for AI training. Data protection laws attach wherever personal data are processed, even if scraped from public websites. European regulators, when assessing the operations of AI-related tech firms including Clearview AI and OpenAI, have argued that public accessibility of personal data on its own does not grant a controller a general licence to reuse and further process that data ([Digicon](#)).

According to CNIL, reuse can be highly intrusive and unforeseeable to individuals, violating principles of transparency and purpose limitation. GDPR obligations, including transparency, purpose specification, data minimisation, and accuracy, still apply to public data. This means that data cleaning and curation steps are not just a matter of technical hygiene but legal compliance measures. CNIL's position is that organisations need to filter out or avoid unnecessary personal data and sensitive data during preprocessing. Relatedly, CNIL recommends that training datasets be 'selected and cleaned to optimise algorithm training while avoiding the use of unnecessary personal data' ([CNIL](#)). Removing or masking direct identifiers, deduplicating entries, and excluding special-category data are seen as prudent steps to meet data minimisation and privacy-by-design duties. In short, scraping large swathes of personal info without safeguards is fraught with legal risk – firms must justify why each piece of personal data is needed and show they've taken steps to limit usage to what is genuinely necessary ([Hogan Lovells](#)).

The EU's developing AI regulatory framework adds another layer of transparency expectations even before formal enforcement begins. Under the EU AI Act, which will impose product-lifecycle governance requirements, developers of foundation models or general-purpose AI are encouraged (via an interim Code of Practice to document and disclose their data sources, usage rights, and safety testing ahead of the law's full effect ([Code of Practice on General Purpose AI](#))). The Code of Practice focuses on three key areas: transparency, copyright/respect for intellectual property, and safety/security in advanced AI systems. Among other things, the Code of Practice calls on model providers to publish a summary of the datasets used (including any copyrighted content), implement measures to honour copyright reservations (for example, by respecting website opt-outs in robots.txt), and conduct thorough safety tests (such as adversarial or 'red-team' evaluation of models) ([Paul Weiss](#)).

This initiative, backed by EU regulators, reinforces the point that even during this transition period for the implementation of the AI Act, companies should be transparent about training data provenance and rights and proactively address risks, rather than assuming that anything on the open web is fair game. The ICO's guidance, CNIL's recommendations and the EU's code of practice point to a common conclusion: AI developers must treat data sourcing and cleaning as integral compliance steps. Public personal data is not 'free': AI developers need a solid lawful basis for their activities, and must apply data protection principles at every stage to avoid regulatory backlash or litigation ([Hunton](#)).

The European Commission's Digital Omnibus initiative, announced on 19 November, envisages revisions to EU digital and AI-related laws, including the AI Act and the GDPR, with a view to 'streamlining' rules on AI, cybersecurity and data protection, and enabling 'Europe's businesses, from factories to start-ups, will spend less time on administrative work and compliance and more time innovating and scaling-up' ([Digital Omnibus](#)). Among other things it proposes extending the timeline for introducing rules relating to high-risk AI systems and introducing 'targeted simplification measures to ensure timely, smooth, and proportionate implementation of certain of the AI Act's provisions'. The long-term implications of the Digital Omnibus for the UK are unclear. Since the UK is not subject to the AI Act and has already set out its own, distinct path to AI governance and regulation, it is not immediately affected by EU developments. If the Digital Omnibus is adopted in something like the form proposed (which is unclear at the time of writing), the resulting liberalisation of EU rules may lead to a degree of convergence between UK and EU law practice, potentially eroding the competitive advantage sought by UK-based policy makers.

4. Intellectual Property Law

4.1 Copyright: the Current Law

In UK law, copying protected works to train AI generally requires the permission of the copyright holder, unless an exception applies. The only cross-cutting exception relevant to training is currently the text and data mining (TDM) exception in [s.29A of the Copyright, Designs and Patents Act 1988](#), which is narrowly limited to copies for text/data analysis for non-commercial research where the user already has lawful access; there is no general commercial TDM exception. Government guidance from the [Intellectual Property Office](#) states this plainly. The IPO's [Copyright and AI Consultation](#), beginning in December 2024, explored moving to a broader, rights-reservation/opt-out model and related transparency measures, but this has proved controversial.

Section 29A CDPA permits copying 'for text and data analysis for non-commercial research' by a person with lawful access (for example, a paid subscription). The exception covers making copies for analysis; it does not grant broader reuse rights. The [IPO guidance](#) reiterates both limits (non-commercial only; lawful access is still required). The consultation considers an opt-out-based commercial TDM route, closer to the EU model; outcomes are still 'analysis pending'. As discussed earlier (section 3), web-scraping where personal data is involved also interfaces with GDPR rules.

UK law recognises '[computer-generated works](#)': where there is no human author of an LDMA work, the author is deemed to be the person who made the arrangements, and the term is 50 years from the end of the year of creation ([CDPA s.9\(3\) and s.12\(7\)](#)). After reviewing this area in June 2022, the government decided not to change the CGW rule at that time; the 2024–25 consultation re-opens the question alongside options including output labelling.

Beyond copyright in individual works, the UK [sui generis Database Right Regulations](#) protect against extraction and re-utilisation of a database where there has been substantial investment. Case law

(*BHB v. William Hill*, 2005) clarifies scope and infringement issues including those arising from repeated or systematic extraction of parts of datasets. In the case of transient technical copies made by ordinary browsing, the decision of the UK Supreme Court in *PRCA v. NLA* (2013) confirms the application of the temporary copies exception.

The training of AI on web-based content implicates not only classical copyright but also potentially sui generis database rights and certain contractual limitations on use. While the UK retains the concept of ‘computer-generated works’, there is growing doubt about the utility of these provisions in resolving the question of whether an AI system itself can be deemed a creator or infringer. This uncertainty is particularly salient given that existing intellectual property categories were not designed with large-scale, machine-led synthesis in mind.

4.2 Database Rights and Structured Data Extraction in Detail

Web scraping, the automated harvesting of data from websites, has become integral to assembling the large datasets used for training AI models. In the UK, the legality of this practice is uncertain and highly context-dependent. No single statute outright forbids web scraping, but ‘unauthorised use of publicly available web content can amount to a breach of contract, infringement of intellectual property rights, and a criminal offence in some circumstances’ (*Bird & Bird*). In particular, scraping implicates UK copyright law and the sui generis database right, and it may trigger criminal liability under the *Computer Misuse Act 1990* if done without the data owner’s consent. These overlapping legal frameworks create a complex patchwork of obligations and exceptions that make the permissibility of web scraping far from clear-cut.

Web scraping involves making copies of website material (for example, downloading HTML or text to parse it), so unless an exception applies or the use is licensed, it risks copyright infringement (*HFS Kramer*). UK law does provide a narrow exception for transient or incidental copies as part of a technical process (implementing Article 5(1) of the EU Copyright Directive). In the *Newspaper Licensing Agency v. Meltwater* litigation (2013), the UK Supreme Court recognised that merely browsing a web page, which creates temporary copies in the user’s cache and screen, falls under this transient copying exception and thus does not require the copyright owner’s permission (*RPC Legal*).

In this case, users of a news aggregation service were held not to need a licence just to view copyright snippets online, as the copies made in the act of browsing were temporary and had ‘no independent economic significance’. However, the Court stressed that this defence applied only to ephemeral copies for viewing, not to more permanent reproductions. Web scraping typically goes beyond mere transient caching, it downloads and stores data for later use, and therefore would not be protected by the “browsing” exemption. In the *Meltwater* scenario, while end-users escaped liability for viewing content, the service provider itself still needed a licence to reproduce and distribute the material in its reports). By analogy, an AI developer which systematically scrapes protected works to build a training dataset is engaging in acts of reproduction that are not purely transient. In the absence of a specific exception, each non-trivial copy made during scraping (e.g. copying articles, images or code from the web) can infringe copyright if done without authorisation (*RPC Legal*).

One potential shield for scrapers in the UK is the ‘text and data mining’ exception introduced in 2014. Section 29A CDPA permits copying works for text and data analysis but only for the purpose of non-commercial research and only when the researcher has lawful access to the material. This limited exception was intended to remove barriers for data mining in scientific research, but it does not cover commercial AI training or other uses outside pure research, nor does it apply to database rights (*HFS Kramer*). In practical terms, a company crawling websites to gather data for a machine

learning model cannot rely on section 29A if the mining is part of a commercial endeavour. Any copies made in the process would thus require a licence or another defence to avoid infringing copyright.

The narrow scope of the UK's mining exception stands in contrast to the EU, which in 2019 adopted broader text and data mining exceptions, one mandatory for non-commercial research and one optional for other purposes, the latter allowing rights-holders to opt out ([HFS Kramer](#)). The UK chose not to implement the EU's 2019 provisions post-Brexit. Initially, the UK government proposed to expand the TDM exception to cover mining 'for any purpose'. This was a radical change that would have allowed web scraping and data mining for commercial AI development by default ([HFS Kramer](#)).

The proposed exception would still have required 'lawful access' to the source content and would have permitted rights-holders to charge for access to their data (for example via paywalls or subscriptions), but rightsholders would not have been able to object to or charge specifically for the act of mining itself. This plan, announced in 2022 as part of a pro-innovation strategy, was intended to 'ensure the UK's copyright laws are among the most innovation-friendly in the world' and make the UK a global hub for AI. However, it sparked intense backlash from publishers and creative industry groups, who saw it as undermining their copyright interests ([HFS Kramer](#)).

By early 2023 the government reversed course: it announced it would not proceed with the broad TDM exception. Instead, the status quo remains that the only TDM exception is for non-commercial research, a limitation that 'may mean that AI developers are more cautious about doing R&D work in the UK' than they would be under a more permissive regime ([HFS Kramer](#)). Absent specific permission or licensing, using web scraping to obtain training data for commercial AI systems continues to carry a high risk of copyright infringement under UK law.

Even where the individual pieces of content gathered by a scraper (for example, factual data or lists) are not themselves protected by copyright, the act of scraping may implicate the UK's sui generis database right. This is a separate intellectual property right, originating from EU law (the Database Directive 96/9/EC), which protects substantial investment in the collection and arrangement of data. The UK Copyright and Rights in Databases Regulations 1997 grant database makers the right to prevent extraction or reutilisation of all or a substantial part of a database without consent. The database right is automatic and does not require registration; it arises so long as there has been a 'substantial investment in obtaining, verifying, or presenting' the contents of a database. If a web scraper gathers a significant portion of data from a structured collection (for example, by copying thousands of entries from a company's price database or flight schedule), it may be extracting a substantial part of a protected database, thus infringing the database right ([Bird & Bird](#)).

Notably, 'substantial' here can be assessed quantitatively or qualitatively, so that the repeated extraction of many insubstantial portions can amount to extracting a substantial part in aggregate. Thus deploying a bot to scrape small bits of data from a database over and over can legally equate to taking a large chunk in one go. For example, a price comparison scraper that continuously queries a competitor's database for product prices could violate the database right if the target's data compilation required substantial investment to create ([Bird & Bird](#)).

A leading illustration is the case of [British Horseracing Board Ltd v. William Hill Organisation Ltd](#). There, the British Horseracing Board (BHB) had compiled an official database of horse racing times, runners, and riders. Betting firm William Hill was scraping and reusing those race schedules on its website without BHB's permission. The question was whether BHB's database was protected and, if so, whether William Hill's use amounted to extracting a substantial part. In 2004 the Court of Justice

of the EU (CJEU) held that BHB's database did *not* qualify for sui generis protection because BHB's investment was primarily in creating the racing information (the list of runners and race details) rather than in obtaining or verifying data from external sources. As BHB had no database right to assert, William Hill's scraping was lawful.

At the same time, this decision made it clear that the database right will not protect every collection of data. It protects the maker's investment in collecting existing information, but not investment in generating content ex nihilo. When the right does apply, it gives database owners potent control over data scraping. Taking an insubstantial portion repeatedly (say, daily race results) can infringe the database right if it undermines the investment made in the entire database. Thus, web scrapers must assess not only the copyright position, but also whether the target website's content is part of a protected database. If so, scraping large or cumulative portions without consent could lead to liability for database right infringement ([Bird & Bird](#)).

In addition to IP rights, many websites deploy contractual terms of service that explicitly forbid data scraping or crawling. If a scraper is bound by such terms (for instance, through a click-through agreement or other notice), scraping the site can constitute a breach of contract. The legal enforceability of website terms against scrapers can be nuanced, however. Much depends on whether the terms were reasonably communicated and agreed to by the user. In practice, commercial scrapers often fall back on publicly available data without any explicit agreement (for example, sending HTTP requests), which raises the issue of implied consent.

UK courts have recognised that merely making data publicly accessible does not necessarily grant an unconditional licence to harvest it in bulk). The CJEU in *Ryanair v. PR Aviation* confirmed that where database content is not protected by IP rights, a data owner may be able to rely on contract law to restrict scraping of that content. In that case, Ryanair's website terms (which the scraper had accepted) prohibited unauthorised extraction of flight pricing information; because the data (timetables/fares) was not protected by the database right, the question became purely one of contract, and the court left the door open for Ryanair to enforce its clickwrap terms against the scraper ([Bird & Bird](#)).

4.3 Post-Brexit Legal Changes

In the UK post-Brexit, EU decisions such as *Ryanair* remain persuasive and reflect broader principles of law which remain relevant. Contractual restrictions on web scraping can be binding, especially against users who knowingly agree or who are regarded as sophisticated commercial actors rather than average consumers ([Bird & Bird](#)). The remedies for breach of such terms can include damages or an injunction to stop the scraping. Moreover, clearly drafted terms prohibiting scraping bolster other legal avenues. They can be used to negate any argument that the scraper had an implied licence, and to help establish that any access for scraping was explicitly unauthorised, which may also be relevant to potential [Computer Misuse Act](#) violations ([Bird & Bird](#)).

Beyond civil IP and contract law, web scraping can stray into criminal territory if it involves unauthorised access to computer systems. The [Computer Misuse Act 1990](#) (CMA) makes it an offence to 'secure unauthorised access' to any program or data on a computer. In essence, if a scraper accesses data without the owner's permission, this could be construed as a form of hacking, even if the data was obtained over the open web. To date, there is no UK case law definitively applying the CMA to web scraping, but legal commentators note that the Act's broad language 'includes "hacking"' and 'may catch data scraping' in cases where 'the website owner does not authorise the type of access made by a scraper' ([Bird & Bird](#)).

A key issue then is authorisation. A scraper who circumvents password protections or ignores a deliberate block (like a IP ban or anti-scraping mechanism) is more clearly acting ‘without authorisation’. Even if the scraped data is publicly visible on the site, using automated bots might be outside the scope of what the service provider consents to, especially if forbidden by terms of use. In order for CMA liability to arise, the person must know (or at least be aware) that the access is unauthorised. Clear no-scraping terms on a site help put scrapers on notice that their automated access is unauthorised. A would-be defence is to argue that making a website publicly accessible implies permission for anyone (human or bot) to access and read the content ([Bird & Bird](#)).

However, this argument is unlikely to succeed if the manner of access is qualitatively different from ordinary use. Courts would probably agree with the view that implied consent to view does not equal consent to scrape at scale. In fact, the presence of an explicit prohibition would almost certainly negate any implied licence. Thus, a scraper proceeding in the face of ‘no scraping’ notices could be found to have knowingly exceeded authorised access. Breaching the CMA is a criminal offence punishable by fines or even imprisonment). Although enforcement in the scraping context has been rare (and typically aggrieved companies pursue civil remedies first), the risk is real. A data owner could refer such unauthorised access to law enforcement or even undertake a private prosecution under the CMA ([Bird & Bird](#)).

The CMA’s application to scraping may ultimately be tested in court as disputes over large-scale data extraction become more common. In the interim, the mere possibility of criminal liability further underscores how legally perilous web scraping can be in the UK when done against the wishes of the data owner.

The ambiguous legal status of web scraping has significant consequences for AI development in the UK. Modern generative AI systems rely on ingesting massive datasets (text, images, code) often sourced from across the internet. If every scrap of copyrighted or database-protected material requires prior licensing, the transaction costs and legal uncertainties could stifle innovation. AI developers face a dilemma of either invest in obtaining licences for vast amounts of data (if even feasible), limit training to non-copyright or public domain data, or proceed with scraping at legal risk.

The current UK framework, with its ‘piecemeal collection of protections’ in copyright, database right, contract and privacy law, is widely seen as confusing and even ‘prohibitive’ for data mining endeavours. Academics note that the UK’s limited TDM exception addresses ‘only one facet of the multi-layered protections for data’, leaving those who wish to scrape and analyse data to ‘balance a complex range of legal considerations’, often at the risk of infringing another’s rights. This multi-layered legal risk is argued by some to have a chilling effect on data analysis and AI research: organisations may avoid beneficial projects for fear of litigation, or shift AI development to jurisdictions perceived as more permissive or clearer in their text and data mining laws ([CREATE](#)).

Policymakers in the UK are aware of this tension between fostering AI innovation and protecting rightsholders. There is ongoing debate, and indeed policy movement, around how to recalibrate the legal framework. The UK government’s proposed Frontier AI Bill is expected to tackle some of these issues head-on. Initially, in its 2023 AI regulation policy paper, the government signalled a light-touch, principles-based approach rather than a comprehensive statute like the EU’s AI Act. However, as the copyright and data mining controversy has unfolded, ministers have acknowledged the need for AI legislation to address the status of training data.

4.4 Copyright and data scraping: the *Getty v. Stability AI* litigation

The UK's flagship copyright test case is *Getty Images v. Stability AI* (2025). Getty alleges that Stability AI copied millions of its copyrighted images without permission to train its image generation model, Stable Diffusion. The case is the first of its kind in the UK and raises questions around the reproduction right, originality thresholds, and the potential availability of statutory defences.

As the trial opens, commentators emphasise that the judgment could reset market practice and influence the UK's attractiveness for AI development, given the centrality of training data and the unsettled interface between copyright exceptions and model training. As Pinsent Masons' Cerys Wyn Davies observed, the ruling 'could have a major bearing on market practice and the UK's attractiveness as a jurisdiction for AI' (Reuters report). The case therefore functions as a focal point for the broader policy debate over upholding intellectual-property rights while enabling AI innovation.

The significance of *Getty* was seen as turning on three issues. Firstly, input legality: does large-scale web scraping of copyrighted images for model training fit within UK exceptions or require licences? Secondly, output liability: if the model emits images substantially similar to protected works, how should infringement and defences be assessed? Thirdly, remedies and transparency: to what extent will courts require disclosures about training data and impose injunctive or monetary relief that shapes industry norms? A ruling that narrowed 'lawful access' or favoured rightsholder transparency and opt-out frameworks was thought to run the risk of driving UK market behaviour toward licensing and provenance controls. Conversely, a more permissive view could catalyse model development but intensify calls for legislative reform. The litigation was thought to be particularly significant because the UK does not recognise an open-ended fair use doctrine like the United States, enabling defendants to invoke transformative use or broader public interest justifications going beyond the the narrowly tailored CDPA exceptions.

In January 2025 the High Court issued a case-management judgment; during the June 2025 proceedings the Court of Appeal ruled on a mid-trial pleading issue. The scope of the trial was narrowed down significantly when it was conceded shortly before closing submissions that none of the training and development of the Stable Diffusion model had taken place in the UK. The remaining claims related mostly to secondary copyright and trading infringements which were said to have occurred when outputs from the model were imported into the UK. In her [ruling](#) of 4 November 2025, the judge held against Getty on this issue, on the grounds that Stable Diffusion outputs did not contain any 'infringing copies' of Getty's works at the point when they were imported:

The Model itself does not store any of those Copyright Works; the model weights are not themselves an infringing copy and they do not store an infringing copy. They are purely the product of the patterns and features which they have learnt over time during the training process (para [600]).

In another aspect of her ruling, however, the judge considered that electronic copies stored in an intangible form could in principle be 'articles' for the purpose of copyright infringements. This opens the way to claims in cases where the training of models takes place within the UK, and may be persuasive in other jurisdictions, including in the USA where Getty is pursuing separate litigation against Stability AI ([Pinsent Masons](#)).

4.5 Reform of Copyright Law to Permit Data Scraping

The 2024-25 [consultation on copyright and AI](#) proposed an 'exception with rights reservation.' This would allow AI developers to mine copyrighted works for training unless rights holders explicitly

opted out of their works being used in this way. The proposal marked a shift from earlier plans to introduce a blanket text and data mining (TDM) exception, which had met fierce opposition. On 16 July 2025, ministers convened a number of AI–copyright working groups (creatives and AI firms) to work up ‘practical, workable’ solutions. Public commentary remains highly polarised. Legal commentators noted that political pressure, particularly from the House of Lords, forced the government to moderate its position, inserting greater emphasis on transparency and safeguards for creators ([Taylor Wessing](#)).

In mid-2025, ministers confirmed that a planned AI Bill had been delayed to 2026 in order to accommodate copyright-related provisions. A June 2025 letter from the Secretary of State for Science, Innovation and Technology stated that the legislation would ‘likely serve as the vehicle to resolve issues relating to AI and copyright law’, noting the establishment of a working group to assess the policy landscape ([K&S Law](#)).

Parallel to the AI Bill deliberations, the government is gathering evidence and evaluating models for how AI developers can legally use copyrighted materials. The Intellectual Property Office (IPO) ran a consultation on copyright and AI (which closed in February 2025), canvassing options that range from maintaining the status quo (and likely facing continued uncertainty and disputes) to requiring explicit licensing for all AI training uses of copyrighted works, or alternatively introducing new exceptions to facilitate AI training ([K&S Law](#)).

As part of the process of adopting the recent Data (Use and Access) Act 2025, a law mainly concerned with data sharing and reforming UK data protection rules, Parliament engaged in a tug-of-war over amendments aimed at AI training transparency. The House of Lords pressed for provisions that would force AI developers to disclose to rightsholders how copyrighted works were used in training AI models, reflecting creators’ demands for accountability. The House of Commons ultimately rejected inserting such rules directly into the data law, deferring the issue to the dedicated AI/copyright workstream.

The compromise, however, was telling. The new DUAA 2025 requires the government, within nine months of its June 2025 assent, to draft proposals for improving transparency to copyright owners regarding the use of their works in AI training ([Hunton](#)). It also mandates an economic analysis of various policy options, including (1) doing nothing (and risking ongoing legal uncertainty), (2) a strict regime of ‘licence required for any AI training on copyrighted content’, (3) a broad copyright exception allowing text and data mining for any purpose (as was briefly proposed earlier), and (4) a narrower exception permitting mining for AI only if rightsholders have not opted out of such use ([K&S Law](#)).

Commentary has argued that the government’s approach risks creating significant uncertainty. Analysts at [Osborne Clarke](#) highlight the point that both copyright and database rights may be infringed by large scale scraping, and that existing exceptions in UK law are too narrow to cover the kind of mass dataset creation used in AI training. Meanwhile, the sector regulator for competition law and policy, the [Competition and Markets Authority \(CMA\)](#), has raised concerns: if access to training data is relaxed without safeguards, dominant firms may consolidate control over the highest quality datasets, undercutting the government’s goal of supporting startups and SMEs.

Strong opposition to the government’s proposals has come from the creative industries. Cultural leaders and trade bodies have argued that any opt out model effectively reverses the burden of copyright protection, forcing creators to police use of their works. As [The Guardian](#) reported, publishers, musicians, and writers described the government’s plans as an existential threat to their

livelihoods. Their resistance has turned data mining into a political economy issue: the state seeks to catalyse AI driven growth while also preserving the UK's globally significant creative exports.

Academic and policy analysts have situated the UK's debate in a wider international context. A [2025 OECD report](#) argued that diverging too far from established copyright norms risks isolating the UK. While a permissive opt out model might attract AI firms, it could also leave UK trained models less interoperable in jurisdictions with stricter copyright regimes, such as the EU.

After intense lobbying from both the creative industries and the tech sector, the UK Government withdrew its 2022 proposal for a blanket TDM exception that would have permitted commercial use of copyrighted works. Instead, a more balanced regime has been proposed, involving an opt-out framework allowing AI developers to scrape data unless the rights holder explicitly reserves their rights.

The Intellectual Property Office (IPO) has taken the lead on consultations, alongside the Department for Science, Innovation and Technology (DSIT). According to the Government's 2024 [consultation](#), AI training would be permitted by default on works where rights have not been reserved, coupled with a transparency obligation on AI developers to disclose their data sources.

This mirrors Article 4 of the EU's DSM Directive 2019/790, which allows TDM for any purpose so long as rights holders have not opted out. The UK's model would incorporate machine-readable signals (such as metadata and robots.txt) to operationalise this right reservation mechanism. Transparency obligations, possibly enforceable through future AI regulation, would ensure that rights holders can identify and contest unauthorised uses.

The UK model would operationalise opt outs through machine readable signals metadata, robots.txt. Transparency measures potentially enforceable through future AI regulation would help rights holders identify and challenge unauthorised uses.

Developers must therefore closely assess the nature of data they use, comply with restrictions, and obtain licences where feasible. UK law does not yet provide a comprehensive answer to 'can I scrape this website for my AI project?'. Legality depends on whose data is used and under what conditions, often falling into a grey zone between lawful innovation and infringement. Ongoing legal and policy processes aim to clarify this, seeking an equilibrium where innovation can progress without undermining creators' rights or incentives ([K&S Law](#)).

4.6 Parliamentary Debates on AI and Intellectual Property

The Government has reiterated in several Parliamentary debates that it is preparing a consultation on AI legislation. In a Lords debate in July 2024, Lord Vallance confirmed that ministers were 'preparing a consultation on AI legislation in order to gather views on the proposals' but resisted calls for immediate publication, stressing that 'the need to get the legislation right for a more widespread AI Bill is important and has to be taken with due consideration. It would be very wrong to try to rush this' ([Hansard](#)).

Peers including Viscount Stansgate pressed for pre-legislative scrutiny, while Lord Holmes highlighted regulatory gaps in areas like hiring and recruitment. Lord Vallance replied that existing regulators would remain the primary oversight bodies, though 'some aspects of AI need to be looked at across AI generally', making consultation the necessary next step.

Across both Houses, ministers have emphasised the desirability of a domain-specific regulatory model in which ‘most AI systems should be regulated by the existing regulators. They are the experts’. To support cross-cutting issues, the Government pointed to initiatives such as the Digital Regulation Cooperation Forum’s AI advisory hub and the Regulatory Innovation Office.

Urgency was a recurring theme in these debates. Lord Clement-Jones warned that ‘state-sponsored hackers are using AI to write malicious code’ and that criminals are using deepfakes for fraud, stressing these harms are ‘real, tangible... happening right now’. Lord Vallance agreed on the seriousness of the risks and cited measures in the Online Safety Act, the Data (Use and Access) Act and the Crime and Policing Bill, while maintaining that a full AI Bill must follow consultation to “get this absolutely right”.

Parliamentarians also examined AI safety testing. Viscount Colville highlighted Google’s release of its Gemini 2.5 model without a safety card as evidence that voluntary codes may be insufficient. Lord Vallance pointed to the AI Safety Institute’s work on frontier testing and vulnerability analysis.

International comparisons featured prominently. Ministers stressed that the UK is taking a ‘rather different approach’ from the EU’s AI Act by relying on existing regulators rather than establishing a single authority. Viscount Camrose noted that more than 150 European businesses had criticised the EU model for ‘rigidity, complexity, overregulation and threat to competitiveness’. While monitoring developments, the Government intends to preserve a lighter, more flexible system.

In a parallel Westminster Hall debate, MPs focused on AI’s impact on intellectual property and the creative industries, which contribute over £120 billion annually and support 2.4 million jobs. MPs expressed ‘deep alarm’ at AI models trained on unlicensed or pirated content. Mr James Frith warned that ‘whole sections of our creative industries’ were having their work taken without permission, likening the situation to the early 2000s music piracy era.

The debate highlighted concrete economic risks: projected revenue losses for musicians of up to a quarter by 2028, photographers reporting £14,000 in lost earnings due to AI competition, and more than half of professional musicians earning under £15,000 a year. Authors and publishers pointed to extensive use of pirated books in training datasets, with Meta’s use of millions of illegally copied texts cited as a key example. Visual artists noted they would license their works for fair payment but many currently earn below the minimum wage. MPs also raised concerns about unauthorised use of performers’ voices and likenesses, and about impacts on regional culture, including the Welsh language sector.

Contributors criticised the Government’s proposed opt-out system as unworkable and unfairly burdensome on creators. Dame Caroline Dinenage highlighted the success of licensing models used by Getty Images and Adobe. MPs also called for granular transparency obligations, requiring developers to disclose which copyrighted works informed model training. A YouGov poll showing 92 per cent of MPs support disclosure requirements was cited as evidence of strong political consensus.

Responding, Minister Chris Bryant reaffirmed the Government’s commitment to protecting creators, stating that ‘it is patently wrong to use pirated material to train large language models’. He confirmed that no opt-out provision would be included in the Data (Use and Access) Bill, supported transparency obligations (while noting technical challenges), and pledged further industry consultation. He concluded that a system providing consent, remuneration and transparency would place the UK ‘genuinely leading the world’.

Parliamentary scrutiny of AI-related copyright policy has intensified. During the 2023–2024 passage of the Data Protection and Digital Information Bill, the House of Lords Communications and Digital Committee warned that the Government’s approach was ‘underpowered and opaque’ and that failing to provide legal certainty risked undermining both innovation and creative rights. The Secretary of State for Science, Innovation and Technology later confirmed that the previously proposed blanket TDM exception had been abandoned in favour of a new statutory approach involving transparency and opt-out mechanisms, expected to appear in the forthcoming Artificial Intelligence Regulation Bill and related statutory instruments.

During the Data Act debates, Lords sought to embed transparency obligations directly into the statute, requiring developers to disclose whether and how copyrighted works had been used in AI training. The Commons rejected these proposals, deferring them to the forthcoming AI Bill. The final Act instead requires the Government to consult on technical and economic models for enhancing copyright transparency by March 2026.

4.7 Critical Commentary on the Copyright Debate

UK copyright law debates on AI hinge primarily on two statutory elements: the narrow text and data mining exception in [section 29A of the CDPA 1988](#), and the UK’s ‘computer-generated works’ provision in section 9(3), which attributes authorship to the person making arrangements and provides a 50-year term. These define the contours of legal analysis across three axes: the legality of training on protected inputs, the liability for and protectability of AI-generated outputs, and the suitability of mechanisms for transparency or remuneration beyond existing law.

On training inputs, [Kretschmer, Margoni and Oruc](#) trace pressure points across the machine learning lifecycle, arguing that ‘lawful access’ effectively lets rightsholders block AI unless licensed. [Rosati](#) reaches a similar conclusion: licensing remains the default unless reforms are enacted. [De la Durantaye](#) maps cross-jurisdictional regimes split between opt-outs, transparency, and remuneration, placing the UK toward the licensing-heavy end. [Buick](#) argues that transparency alone offers little leverage without structural reform, while [Quintais](#) explains how the EU AI Act integrates with DSM Directive text and data mining rules, providing a comparative benchmark.

On AI-generated outputs, [Hugenholtz and Quintais](#) propose a four-step EU originality test for human-directed work. [O’Callaghan](#) doubts whether granting copyright to autonomous output offers benefits, especially given the UK IPO’s inaction on CGW reform. [Ahn Le](#) draws historical parallels with photography to support a human-centred threshold for authorship.

Regarding liability, [Rosati](#)’s ‘Infringing AI’ paper outlines possible doctrines for UK infringement, liability allocation, and defences. [Lin and Guan](#) advocate ‘AI harbours’ with differentiated duties across actors, and [Samuelson](#) outlines how *Getty* and other disputes may reduce training corpora to licensed or public domain sets.

On transparency and remuneration, [Militsyna](#) questions whether EU marking solves core copyright or copyfraud concerns. [Zhang](#) proposes a ‘train freely, regulate outputs’ model, and [Geiger](#) makes a human rights-based case for training remuneration.

Commentators from the [CREATe Centre](#) at the University of Glasgow stress that layered protection confuses users and chills innovation where IP, contract and privacy law intersect. [Matulionyte et al.](#) highlight the point that rightsholders cannot enforce rights without insight into how their content is used in training.

According to [The Entrepreneur's Network](#), UK SMEs face legal uncertainty compared to AI developers in jurisdictions with broader TDM exceptions such as the EU or Japan. This uncertainty cascades down to users and risks de facto convergence with the US fair use system, but without its constitutional defences. Scholars argue the UK's hybrid model must be codified to preserve innovation incentives and legal certainty.

Together, this review of legal commentary suggests a broad consensus: operational clarity and enforceable statutory norms are essential. Legal uncertainty must be resolved if the UK is to develop a globally competitive AI framework that respects both innovation and rights protection.

4.8 Legal Uncertainty and Developer Risk in the Current UK Framework

As of late 2025, the legal status of web scraping for AI training in the United Kingdom remains unsettled. As we have seen, practice sits at the intersection of several overlapping regimes, including copyright, sui generis database rights, contract law, and the Computer Misuse Act 1990. While non-commercial research enjoys limited protection under section 29A of the CDPA, commercial developers face a thicket of potential liabilities. In practice, scraping protected material without a licence may constitute infringement or even unlawful access depending on the technical means and site policies involved.

The current lack of a general-purpose text and data mining (TDM) exception has raised concerns that the UK may deter domestic AI innovation or drive it offshore. Industry stakeholders have warned that without either clearer rules or a licensing infrastructure, companies may operate in legal uncertainty. This includes small developers unsure how to audit their datasets and large platforms hesitant to risk reputational harm or litigation. At the same time, policymakers remain mindful of creators' rights, with Parliament reiterating that digital content producers and database investors deserve meaningful protection when their content is repurposed for machine learning.

The promised AI Bill, along with related outputs from the Data (Use and Access) Act 2025, is therefore likely to be decisive. Until then, the prevailing position is that large-scale scraping, especially for model training or other commercial purposes, must be approached with caution. Developers are advised to assess whether data are protected, examine terms of use, and obtain licences where feasible. The legal ambiguity remains significant, with no default right to scrape and no statutory safe harbour yet in force.

4.9 International Regulatory Spillover and Market Dynamics

UK policymakers must consider the international consequences of divergent copyright rules, particularly in the context of AI training. Empirical evidence from the implementation of the GDPR suggests that stringent regulatory models can trigger global compliance adaptations: the 'Brussels effect'. Companies often apply the highest regulatory standard across markets to avoid legal fragmentation and compliance burdens (Network Law Review, ResearchGate). Similar spillover effects are likely if the UK adopts a permissive or restrictive approach to AI scraping without alignment to the EU or US frameworks.

Academic commentators have warned that fragmented regulation could inadvertently penalise UK developers or researchers, particularly if they operate cross-border and must satisfy multiple, possibly conflicting, regimes. At the same time, stronger UK rules might shape international norms if they become a model for ethical scraping and responsible AI development. As the UK AI Bill develops, its copyright and data access provisions will thus carry outsized significance, not only for

domestic innovation policy, but also for global interoperability, research funding criteria, and commercial AI viability across jurisdiction.

5. Product Liability, Safety, Negligence, and Post-Deployment Duties

5.1 Overview

The recent EU [Product Liability Directive](#), Directive (EU) 2024/2853, updates strict no-fault liability to the digital era. It expressly includes software and AI within the definition of ‘product,’ extends potential liability across a wider set of economic operators (including certain fulfilment and platform actors), introduces disclosure mechanisms, and eases the burden of proof in technically complex cases through rebuttable presumptions in defined circumstances. Member States must transpose the Directive by December 2026. Authoritative text and leading analyses agree that data loss and corruption are within recoverable damage categories and that post-sale dynamics, updates, cyber vulnerabilities and model regressions, may constitute a defect ([Hogan Lovells](#)).

Specialist bar and firm commentaries detail how software and AI are now squarely captured, how presumptions will work, and how plaintiffs can leverage disclosure to overcome information asymmetries in complex AI cases. They also underline the new litigation posture for producers and deployers operating in the EU ([IBA](#)).

Post-Brexit, the UK is not subject to the new EU Product Liability Directive, relying instead on the [Consumer Protection Act 1987](#) and common-law negligence, supplemented by sectoral guidance from regulators. This preserves flexibility but leaves more evidential uncertainty for claimants and producers until any reforms land.

An independent study commissioned by the [Office for Product Safety and Standards](#) identified challenges for both product safety and product liability. The challenges included limited evidence of real-life examples of harm caused by AI consumer product and the unclear scope of ‘product’ in [General Product Safety Regulations 2005](#) that apply to all manufactured products except vehicles, pharmaceuticals, and food. As in the case of consumer protection laws, it is unclear whether product safety laws apply to software products. This makes the impact of the regulatory frameworks for both product safety and product liability particularly difficult to determine given the blurred lines between product and services, increasing ability of AI products to cause immaterial harms (such as mental health and discrimination), increasing complexity of supply chains for consumer products, and built-in obsolescence and maintenance throughout the product cycle.

Overall, the EU framework shifts both ex-ante assurance and ex-post litigation dynamics toward formal documentation, traceability and broadened responsibility for digital products, while the UK’s principles-based approach heightens the importance of demonstrable governance and professional diligence to manage negligence exposure in ADM-driven civil contexts.

5.2 Civil Liability in Connection with Automated Decision-making

As automated decision making (ADM) tools move into civil disputes and insurance claims, liability risk is increasingly tied to professional diligence. Courts and regulators expect documented human verification, traceability of model use, and defensible audit trails. The EU AI Act hard-codes these expectations for high-risk systems: providers and deployers must ensure event logging over the system lifecycle (Article 12), rigorous data and data-governance controls for training, validation, and testing data (Article 10), and meaningful human oversight calibrated to the system’s purpose and risks (Article 14). These duties exist to enable post-incident reconstruction and accountability, and

they expressly link logs to post-market monitoring and risk management ([EU Artificial Intelligence Act](#)).

Key applicability milestones reinforce that these obligations are coming online in phases: unacceptable-risk bans applied from 2 February 2025, general-purpose AI transparency duties apply 12 months after entry into force, and high-risk obligations phase in by 36 months. Authoritative timelines from the European Parliament and practitioner briefings (for example, WilmerHale) map these dates and documentation expectations in detail. This may however be subject to change if the [EU Digital Omnibus](#) is adopted.

In the UK, even without a cross-cutting AI statute, the government's regulator-led framework explicitly requires accountability evidence. The 2024 government response to the AI White Paper instructs regulators to apply common principles, safety, transparency, fairness, accountability, and contestability and to coordinate through the Digital Regulation Cooperation Forum and the AI & Digital Hub so firms can evidence explainability, testing rationales and records of decision-making. The [ICO's guidance under Article 22 UK GDPR](#) sets out guidance on the right not to be subject to solely automated decisions with legal or similarly significant effects, reinforcing the need for human review routes and well-kept records when ADM is used. However, this guidance is currently under review following the changes made to Article 22 in the [Data \(Use and Access\) Act 2025](#) (DUAA), which have loosened the restrictions previously imposed on solely automated decision making.

5.3 Scope of 'Product' and 'Good' in Consumer Protection Laws

The [Consumer Protection Act 1987](#) ('CPA') implemented the original EU [Product Liability Directive](#) 85/374/EEC in the UK which regulates products in circulation. Since the CPA was introduced, the range of available products, particularly in the context of digital technology, has developed significantly. It is recognised that the product liability regime has not kept pace with those developments. The Law Commission's project on product liability remains pending although scheduled to begin in 2025 ([Law Commission](#)). The Law Commission's Discussion Paper on [Artificial Intelligence and the Law](#) (2025) states that it is 'doubtful' whether the CPA applies to software and that it seems 'unlikely' that a producer of an AI system that was solely in the form of software could be made liable in the current product liability frameworks.

In [Computer Associates \(UK\) Ltd v. The Software Incubator Ltd](#) it was concluded that software was not a 'good' for the purposes of the Commercial Agents (Council Directive) Regulation 1993, which further reduced the likelihood of the courts finding that software is a 'product' under the CPA. The court relied on a previous judgment, [St Albans City and DC v. International Computers Ltd](#), where it was held that software is not a 'good' under the Sale of Goods Act because it is intangible, while 'good' denotes a tangible 'thing'. Correspondingly, it is only where software is contained on hardware that the software and hardware combination is a 'good'. However, the CJEU took a different view on the scope of the 1993 Regulation, deciding that the purely electronic sale of software constituted a sale of goods ([TLT](#)). How far this ruling applies in other relevant contexts post-Brexit is unclear.

Further legislation that could potentially expand the scope of 'product' for consumer protection in the near future is the [Product Safety and Metrology Act 2025](#). While the government has clarified that the bill was not intended to regulate AI itself, it will apply to products and production processes using or containing AI ([DBT](#)). Section 1(7) of the Act defines 'product' as a tangible item that results from a method of production. Section 1(9) defines 'intangible' components to include software. Section 2(2)(a) states that the regulations may include product requirements in relation to the production, components (whether tangible or intangible), composition or other characteristics of

products. While the Act might help expand the scope of ‘product’ to include products that *contain* components of AI, this expansion of the definition of ‘product’ is marginal as it will continue to exclude AI products that are completely software-based.

5.4 Sector-specific Guidelines for Product Safety

5.4.1 Automobiles

The [Automated and Electric Vehicles Act 2018](#) granted users of automated vehicles immunity from prosecution where those vehicles commit driving offences or are involved in accidents. Instead, the Act provided for liability to be attached to an organisation (such as the manufacturer or operator of the vehicle) and extensive data sharing requirements to be introduced to ensure that the cause of incidents can be properly established. This Act is set to be superseded by the [Automated Vehicles Act 2024](#) in a phased manner. The listing procedures of the 2018 Act are still in force until the authorization procedures of the 2024 Act are implemented (planned to be implemented through secondary legislation in 2026). Under the current law, vehicles that are capable of safely driving themselves may be listed under section 1 of the Automated and Electric Vehicles Act 2018. All listed vehicles under the 2018 Act are to be treated as authorised vehicles for the purposes of misleading marketing (2024 act, s 81(5)). However, once the more rigorous authorisation procedure of the 2024 Act comes into force, the new listing procedures will supersede the listing procedure under the 2018 act ([HFW](#)).

5.4.2 Health

British Standards Institution supported by Department of Health and Social Care has published [recommendations](#) to support emergence and regulation of AI in the healthcare sector. The [position paper](#), targeted at developers, recognises the need for a joint US-UK taskforce to update existing regulatory frameworks for health software and IT systems. In particular, the [standard IEC 62304: 2006](#) applies to ‘medical device software’ and its lifecycle requirements for medical. A new edition is in development with an expanded scope that will cover all health software. The related risk management strategies require a mapping of all essential features for safety and performance and communication with communities and dissemination of knowledge about use-cases. The [Regulatory Innovation Office](#), a directorate within the ministry with responsibility for science and innovation, DSIT, has chosen to focus on the use of AI in healthcare as one of four areas in which to conduct a review of whether existing regulations are holding back innovation.

5.4.3 Education

The Department of Education has also published [Guidelines for Product Safety Expectations](#) concerning AI products and systems in educational settings. The guidelines are targeted at edtech developers and suppliers as well as schools and colleges and list the following standards:

- *Filtering (preventative) standards* for child-facing products that require Generative AI products to effectively and reliably prevent access to harmful and inappropriate content by users. These will further help schools to comply with the 2005 [statutory guidance](#) (updated in 2015) on keeping children safe in education, [filtering and monitoring standards](#) for schools and colleges, and their [public sector equality duty](#). They also help the edtech developers and suppliers to comply with the [Online Safety Act 2023](#) (section 60 of which is concerned with content that is considered harmful to children);
- *Monitoring and Reporting (reactive) standards* for child-facing products that require AI products to maintain robust activity logging procedures. These can be integrated into an AI

tool or provided as an additional solution and includes recording inputs and responses, analysing performance metrics, and alerting local supervisors when harmful or inappropriate content is accessed or attempted to be accessed. They are intended to help schools to comply with the 2005 [statutory guidance](#) on keeping children safe in education and [filtering and monitoring standards](#) for schools and colleges. For edtech developers and suppliers, they will ensure compliance with [data protection laws](#) governing data protection impact assessments, the [Information Commissioner's Office Age-Appropriate Design Code](#), and the [Data Use and Access Act 2025](#);

- *Security standards* for both child-facing and teacher-facing products that require generative AI product to be secured against malicious use or exposure to harm. They include prioritising technical objectives of reliability, security, robustness, ensuring safe operation under various conditions, including unexpected changes and adversarial attacks. They will further help schools and colleges to comply with [Cyber Security Standards](#) for schools and colleges and the [Computer Misuse Act 1990](#);
- *Privacy and data protection (DP) standards* for both child-facing and teacher-facing products that require AI products to have a robust approach to data handling and transparency around personal data processing, including compliance with data protection and lawful data collection. They will help edtech developers and suppliers to comply with data protection laws and the UK GDPR, ICO's [Children Code](#), and ICO's [Guidance on AI and Data Protection](#);
- *Intellectual property standards* for both child-facing and teacher-facing products that prohibit the AI product to store or collect intellectual property created by pupils for commercial purposes unless consented to by the copyright owner or their parent or guardian. They are intended to help edtech developers and suppliers to comply with the Copyright, Designs and Patents Act 1988;
- *Design and testing standards* for both child-facing and teacher-facing products that require the AI product to prioritise transparency and children's safety in its design. They include requirements of technical or operational mitigations for identified risks, child-centred design and operation, and testing with stakeholders for safety. They enable the schools and colleges to comply with the [public sector equality duty](#) and help edtech suppliers and developers to comply with [ICO's Children's Code](#), [Equality Act 2010](#), [ICO's Guidance on AI and Data Protection](#), [UK GDPR](#), and [General Product Safety Regulations](#);
- *Governance standards* for both child-facing and teacher-facing products that require the AI product to be operated with accountability and require risk assessments, formal mechanisms for lodging complaints and policies or processes for governing AI safety decisions. They help edtech developers and suppliers to comply with [UK GDPR](#), [Data Protection Act 2018](#), and [ICO's Children's Code](#).

5.4.4 Others

Other product-specific regulations that will need to be adapted to include AI products, and have not yet been addressed, include the following:

- The [Toys \(Safety\) Regulations 2011](#), that apply to toys designed or intended (whether or not exclusively) for use in play by children under 14 years old;
- The [Electrical Equipment \(Safety\) Regulations 2016](#), that apply to all electrical equipment that is designed or adapted for use between 50 and 1,000 volts (in the case of alternating current) and 75 and 1,500 volts (in the case of direct current);
- The [Supply of Machinery \(Safety\) Regulations 2008](#) to ensure that safe machinery is placed on the market or put into service by requiring manufacturers to show how their machinery meet the 'essential health and safety requirements'.

- The [Radio Equipment Regulations 2017](#) that require equipment placed on the Great Britain market to comply with a high level of safety (in terms of the health and safety of persons and domestic animals and the protection of property); with an adequate level of electromagnetic compatibility; and to operate in a manner that promotes efficient use of the radio spectrum.

5.4.5 Voluntary Standards

Various international organisations and industry associations have also adopted voluntary standards that apply to AI products. For instance, The [OECD AI Principles](#) require AI systems to be robust, secure and safe throughout their entire lifecycle with risk-mitigating and integrity mechanisms in place to ensure safety and freedom of expression. Additionally, the [Ethics Guidelines for Trustworthy AI](#), by High Level Expert Group on Artificial Intelligence set up by the European Commission, list ‘technical robustness and safety’ as one of key requirements for trustworthy AI.

The [White Paper](#) on Ethically Designed AI published by the IEEE lists tools, recommendations, assessments metrics, and further resources to help businesses build safe AI products. Some examples include Indicators and toolkits can inform business decisions and assess impacts, empowering and encouraging employees to raise ethical concerns in day-to-day professional practice, setting up of corporate ethical review boards, *stakeholder inclusion, and values-based design*.

6. Labour and Employment Law

6.1 Overview

Despite [evidence](#) of recent growth in practices coming under the broad heading of ‘algorithmic management’, including the use of algorithms in recruitment, workflow management, rating of employees, and the operation of disciplinary and dismissal procedures, there is no legislation in the UK specifically addressing the issue of AI usage in the workplace, and relatively little case law. The recently adopted EU Platform Work Directive, having been agreed after Brexit, is not binding on the UK, and the current government has no plans to adopt it. British labour law recognises the employer’s right to introduce new technology into the workplace, subject only to a loosely defined obligation to offer training in new techniques as long as the employment relationship subsists ([Cresswell v. Board of Inland Revenue](#), 1984). Redundancy on technological grounds is a potentially fair reason for dismissal, and an obligation to consult employee representatives over proposed dismissals only arises if a significant number of employees are affected by a collective redundancy (normally 20 or more employees in a single establishment). The [Health and Safety at Work Act 1974](#) imposes a duty to consult over the introduction of new technologies which in principle would extend to algorithmic systems, but the scope of this obligation is confined to physical and psychological risks. [Unfair dismissal law](#) requires the employer to provide a reason for dismissal and, by extension, to justify disciplinary action for misconduct or underperformance; in principle, then, there is limited scope for the employer to rely on algorithmic decision making which is not at least confirmed or supplemented by human judgement. However, dismissal protections only apply to ‘employees’, a narrowly defined category in English law which excludes not just independent contractors but many situations of irregular or intermittent work. Although a major new labour law reform, the [Employment Rights Bill](#), is currently before Parliament and is due to be given the Royal Assent in either 2025 or 2026, it does not address risks specific to AI use. In so far as there is a trend in the government’s attitude to algorithmic management, it is a deregulatory one, as exemplified by the decision to lift some of the constraints imposed on automated decision making under Article 22 of the UK GDPR; following the [changes made by the DUAA 2025](#), a somewhat looser version of Article 22 now applies in the UK than the one operating under the original version of the GDPR, which

continues to apply across the EU. The capacity of discrimination law to address bias arising from the use of algorithms in employment remains largely untested.

6.2 Data protection law relating to employment

Two provisions of the [GDPR](#) have particular relevance for employment law: Article 15, which contains a right to receive information concerning automated decision making, and Article 22, which regulates automated processing. Both have been part of UK law since the UK's pre-Brexit adoption of the GDPR in 2018, but Article 22 rights are now subject to changes introduced by the DUAA 2025.

Data protection law confers rights and obligations on 'data subjects' and 'data controllers' and 'data processors' respectively; these concepts do not map precisely on to the labour concepts of 'employee' or 'worker' and 'employer', but there are numerous instances in which firms using AI-systems will need to pay regard to data protection laws. The UK ICO's [guidance on data protection rights relating to automated processing](#) gives as one of its principal illustrations the use by an employer of a recruitment aptitude test.

Under Article 15 of the GDPR, a 'data controller' must provide a 'data subject' with information concerning 'the existence of automated decision-making, including profiling', which extends 'at least' to 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'. Article 15 is essentially informational; it does not extend to a right to correct the workings of an automated decision-making systems, or to compensation for harms caused by its operation. Nor does it clearly require the user of an AI-based system to disclose information on the internal workings of an algorithm, such as the source of training data or aspects of the design of a machine learning model, such as the weights used.

As originally enacted, Article 22 GDPR provides that 'the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her', unless one of three exceptions applies: the processing is necessary for entering into or performance of a contract between an organisation and the individual, authorised by law, for example, for the purposes of fraud or tax evasion, or based on the individual's explicit consent. Profiling means 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements' (Article 4(4)). For 'special category personal data', a category which includes data on trade union membership, racial or ethnic origin, religious or philosophical belief and political opinion, as well as genetic and biometric data, processing is allowed only in the case of the individual's explicit consent, or by reasons of substantial public interest. While potentially far-reaching in its implications for employment, Article 22 is limited in scope by the requirement for the decision to be based 'solely' on automated processing. According to the [ICO](#), this means 'a decision made by automated means without any human involvement', for example, 'a recruitment aptitude test which uses pre-programmed algorithms and criteria'. It would seem then adding a 'human to the loop' in the process of implementing an automated decision is likely to take the process outside the scope of Article 22.

Where Article 22 can be shown to apply, the prohibition it imposes can be overridden by the individual's consent, subject under Article 22(3) to the data controller implementing 'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests', including 'at least the right to obtain human intervention on the part of the controller, to express his or her point

of view and to contest the decision'. While potentially extensive, these rights again stop short of a right to correct the workings of an algorithm or to compensation for its harmful operation.

Article 88 of the GDPR provides that 'Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship'. CJEU case law suggests that when member states make use of this provision, they face a high bar in showing that such measures are compatible with the protection of employees' privacy rights. However, as explained by [Abraha](#) and [Aloisi et al.](#), few EU member states, including the UK pre-Brexit, made use of Article 88, and it is hard to see the post-Brexit CJEU case law having any tangible influence on the British courts' interpretation of the UK GDPR.

The UK is not subject to the EU's Artificial Intelligence Act, but it is unclear in any case how far the Act goes further than the GDPR. Article 86 of the Artificial Intelligence Act sets out a 'right to explanation of individual decision-making', under which any person subject to a decision by the 'deployer' of a high-risk AI system is entitled to obtain from that deployer 'clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken', in any case where such a decision 'produces legal effects or similarly significantly affect that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights'. High-risk AI systems include, under Annex III of the AI Act, 'AI systems intended to be used for the recruitment or 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'. In common with Articles 15 and 22 of the GDPR, there is no express requirement for deployers of AI systems to provide information on the source of training data, nor to inform persons affected by an algorithm of the weighting system used. It remains open to employers, in so far as they are constituted as AI 'deployers', to argue that they do not need to provide an explanation of the workings of AI systems they buy off the shelf.

The limitations of the GDPR notwithstanding, national courts in several EU member states have found platform companies in the ride hailing and food delivery sectors liable for breaches of the Regulation, in circumstances where personal data was used, among other things, to rank labour service providers by reference to their performance, alter prices, and ration access to the app ([Hiessl](#)). One of the proposals contained in the recent [EU Digital Omnibus](#) is to loosen GDPR rules in this area. This proposal has already proved highly controversial ([Ada Lovelace Institute](#)) and it remains to be seen whether or how far it will eventually lead to a revision of the Regulation.

In the case of the UK, a weakening of the GDPR has already occurred, by virtue of changes made to Article 22 of the UK version of the Regulation in the DUA 2025. Section 80 of the DUA substitutes [new Articles 22A-22D of the UK GDPR](#), granting the Secretary of State powers to make regulations stipulating when there is no 'meaningful human involvement in the taking of a decision' so as to take it outside the scope of the regulation. As a result of this change, the ICO is in the process of [reviewing its existing guidance](#) on automated decision-making, including in the employment context.

6.3 General Labour and Employment Law Relating to AI

There is no specific AI-related labour or employment law in the UK, but the general law will impose certain constraints on the use of AI-related HR systems including in the contexts of automated recruitment and algorithmic management. Where the use of an algorithm leads to discrimination on the grounds of a protected characteristic such as sex or race, the Equality Act 2010 will be triggered. Pre-Brexit EU case law, in common with US law on ‘[disparate impact](#)’, establishes that a seniority or ranking system which causes significant disadvantage over time for women workers, for example, is likely to be regarded as *prima facie* indirectly discriminatory, and therefore in need of justification by the employer. While there is no clear precedent on how far this principle would limit the use of AI-related algorithms, it would be no defence for the employer simply to argue that the operation of the algorithm was a ‘black box’ if it was shown to have discriminatory effects. Justification tests have become stricter over time, requiring the employer to show that the practice being questioned serves a legitimate aim by proportionate (least disadvantageous) means. In addition, the use of an algorithm with discriminatory weights or data built into it could be classified as directly discriminatory, and thus not capable of being justified ([Adams-Prassl et al.](#)) Since the Equality Act 2010 applies at the hiring stage as well as to the treatment of individuals in work, it potentially affects the use of recruitment algorithms.

While data protection law stops short of providing a clear right to an explanation in the context of automated decision making, UK employment law, following in this respect International Labour Organization standards, requires the employer to provide a reason for the dismissal of an employee, which by extension applies to most contexts of disciplinary action leading up to a dismissal. Where a dismissal is based on a ranking or performance appraisal system which makes use of predictive AI, for example, to associate particular traits or behaviours with underperformance, it seems unlikely in the current state of the law that the termination of employment would be characterised as being for a potentially fair reason, in the absence of evidence relating specifically to the individual affected ([Collins](#); [Atkinson and Collins](#) ; [Atkinson and Collins](#)). An AI-related case of precisely this kind has not yet been considered by a British employment tribunal, but case law in other European countries suggests that employers cannot rely on AI-based algorithms to substitute for normal rules of due process in the dismissal context ([Hiessl](#)).

A potential weak point in the application of labour and employment laws to the use of AI-related algorithms is that they do not apply to labour service providers who lack employee or worker status. Case law on the employment status of ‘gig’ or platform workers in the UK lacks consistency ([Deakin](#)). While workers in the ride-hailing sector benefited from the decision of the UK Supreme Court in *Uber v. Aslam*, according to which Uber drivers qualified for minimum wage protection ([Bogg](#)), a later Supreme Court decision, *Deliveroo*, classified food delivery drivers as self-employed, denying them collective bargaining rights ([Pitt](#)). The major labour law reform measure currently being considered by Parliament, the Employment Rights Bill, does not contain any provisions on employment status, although the government is committed to consulting on a reform of the employee and worker definitions in the near future ([Make Work Pay](#)).

6.4 The EU Platform Work Directive

The EU [Platform Work Directive](#) (PWD), adopted on 23 October 2024 and due to be implemented at member state level not later than 2 December 2026, creates several new digital law rights in the context of platform work, while seeking to establish clearer rules on the status of those supplying labour services via digital platforms. The new digital rights relate to limitations on the processing of personal data by means of automated monitoring systems (AMSs) and automated decision making systems (ADMSs) (Article 7); data protection impact assessments (Article 8); transparency with

regard to AMSs and ADMSs (Article 9); human oversight of AMSs and ADMSs (Article 10); and human review of ADMSs (Article 11). Articles 12-14 extend the scope of certain labour law rights relating to safety and health, information and consultation and provision of information in the platform sector.

The digital rights contained in the PWD go beyond Articles 15 and 22 GDPR. Article 9 specifies that information on automated monitoring must include ‘the aim of the monitoring and how the system is to carry out that monitoring’ and ‘the categories of data and action monitored, supervised or evaluated by such systems, including evaluation by the recipient of the service’, while information on automated decision making systems must refer to ‘the categories of data and the main parameters that such systems take into account and the relative importance of those main parameters in the automated decision-making, including the way in which the personal data or behaviour of the person performing platform work influence the decisions’. Although there is no specific obligation to disclose the origin of training data, the wide formulae contained in Article 9 are arguably capable of extending this far. Similarly, Article 10 establishes for the first time a clear right to alter the mode of operation of an AMS or ADMS; if a biannual review of the operation of an AMS or ADMS ‘identifies a high risk of discrimination at work in the use of automated monitoring systems or automated decision-making systems or finds that individual decisions taken or supported by automated monitoring systems or automated decision-making systems have infringed the rights’ of those affected, steps must be taken to avoid such decisions in future up to and including the ‘modification’ of the AMS or ADMS, and the ‘discontinuation of its use’. Article 10 also requires any decision to restrict, suspend or terminate a contractual relationship or account ‘shall be taken by a human being’. Article 11 requires ‘an oral or written explanation’ to be provided ‘without delay’ for any decision taken or supported by an AMS or ADMS, and a written statement of reasons for any decision taken by an ADMS to close or restrict an account, refuse payment for work, or determine contractual status; any other decision with equivalent effects; and any decision ‘affecting the essential aspects’ of an employment or other contractual relationship.

These digital rights apply not just to employment or work relations as defined by EU law or relevant provisions of national law, but in addition to any situation in which work is ‘organised through a digital labour platform’, a category designed to include the provision of labour services by independent contractors beyond the scope of labour laws. At the same time, the Directive seeks to extend the scope of labour laws by providing for a presumption of employee or worker status in any context where a digital labour platform exercises ‘control’ over ‘a person providing platform work’.

While significantly extending the scope of both digital law and labour law protections ([Countouris and De Stefano](#); [Sanders](#)), the PWD only applies to the provision of work via a ‘digital labour platform’, which is defined here as a natural or legal person providing a service (i) ‘at least in part, at a distance by electronic means, such as by means of a website or a mobile application’; (ii) ‘at the request of a recipient of the service’; (iii) involving ‘as a necessary and essential component, the organisation of work performed by individuals in return for payment, irrespective of whether that work is performed online or in a certain location’; and (iv) involving ‘the use of automated monitoring systems or automated decision-making systems’. The Directive has no application to the use of algorithms in other workplaces. This has led to calls for a measure on employment-related AI use more generally, with the European Parliament’s Committee on Employment and Social Affairs proposing a [draft directive on algorithmic management](#) in 2025.

While the UK, post-Brexit, is not bound by the PWD, its implementation across the EU and its use as a model beyond Europe ([CBR Platform Work Index](#)) suggests that it may soon be a benchmark against which UK laws are judged, and potentially found wanting, including on the issue of employment status. Political impetus for a reform of UK employment law to clarify the employment status of, among others, platform workers, has recently been building ([Guardian](#)).

7. Competition Law

7.1. Overview

AI adoption has been increasing exponentially among businesses over the last few years which could stifle effective competition. According to the [Stanford AI index](#), 78% of the organisations worldwide used AI in 2024, as opposed to 55% in 2023. There are many risks that competition law is grappling with when it comes to AI ([CMA AI Strategic Update](#)). These risks can be broadly classified in two categories. The first relates to the risk of AI adoption by market participants and how that could stifle competition, which has been highlighted by competition authorities across the world ([Dutch Competition and Markets Authority ACM](#)). Examples include the use of algorithmic systems to distort competition in activities like setting prices, influencing supply and demand, and price discrimination and collusion ([Loyens and Loeff](#)). The second types of risk relates to regulating competition in cloud services market.

The [UK's new digital markets competition regime](#) seeks to address both these challenges. The new regime was introduced by passing of the [Digital Markets, Competition and Consumers Act 2024](#) (DMCCA) that brings the most substantial reforms since the introduction of the current merger control regime over 20 years ago, impacting digital markets, merger control, antitrust rules, and consumer law ([Bird and Bird](#)). From January 2025, new responsibilities for the Competition and Markets Authority (CMA) came into force under the DMCCA 2024 that enables the CMA to promote competition in fast-moving digital markets, while protecting UK consumers and businesses from unfair or harmful practices by the very largest technology firms.

At the heart of this new regime is proportionality and the 'SMS Regime'. It is designed to apply only to the very largest firms. If certain conditions are met, these firms can be designated with Strategic Market Status (SMS) in relation to a particular digital activity. If the CMA designates a firm with SMS, some of the key implications include ([CMA Guidance 2025](#)):

- Conduct Requirements: the CMA will be able to guide the behaviour of SMS firms, tackling conduct that could undermine fair competition, or exploit people and businesses.
- Pro-Competition Interventions: the CMA will be able to address specific competition problems arising from a firm's market power in a particular digital activity.
- Additional merger reporting requirements on SMS firms: to make sure the CMA has earlier sight of mergers and acquisitions that could harm competition in digital markets.

7.2. Effects of AI Adoption on Competition and Algorithmic Collusion

Both UK and EU competition law prohibit agreements, arrangements and concerted practices that, by object or by effect, prevent, restrict or distort competition in the relevant market (Chapter I, Competition Act 1998 (1998 Act); Article 101, Treaty on the Functioning of the European Union (TFEU)) ([Mayer Brown](#)).

In 2016, the UK's CMA found that two online poster sellers agreed that they would not undercut each other's prices for licensed sport and entertainment posters and frames that were sold on Amazon's UK website ([Decision of CMA: online sales of posters and frames, Case 50223](#)). The agreement was implemented using automated repricing software, which allowed both parties to automatically adjust the prices of their products in response to the live prices of their competitors. This is an example of what the UK's CMA has termed as 'pricing algorithms' potentially leading to 'algorithmic collusion'. ([TaylorWessing](#))

In a [2018 working paper](#), the CMA discussed how pricing algorithms can exacerbate risks of harm:

- Concentrated markets: Because of algorithmic pricing, both explicit and tacit co-ordination could occur in less concentrated markets. This is because algorithms can collect information about more competitors at a faster rate than humans.
- Market transparency: increasing availability of data and use of pricing algorithms can increase market transparency (especially online), even if there are many products with complex offers. This is because algorithms can scrape data from many websites more quickly than humans would be able to. Therefore, price deviations can be detected more quickly.
- Frequency of interaction and price setting: Pricing algorithms allow firms to set their prices automatically. This means that whenever a price change occurs, competitors can respond by undercutting or matching very quickly with low or zero transaction costs. Further to this, an algorithm could allow firms to test their competitors' responses to changes in price during periods of low demand.
- Low buyer power or small regular purchases: Online markets operate 24 hours a day, and sometimes internationally, therefore there can be a high frequency of purchase with low buyer power.

7.3. Competition in the Cloud Services Market and Merger Control

In the UK, the CMA has launched a Data, Technology and Analytics unit to equip it to better understand, and respond to, the competition questions that are arising from emerging technologies including AI ([Mayer Brown](#)). Further, a market investigation into public cloud infrastructure services that was launched on 5 October 2023, where the CMA considered the potential impact of AI on how competition works in the cloud services market ([Cloud Services Market Investigation](#)). The market investigation recommended that the CMA use its digital markets powers to prioritise commencing Strategic Market Status (SMS) investigations, to consider designating the 2 largest providers – Microsoft and Amazon Web Services (AWS) – with SMS in relation to their respective digital activities in cloud services ([Cloud Services Market Investigation](#)).

As a result, the CMA announced in a [press release in June 2025](#) that Google be designated as SMS based on its [SMS investigation into Google's general search and search advertising services](#). Similar investigations were also launched into [Google's](#) and [Apple's](#) mobile platforms. Additionally, the press release mentioned that further actions will be taken to address more complex issues over a longer period (starting in the first half of 2026) in line with UK's pro-innovation approach. These include concerns about the impact of Google's bargaining position on publishers, its treatment of rival specialised search firms, and concerns about transparency and control in relation to search advertising.

These actions follow the CMA's 2023 decision to clear Microsoft's acquisition of Activision Blizzard on the condition Microsoft would not acquire Activision's cloud streaming rights outside the EEA ([Slaughter and May](#)). Another example is the CMA's initiation of an investigation into the partnership between Microsoft Corporation and OpenAI Inc using its merger control powers on 8 December 2023 ([CMA AI Strategic Update 2024](#)). Similar investigations have been opened in Europe including the European Commission's antitrust investigation into Meta's new policy regarding AI providers' access to whatsapp (https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2896).

Under the new law, there are plans to introduce an 'acquirer-focused' merger control threshold targeting so-called 'killer acquisitions', which may be relevant to transactions where large acquirers buy start-ups such as generative AI software companies.

8. Legal Tech

8.1 The UK Legal Tech Sector: Overview

The UK legal tech market is expanding rapidly. The UK is home to roughly 350 lawtech companies, about 44% of all legal tech startups in Europe, which attracted over £5.5 billion in investment in 2023 alone ([Non-Billable](#)). This growth is driven in part by the UK's large domestic legal industry (valued at ~£47 billion) and the presence of many global law firms. Technology uptake, however, has historically been gradual in the legal sector, and many firms only recently began deploying advanced tools. The advent of generative AI in late 2022–2023 (spurred by tools like OpenAI's ChatGPT) markedly accelerated interest – numerous UK startups have launched AI-powered products for legal research, contract drafting, and document analysis. Surveys indicate that a majority of legal professionals see AI as 'transformational': in one report, two-thirds said AI (especially GenAI) will significantly impact how they work ([Thomson Reuters Institute](#)). In-house legal teams are also on board as 65% of UK corporate legal departments are already using AI tools for low-risk, routine tasks as of 2024 ([Inview](#)). That said, deployment of AI for high-complexity legal work remains nascent (only ~15% use AI for complex matters so far, reflecting a cautious, step-by-step adoption ([Inview](#))).

Several factors are propelling lawtech uptake. For commercial law firms and corporates, cost pressure and efficiency needs are paramount. Major clients increasingly demand 'more for less' – they expect their lawyers to leverage technology to deliver services faster and cheaper ([SRA](#)). Automating labour-intensive tasks (like document review or due diligence) via AI and workflow software helps firms optimize billable time and offer alternative fee arrangements, addressing client pressure on hourly billing. In-house legal teams, facing budget constraints, use tech to absorb more work internally and reduce outside counsel spend ([Thomson Reuters Institute](#)).

At the same time, access to justice concerns drive lawtech innovation for consumers and small businesses. Many individuals and SMEs forego legal advice due to cost, creating a large 'unmet legal need' ([SRA](#)). Technology – from online legal platforms to document automation – is seen as a way to lower costs and expand access to legal assistance. Regulators including the Solicitors' Regulatory Authority note that if tech can improve efficiency, firms could profitably serve clients who otherwise couldn't afford help ([SRA](#)). This dual pressure of corporate efficiency and public accessibility has primed the UK market for solutions that make legal services quicker, more affordable, and data-driven.

The past few years have seen widespread digitisation and the rise of AI-driven tools. Automation of 'low-value' processes (like billing, contract templates, or case management) is now common even in conservative firms. Notably, the generative AI 'boom' of 2023 led many UK firms to pilot AI assistants for legal research, drafting, and answering staff queries ([Non-Billable](#)). Law firms are also shifting their business models in response – 43% of legal professionals foresee a decline in the billable hour model within five years due to these efficiency gains ([Thomson Reuters Institute](#)). The focus is on freeing lawyers for higher-value advisory work while machines handle repetitive tasks. Indeed, handling large volumes of data, improving response times, and reducing human error are cited as the top anticipated benefits of AI.

At the same time, legal tech investment hit record highs: many companies raised substantial funding to scale up. For example, London-based Luminance (an AI document review platform) closed a \$40 million Series B in 2024 and contract-management startup ContractPodAi has raised over \$170 million to date (including a \$115 million Series C venture capital funding round in 2021) ([Non-Billable](#)).

8.2 Key Players in UK Lawtech

The UK hosts a wide ecosystem of lawtech providers, ranging from startups to global tech companies, often in close collaboration with law firms and investors.

One of the UK's flagship lawtech successes is Luminance, a Cambridge-founded company that applies machine learning to rapidly read and analyse contracts. Launched in 2016, Luminance's platform is used for due diligence, compliance reviews, and contract management, boasting users in over 80 countries ([Non-Billable](#)). Early backing for Luminance came from innovators in both tech and law – it was seed-funded by Invoke Capital (the fund of Autonomy's Mike Lynch) and piloted by elite law firm Slaughter and May, which later invested in the company ([Global Legal Post](#)). Today Luminance is a market leader: over a quarter of the world's top 100 law firms use its AI, alongside corporate clients like Hitachi and Rolls-Royce. Its recent \$75 million Series C raise in 2024 (one of Europe's largest legal AI funding rounds) underscores investor enthusiasm for this segment. Another notable UK startup is Robin AI, founded by a former Clifford Chance lawyer. Robin AI combines machine learning with human review to streamline contract drafting and negotiation, and has secured ~\$69 million in funding (including a Series B round in 2024). Its platform is already used by major corporations like Pfizer and PwC ([Non-Billable](#)). These companies exemplify how UK-founded AI solutions are tackling the 'heavy lifting' of legal data processing, allowing lawyers to focus on higher-level judgment.

Several UK firms specialize in end-to-end contract lifecycle management (CLM) for in-house legal teams. ContractPodAi, headquartered in London, offers a platform to draft, track, and manage contracts with AI assistance. It has raised over \$170 million to date and counts large enterprises like Philips and PwC among its clients. Likewise, Juro (London-based, founded 2016 by a former Freshfields lawyer) provides a collaborative contract management SaaS. It raised a \$23 million in a Series B funding round in 2022 and serves tech-forward businesses such as Deliveroo and Trustpilot). Definely, a newer startup (founded 2020 by two ex-Freshfields lawyers), takes a different slice of the problem: its tools integrate with Microsoft Word to help lawyers instantly navigate defined terms and clauses in complex contracts. Definely's assistive drafting technology, which emerged from one founder's need as a blind lawyer for better document accessibility, has attracted the support of several leading ('magic circle') law firms; Slaughter and May, Allen & Overy, and Dentons have been early adopters ([Non-Billable](#)).

UK legal tech also spans research tools that use AI/NLP to sift case law or provide litigation insights. For instance, Casetext (recently acquired by Thomson Reuters, though originally US-based) and vLex (which has a significant London presence and merged with Fastcase) are bringing advanced research platforms to UK law firms and chambers. Home-grown ventures like CrowdJustice (by former Linklaters lawyer Julia Salasky, who also founded compliance tech startup Legl have explored crowdfunding for legal cases, while others like CaseMine and Justis focus on AI-aided legal research in the UK common law corpus. The UK's strong academic base in AI and law provides a pipeline of innovation for this segment ([Non-Billable](#)).

A number of startups target niche needs. Thirdfort (London, founded 2017) tackles legal cybersecurity and client due diligence. Its app verifies client identity and screens for anti-money-laundering (AML) risk, used by many property law firms and banks. Legl (London, founded 2019) similarly offers law firms a digital platform for client onboarding, KYC checks, and online payments to modernise back-office processes. In the dispute resolution arena, platforms for online mediation and small claims have gained traction (e.g. Justice Online or trial ODR systems supported by HMCTS). Consumer-facing lawtech has seen entrants like Farewill (online wills) and DoNotPay (an automated legal advice chatbot originally launched in the UK). Though regulatory scrutiny around unqualified

advice has tempered some of these services. Overall, the UK sector covers everything from barrister booking platforms to AI-driven compliance tools, reflecting a diverse commercial landscape ([Non-Billable](#)).

A distinctive feature of the UK lawtech scene is the active involvement of major law firms through incubators and accelerators. Several leading law firms have created in-house innovation programs to partner with startups. Allen & Overy's 'Fuse' was one of the first law firm tech incubators. Fuse invites a cohort of mature startups to co-locate in A&O's London office and work alongside the firm's lawyers and clients on developing solutions ([Legal Geek](#)). The idea is to create a sandbox environment where lawyers can test new tools (in areas like transaction management, AI doc review, or regtech) and provide feedback, while startups benefit from mentorship and exposure. Fuse has hosted companies like Legatics (a deal management platform) and Avvoka (document automation), some of which later became vendors to A&O or other firms.

Mishcon de Reya's MDR Lab was founded in 2017 in partnership with tech investor L Marks. It runs an annual program for early-stage lawtech startups. Selected startups spend 10 weeks embedded at Mishcon's offices, gaining access to the firm's lawyers and business experts to pilot their products in real legal use-cases. MDR Lab has a track record of nurturing startups that tackle practical pain points identified by lawyers. For example, past cohorts included a litigation management software (Everchron), a time-tracking automation tool (Ping), and an AI contract review tool (Surukam). Mishcon has gone on to invest in or formally partner with MDR Lab graduates ([Legal Geek](#)).

Slaughter and May's Collaborate was set up as a lawtech incubator around 2019. It offers startups a programme of mentorship and testing. One alumnus is Atria AI, which uses AI to extract insights from contracts; Atria graduated from Collaborate and leveraged Slaughter and May's feedback to refine its product ([Non-Billable](#)). Slaughter and May has also directly backed companies (it was an early investor in Luminance, as noted) and generally is known for closely working with legal AI providers to tailor them to complex transactional work ([Global Legal Post](#)).

Other notable programs include Dentons' Nextlaw Labs (a global innovation network with presence in London), CMS's equiP accelerator for legal tech startups, and the Barclays LawTech Eagle Lab in Notting Hill (run in partnership with the Law Society to support lawtech SMEs). Such incubators not only provide startups with validation and credibility but also signal a cultural shift in law firms from viewing tech disruptors warily to actively collaborating with them. Many large UK firms now boast dedicated 'innovation teams' or R&D budgets to pilot new tools, often sourcing them through these incubator pipelines.

The UK lawtech sector has seen increasing venture capital and M&A activity, indicating commercial maturation. In addition to the big funding rounds for startups mentioned earlier, there have been some high-profile exits: for example, Thomson Reuters' acquisition of HighQ in 2019. HighQ, a London-based provider of legal deal-room and collaboration software, was bought for a reported £200 million ([The Lawyer](#)), demonstrating that global incumbents are willing to pay a premium for proven UK legal tech. Another example is iManage's acquisition of RAVN (a UK AI search startup) in 2017 to integrate AI into document management. More recently, international interest in UK companies continues – e.g. Clio (a Canadian legal software unicorn) acquiring Lawyaw (a UK document automation tool) in 2021, and NetDocuments (US) acquiring Tikit from BT. Meanwhile, UK startups are raising later-stage rounds: in 2023-25 we've seen \$50M+ growth financings for companies like Eigen Technologies (contract AI), Clio (for its UK/EU expansion), and EvenUp (a personal injury AI firm opening a London office ([Global Legal Post](#))). This capital influx is not only funding product development but also fuelling consolidation and partnerships that further integrate lawtech into the mainstream legal industry.

8.3 Government Initiatives and Academic-Industry Collaboration

The UK government and allied organisations have launched several initiatives to bolster the lawtech sector and modernise legal services.

A centrepiece is LawtechUK, a Ministry of Justice-backed initiative dedicated to driving digital transformation in the legal sector. Launched in 2019 with an initial £2 million of funding, LawtechUK has provided resources, education, and acceleration programs to nurture the industry. In its first phase (delivered by Tech Nation), LawtechUK convened a panel of experts and in 2020 created the Lawtech Sandbox, a development environment in which lawtech startups can work alongside regulators and practitioners to test innovative products in a safe setting. For example, one sandbox participant was Legal Utopia, a legal diagnostic app helping consumers identify and solve legal problems. The sandbox offers support on regulatory issues and connections to mentors, helping pioneers bring new solutions to market faster. LawtechUK also built an online knowledge hub and ran events to improve tech awareness in the legal profession ([Ministry of Justice](#)).

The government significantly expanded LawtechUK in 2022, when the MoJ announced a £4 million investment to deliver a second phase of LawtechUK, aiming to ‘modernise the UK legal sector through technology’ and keep it at the global forefront. By 2023, following Tech Nation’s closure, the MoJ awarded the LawtechUK program to CodeBase (one of the UK’s largest tech incubators, based in Edinburgh) in partnership with Legal Geek (a prominent lawtech community and events organiser). This new team received £3 million of funding in 2023 to ‘turbocharge’ growth in legal technology. CodeBase and Legal Geek are working to showcase the UK as a leading lawtech hub, connecting startups with law firms and investors, and continuing support for the UK Jurisdiction Taskforce (UKJT). The UKJT, an industry-led legal panel under the LawtechUK umbrella, focuses on adapting English law for new technologies - for instance, it issued guidance clarifying the legal status of smart contracts and crypto-assets under English law ([Ministry of Justice](#)).

In parallel with fostering private-sector lawtech, the UK government has invested in digitising the justice system itself. The HM Courts & Tribunals Service (HMCTS) Reform Programme (2016–2025) poured around £1 billion into modernising court processes with technology ([Frontier-economics](#); [Think Digital Partners](#)). This programme has launched 14 new digital services across all jurisdictions, transforming everything from filing small money claims online, to handling divorce petitions and probate applications through web portals ([HMCTS](#)). As of early 2025, over 4.1 million cases had been submitted digitally since 2019 on these platforms. The reforms also introduced a ‘Common Platform’ for criminal cases. This is a unified digital case management system now used to manage 2.3 million+ criminal cases and share data between police, prosecutors, and courts. Infrastructure for remote hearings was scaled up, with video technology installed in 70% of courtrooms (and 90% of Crown courts) even before the pandemic. This investment paid dividends when COVID-19 hit, as courts were able to continue operations via video hearings. User feedback has been positive: online services have earned high satisfaction rates (e.g. ~92% for the civil money claims service, 85% for social security tribunals, and 93% for online probate). The digitisation initiative thus both spurs demand for legal tech (lawyers must interface with new court e-filing systems) and demonstrates government commitment to a tech-enabled legal infrastructure.

Additionally, the Ministry of Justice in 2023 released an AI Strategy for Justice, exploring the use of AI to help tackle court backlogs (for example, using algorithms to assist in reviewing evidence or scheduling cases ([Think Digital Partners](#))). This was followed in 2025 by an [AI Action Plan for Justice](#), which seeks to ‘embed AI across the justice system’ while putting ‘safety and fairness first’ and preserving ‘the independence of judges, prosecutors and oversight bodies’. While still in early

stages, these efforts signal that public-sector legal innovation, leading to ‘online courts’ and AI-assisted administration, is seen as an integral part of the UK’s lawtech progress.

The UK’s lawtech ecosystem is bolstered by partnerships between industry, academia, and even international allies. One notable example is the Global Legal Tech Incubator Programme run by Innovate UK (the UK’s national innovation agency) in collaboration with the Legal Innovation Zone (LIZ) at Toronto Metropolitan University. Through this programme, cohorts of UK legal tech startups are selected to spend six months in Toronto, Canada’s leading legal tech hub, to explore North American market expansion and R&D collaboration ([Legal Innovation Zone](#)). In 2025, the third cohort of UK companies, ranging from an AI-driven claims management startup to an ‘AI-powered justice financing’ platform – participated, receiving mentorship, network access, and exposure to Canadian legal markets. The benefit is mutual: UK startups learn from a global incubator, and the host country gains innovative solutions for local consumers. This reflects how lawtech innovation transcends borders, and the UK is actively positioning its startups on the international stage through government-supported initiatives.

Domestically, universities and research centers are increasingly involved in the development of lawtech. University College London and Oxford University have dedicated research centres in lawtech and AI ethics. The SRA commissioned Oxford’s Said Business School for a major study on technology in legal services ([SRA](#)). Many UK law schools now include legal innovation modules on undergraduate and graduate-level courses, support doctorates in law and AI, and run lawtech societies, preparing newly-trained lawyers to work in and alongside lawtech firms. Events such as [Legal Geek](#)’s annual conference in London draw academics, lawyers, and technologists from around the world to share knowledge. These collaborative efforts underscore the government’s aim to build a community of lawtech practice that includes law firms, tech companies, regulators, scholars, and global partners.

8.4 The Regulatory Environment and Legal Framework for Legal Tech

The UK’s approach to regulating legal tech providers is evolving, seeking to balance innovation with safeguards. Several aspects of the legal and regulatory framework shape this landscape.

Unlike some jurisdictions, English law does not reserve all legal advice to licensed lawyers - only specific ‘reserved legal activities’ (such as conducting litigation, rights of audience in court, probate, notarial acts, etc.) are restricted by law to authorised persons ([Legal Services Board](#)). This means that lawtech platforms can offer certain legal services without being SRA-regulated, as long as they steer clear of reserved activities. The sector regulator for the solicitors’ profession, the Solicitors Regulation Authority (SRA), confirms that ‘unless the service is covering a reserved legal activity, unauthorised persons are free to give [legal] advice’([SRA](#)). Conversely, a document automation app or AI legal Q&A tool can operate outside the regulated sector if it only provides unreserved advice or information.

However, if a tech provider encroaches on reserved work (for example, handling court proceedings or real estate transfers), it must involve a duly authorised solicitor or licensed entity to stay compliant ([SRA](#)). This delineation allows innovation by startups, but also raises consumer protection questions when legal services are delivered by unregulated tech companies. A 2020 independent review led by UCL’s Professor Stephen Mayson urged bringing currently unregulated legal services, including lawtech providers, into a regulatory framework to ensure minimum standards and client redress ([UCL](#)).

Legal tech providers in the UK must navigate a strict data protection regime, given the sensitive client data involved. The EU's General Data Protection Regulation (GDPR) was retained in UK law post-Brexit (now termed the UK GDPR) alongside the Data Protection Act 2018 (dlapiperdataprotection.com). All core GDPR obligations - lawful processing, data subject rights, security standards, breach notification, etc. continue to apply in the UK (dlapiperdataprotection.com). This means that a lawtech firm handling personal data (for example, processing contracts or case files containing personal information) must have robust GDPR compliance: clear user consent or other legal bases for data use, strong security controls, and appropriate data transfer mechanisms if using cloud servers abroad.

Implementation of the Data Use and Access Act 2025 is expected to involve an adjustment to privacy rules but not to significantly change day-to-day GDPR compliance requirements for legal tech businesses ([DLA Piper](#)). In addition to GDPR, legal service providers have duties of client confidentiality. Solicitors must ensure any tech they use upholds confidentiality and legal privilege. The SRA advises firms to vet lawtech vendors accordingly; for example, if using an AI tool that involves third-party processing of client documents, the firm may need to obtain the client's informed consent before disclosure ([SRA](#)). Data residency and cloud storage are also key concerns: many firms require that client data remain on UK/EU servers to meet privacy and professional obligations. Overall, regulators expect lawtech solutions to protect client data as rigorously as traditional practice would, under the combined umbrella of GDPR and solicitor confidentiality rules.

The SRA has adopted a principles-based, tech-neutral approach to AI and innovation. It explicitly 'does not intend to impose specific rules on how firms should use AI,' instead applying existing professional Principles and Codes of Conduct to new technologies ([SRA](#)). In a 2018 position paper, the SRA emphasized that outcomes like confidentiality, integrity, and client care must be achieved regardless of the tools used: 'the duty of confidentiality, for instance, applies to an email just as it applies to a letter' ([SRA](#)). By analogy, if a solicitor uses an AI system, its outputs and impacts should be supervised similar to work done by a human junior lawyer. The SRA notes that because AI can 'learn and develop,' firms should train, supervise and review the output of intelligent machines just as they would a trainee solicitor ([SRA](#)). In practical terms, that means validating AI-generated advice or documents before relying on them, and addressing any mistakes the AI might make.

The SRA and Law Society have issued guidance to help firms manage the risks of AI and automation. Key expectations include: ensuring there is appropriate oversight at senior levels (the firm's Compliance Officer should take responsibility for tech governance); conducting due diligence on vendors and impact assessments before deployment; and maintaining 'responsible adoption' with policies, training, and monitoring in place. Crucially, a solicitor's core professional duties, such as confidentiality, competence, honesty and avoiding conflicts, remain in full force when using technology. For example, if a firm joins an online legal marketplace or uses a document platform, it must ensure the arrangement does not compromise client confidentiality or violate rules on advertising and referral fees ([SRA](#)).

The SRA has warned that solicitors cannot escape liability via the use of AI-related technologies: if work is outsourced or automated, the firm 'will always remain accountable to the SRA' for compliance failures ([SRA](#)). In short, the UK's regulatory stance encourages innovation but insists that technology be used in a way consistent with lawyers' existing ethical obligations. There is also an expectation of understanding the legal framework around AI. The Law Society, for instance, has published guidance on upcoming AI-specific regulations and stresses the importance of transparency with clients when AI tools are involved in legal work ([Thomson Reuters](#)).

At the same time, sector regulators have been fairly proactive in supporting lawtech within this framework. The SRA operates an ‘Innovate’ initiative that welcomes queries from startups and provides informal guidance on regulatory questions ([SRA](#)). Through such engagement (and through the [LawTechUK Sandbox](#)), lawtech providers can seek advice on how far their models comply with rules on legal advice, referrals, and reserved activities.

This collaborative approach aims to clarify grey areas. For example, whether a given legal AI output might risk legal professional privilege or whether an automated service should carry indemnity insurance. The SRA generally refrains from giving definitive legal opinions on privilege or third-party liability, but advises that providers consider insurance and potential duties owed if they are effectively giving legal advice ([SRA](#)).

In summary, the UK’s regulatory environment for lawtech is defined by flexibility with guardrails: technology is permitted and even encouraged, but within the bounds of data protection law and the longstanding professional standards for legal services.

8.5 Generative AI in the Courts

As AI is becoming embedded across various aspects of UK legal practice, from contract analytics to research assistants, courts and confronting the question of reliability of citations. Adoption has surged: law-firm leaders report rapid deployment of generative tools for document review, summarisation and drafting; a recent industry survey found 80% of respondents expect AI to have a ‘high or transformational’ impact on legal workflows within five years, with current usage concentrated in review, summarisation and drafting tasks, though tempered by concerns over quality, usefulness and data security, and with overwhelming support for clear human oversight and bright-line limits on AI representation in court and client-facing legal advice ([Thomson Reuters](#)). The Law Society’s practice commentary similarly charts steady, practical uptake since 2016 and highlights measurable efficiency gains in large-scale data analysis, due diligence and information triage ([Law Society](#)).

Under English law, litigants have a duty not to mislead the court, while under general negligence law, professionals have a responsibility to supervise AI outputs. The US decision in *Mata v. Avianca* has been widely cited as the first significant judicial rebuke for use of fabricated authorities produced by a chatbot. UK courts have since developed a granular line distinguishing negligent reliance on AI from deliberate deceit ([Natural and Artificial Law](#); [Natural and Artificial Law](#)).

In *Santander UK plc v. Carlin & Anor* [2023] NICH 5 there was an early warning that AI systems are unable to recognise or correct users’ misuse; the responsibility remains with the litigant or representative ([Natural and Artificial Law](#)). This was followed by *Felicity Harber v. HMRC* [2023] UKFTT 1007 (TC), in which the tax tribunal reaffirmed the harm caused by citing non-existent or false case law, even in areas where the law is settled ([Natural and Artificial Law](#)). In 2024–2025, significant decisions include the following:

- *Crypto Open Patent Alliance v. Wright* (2024): the court differentiated AI-conjured hallucinations from intentional attempts to mislead; sanctions turn on culpability, not merely the tool used ([Natural and Artificial Law](#)).
- *Olsen v. Finansiel Stabilitet A/S* (2025): litigants in person share the universal duty not to mislead, irrespective of experience or use of AI ([Natural and Artificial Law](#)).
- *Bodrul Zzaman v. HMRC* (2025): the appellant used AI to craft their argument; the tribunal dismissed the appeal, emphasising the need for human checks ([Natural and Artificial Law](#)).

- *Bandla v. Solicitors Regulation Authority* (2025): grounds of appeal struck out as an abuse to protect process integrity against false authorities ([Natural and Artificial Law](#)).
- *UB v. Secretary of State for the Home Department* (2025): draft grounds contained unknown and irrelevant cases; a corrected version existed but the draft was mistakenly filed; the court saw this as an illustration of process risk magnified by AI-assisted drafting ([Natural and Artificial Law](#)).
- *Pro Health Solutions Ltd v. ProHealth Inc* (2025): reliance on ChatGPT introduced fabricated quotations as if from legitimate authorities, underscoring professional-duty risks ([Natural and Artificial Law](#)).
- *Ms (Bangladesh) v. Secretary of State for the Home Department* (2025): limited judicial acceptance of AI-assistance provided 'anxious scrutiny' is applied and human responsibility is maintained ([Natural and Artificial Law](#)).
- *HMRC v. Gunnarsson* (2025): once fictitious cases were removed from the skeleton argument, no further action was taken ([Natural and Artificial Law](#)).

The website [Natural and Artificial Law](#) reports that across roughly 50 reported incidents internationally, courts characterise AI hallucinations as a persistent risk requiring management rather than a one-off aberration. The UK position holds users and representatives to the existing duty not to mislead, demands human verification, and calibrates sanction to culpability. The emerging view is that AI exacerbates some familiar wrongs, but that the risks can be addressed if the use of AI is embedded in supervised and auditable workflows ([Natural and Artificial Law](#)).

Empirical research on the uptake of AI in legal practice is reaching a similar position. UK lawyers report concrete time-savings from AI in due diligence and information triage, but emphasise retained professional agency: firms are setting internal guard-rails, requiring human review of AI outputs and excluding AI from privileged, client-identifying or security-sensitive workflows ([Law Society](#); [Thomson Reuters](#)). Surveyed professionals overwhelmingly reject the use of unsupervised AI in court or as a direct provider of legal advice, insisting on human representation and accountability ([Thomson Reuters](#)).

9. Looking ahead

Policy momentum remains real, but a cross-cutting statutory framework has slipped. A possible Frontier AI Bill has been pushed back to at least the 2026–27 session. Plans for a targeted bill focused on advanced/LLM models, including pre-deployment submissions to the AI Safety Institute, have not yet materialised. Copyright has emerged as a flashpoint, with discussion of a separate data bill that would permit training on copyrighted content unless creators opt out. Public sentiment is not in favour of laissez-faire: polling cited in the same reporting notes 88% support for government intervention where AI products pose serious risk and more than 75% support for formal regulation over private self-governance. Labour-market data suggests steady long-term demand for AI-related skills despite short-term vacancy variation.

In practical terms, the emerging legal consensus around AI in law can be distilled into four key dimensions. Reliability remains paramount: courts increasingly treat AI hallucinations as a known but manageable hazard, with sanctions calibrated to culpability rather than the mere use of technology. The judicial message is clear - AI does not dilute professional duties - and practitioners must embed documented human verification, cross-checking, and citation validation into their workflows to ensure accuracy and accountability. Copyright and data protection form the second pillar. The *Getty Images v Stability AI* litigation is expected to establish the UK baseline for lawful model training and transparency; in the meantime, firms and developers will need to prioritise provenance controls, opt-out mechanisms, and robust licensing strategies to mitigate infringement risk. The third dimension,

governance, has been tightened by the Data (Use and Access) Act 2025 and the ICO's AI and Biometrics Strategy, which elevate expectations for lawful bases, automated-decision-making governance, and marketing-data compliance. Effective AI projects now require built-in Data Protection Impact Assessments (DPIAs), records of processing, and conformity with PECR standards as default practice. Finally, professional limits remain firmly drawn: across the judiciary, regulators, and the market, the current consensus is that AI cannot replace human representation or independent judgment in court or client advice. In this hybrid model of practice, technological innovation must reinforce, rather than erode, the foundational principles of legal responsibility and ethical integrity.

With respect to UK lawtech, significant questions remain. Key among these are issues of liability, professional standards, and transparency, each of which can be expected to affect trust and, over time, levels of adoption. The SRA has made it clear that solicitors cannot outsource or automate their way out of their regulatory duties. If a firm uses an AI assistant or an unregulated provider, the firm is still accountable for compliance as if it did the work in-house ([SRA](#)). In practical terms, this means any negligence or breach arising from a tech tool could fall back on the firm's professional indemnity insurance. Many law firms thus approach AI with caution, keeping a 'human-in-the-loop' to review outputs. In fact, legal professionals overwhelmingly insist on human oversight of AI.

A 2024 Thomson Reuters survey found nearly 100% of respondents agreed that lawyers must rigorously oversee AI's output and set clear boundaries on its use ([Thomson Reuters](#)). Moreover, 96% said allowing an AI to represent clients in court would be 'a step too far,' and 83% felt even using AI to provide direct legal advice to clients (without lawyer input) would be inappropriate. This reflects a strong view that ultimate legal accountability cannot be delegated to a machine. Startups and firms are still figuring out the contours of liability. For instance, some lawtech providers carry their own liability insurance or contractual disclaimers, but if they operate outside regulation, clients may have limited recourse if something goes wrong.

This has prompted debate about whether certain direct-to-consumer lawtech services should be regulated to provide consumer protections. Stephen Mayson's 2020 report recommended that providers of technology-based legal services be brought within the definition of 'legal services' and required to register and insure ([UCL](#)), so that consumers are not left exposed to bad advice. As of 2025, this recommendation has not been implemented.

The influx of AI and algorithmic tools into legal practice is testing the profession's ethical frameworks. Lawyers have duties of competence, confidentiality, and to act in clients' best interests - how do these translate when using AI? One challenge is ensuring quality and avoiding 'AI over-reliance.' Many lawyers fear that junior staff might trust AI outputs without proper verification, leading to errors (a fear fed by real-world incidents like AI chatbots fabricating case citations) ([Thomson Reuters](#)). The SRA has warned of the risk of 'over-reliance' and emphasises that the judgment and expertise of lawyers remain crucial. Firms are responding by developing internal policies for AI use e.g., requiring that any AI-drafted document be clearly labelled and reviewed by a solicitor, or prohibiting use of public AI tools for confidential work due to privacy concerns ([Thomson Reuters](#)).

Another ethical aspect is bias and fairness in algorithms. If courts or law firms start relying on AI (say, for risk assessments or document review triage), they need to ensure the technology does not introduce systemic biases (such as disadvantaging certain groups) or violate principles of justice. Professional bodies in the UK have begun discussing industry-wide AI ethics codes or certification standards ([Thomson Reuters](#)). The Law Society's guidance on AI highlights the need for transparency with clients i.e. lawyers should tell clients when AI is being used in their matter, especially if it

materially affects the service ([Eve Legal](#)). Solicitors must understand the limitations of AI models (for example, the tendency of generative AI to produce plausible-sounding but incorrect answers) to uphold competence ([Thomson Reuters](#)). Ensuring that lawyers are adequately trained in technology is itself a challenge, given that many current senior lawyers received little tech education. The SRA's continuing competence regime now encourages training in technology and data security, and law schools are gradually incorporating tech fluency into the curriculum. All told, the profession is grappling with how to maintain high ethical standards in a tech-augmented practice, working out new best practices around things like AI validation, client consent, and safeguarding confidentiality in digital environments.

A related challenge is the 'black box' nature of many AI systems, which can lack explainability. In law, reasoning and rationale are paramount - a lawyer or judge needs to understand *why* a conclusion was reached. If an AI tool cannot explain its suggestions (as is the case with some deep learning models), this can undermine trust. For use in tasks like legal research or outcome prediction, there are open questions about how to ensure algorithmic transparency. The UK's approach to AI regulation, following the lead set by the 2023 White Paper, leans toward requiring that AI applications, especially in high-stakes areas like justice, have appropriate transparency and oversight mechanisms. This concern is already manifest in client expectations: clients are reportedly becoming more AI-literate and are starting to ask law firms for assurance that AI tools used on their matters are 'secure and ethical' and do not replace the lawyer's judgment ([Thomson Reuters](#)).

Corporate clients may demand to know if work was done by AI and whether that saved cost is passed on, raising transparency in billing. There is also the matter of algorithmic accountability in public sector use. For example, if an AI system aided a judicial decision or a government legal aid triage, the individuals affected might demand an explanation or have the decision reviewed by a human (echoing the 'human in the loop' principle). The lawtech community is actively discussing solutions like 'explainable AI' for law: designing AI that can show the evidence or rules it relied on, or at least indicate confidence levels and allow for audit. While these technical solutions mature, the default in the UK remains that human professionals must stand between AI and the client or public, to ensure decisions can be justified in conventional terms. This cautious approach aims to preserve rule-of-law values as we integrate powerful but opaque technologies.

Beyond AI-specific issues, broader questions persist about legal tech for consumers. Many lawtech offerings, such as will-writing apps and online legal chatbots, operate outside traditional sector regulation. However, consumers may assume that these legal services are regulated, and that they will have recourse if something goes wrong; but this is not the case for unregulated tech products ([UCL](#)). Where the service or product is unregulated, there is no access to the Legal Ombudsman, no guarantee of an insured provider, and potential confusion over the service's legal status. Regulators are monitoring this space but have yet to act. The CMA and Legal Services Board have explored whether consumers understand the difference between regulated and unregulated providers. The prevailing strategy has been to improve transparency (requiring law firms to publish prices and credentials, for example) and to educate the public. However, if lawtech significantly expands access to legal help, regulators may need to step in to mandate baseline consumer protections, extending to currently unregulated activities. This is an open policy question that will shape the next phase of lawtech growth: how to encourage accessible legal services via tech, without creating a two-tier system of protected vs. unprotected consumers.

Thus the UK's lawtech sector finds itself navigating a delicate balance: embracing innovation and its benefits, while confronting the new risks it introduces. Liability regimes, ethical guidelines, and regulatory boundaries are all in flux, and stakeholders are actively debating how to strike the right balance. The coming years will likely see clearer rules on AI use in law (potentially informed by

broader AI legislation and professional self-regulation), and perhaps an extension of the regulatory perimeter to capture more tech-based services for consumer protection. Successfully resolving these issues will be key to sustaining trust in legal technology.

10. Conclusions

In this report we have surveyed the present state of laws and regulations governing AI in the UK. The principal point to emerge from our survey is that the UK has adopted what the government describes as a [pro-innovation, sector-specific approach](#) to regulating AI. This means delegating the task of designing rules and principles of AI governance to sector-level regulators, which are tasked with striking a balance between the need to encourage innovation while identifying emerging areas of AI risk. Although the current government has not ruled out introducing legislation addressing risks of more advanced or ‘frontier’ AI in due course, it has so far avoided going down the route of an overarching or general AI-related law similar to the EU’s AI Act.

In order to assess the current state of AI law and regulation, it is necessary to look at specific areas or domains of regulation to see how the UK’s approach to AI is taking shape. In our report we covered the following fields: data protection, intellectual property, product safety, employment, competition, and the provision of legal services.

Data protection law is one of the areas in which rules and principles governing AI have been most rapidly evolving. The UK’s data protection regulator, the Information Commissioner’s Office, has issued guidance on a number of AI-related issues, including a document setting out its overall approach to AI, [Regulating AI: The ICO’s Strategic Approach](#), published in 2024. In 2025 Parliament passed legislation, in the form of the [Data \(Use and Access\) Act 2025](#), amending the UK GDPR and the Data Protection Act 2018. The ICO is currently amending its guidance in the light of the reforms made by the 2025 Act, which are intended to simplify aspects of the data protection regime, and appear to indicate a more flexible approach to regulation of AI. The compatibility of practices related to AI, such as data scraping, remains to be clarified under the new legislation. The ICO had previously taken the view that AI developers must implement strong transparency measures and opt-out mechanisms in cases where they engage in covert scraping or without the prior permission of the rightsholder.

Intellectual property is an area in which there has been intense public debate concerning the implications of the law for AI, but so far little clarity. Whether data scraping is consistent with UK copyright law, and under what conditions, is not yet resolved. The matter has not been the subject of recent legislation, and the recent High Court ruling in the litigation between [Getty and Stability AI](#) stopped short of providing a clear answer.

Product safety is an area in which the legislator and regulators have been active in a number of fields. The use of autonomous vehicles is being encouraged through legislation, the [Automated Vehicles Act 2024](#), which sets up a process for self-driving vehicles to be authorised for testing and use. This is a model likely to be followed with respect to other products. Liability for harms caused by software is a developing area; the EU’s efforts to align the rules on software with those for products generally has not been followed in the UK, leaving it for the courts to decide how far existing consumer protection legislation applies to digital services.

In the area of labour and employment law, there is no AI-specific legislation, and so far little case law, although there is considerable discussion about the possible implications of AI for existing laws on matters such as dismissal protection and discrimination. The provisions of the UK GDPR with

implications for employment are being loosened as a result of the adoption of the [Data \(Use and Access\) Act 2025](#).

With respect to competition law, the recently adopted [Digital Markets, Competition and Consumers Act 2024](#) grants the Competition and Markets Authority new powers to promote competition and innovation in fast-moving digital markets while protecting consumers against any abuses of power by the larger tech firms. There is discussion on introducing an ‘acquirer-focused’ merger control threshold which would regulate so-called ‘killer acquisitions’ involving larger firms buying up start-ups in areas including AI.

The commercial landscape for legal tech in the UK is undoubtedly thriving, characterised by accelerating adoption, a robust cadre of startups and scale-ups, and supportive engagement from both government and the legal profession. Law firms and in-house legal teams are increasingly investing in technology to improve efficiency, cut costs, and deliver better value to clients, spurred lately by advances in AI and heightened competition in the legal market. However, regulators including the [Solicitor’s Regulatory Authority](#) have emphasised that law firms are responsible for managing risks emerging from the use of AI. There is an emerging debate within the legal profession over the implications of growing use of generative AI in litigation, with a rising number of mis-citations or AI-related ‘hallucinations’ being reported. The government has taken the view that rolling out AI-use across the court system has potential to improve efficiency and cut costs.

Thus overall, the UK’s regulatory approach has so far to enable the use of AI and to encourage innovation while protecting parties at risk from AI-related hazards as they emerge. Regulators have signalled openness to innovation, provided sandboxes and guidance, and avoided over-prescriptive rules, all while insisting that fundamental legal and ethical standards persist in the digital age. This environment has fostered a growing AI-related sector, not least with respect to the legal system, with several world-leading lawtech ventures (from Luminance to ContractPodAi and beyond) attracting significant investment, solidifying the UK’s reputation as a global leader in legal innovation.

On the other hand, the lawtech sector illustrates the wider issue at stake. As our analysis has shown, the rise of lawtech comes with complex challenges. Ensuring data privacy, security, and ethical AI use is paramount in a domain as sensitive as law. The profession is wrestling with how to maintain its high standards of integrity and client care when some services are delivered by algorithms or non-lawyer technologists.

Questions of liability and accountability loom large: the age-old promise that clients can rely on their solicitor’s duties and insurance is being tested when part of the service is performed by a machine. Similarly, the legal system’s legitimacy may eventually require that AI-driven outcomes are explainable and fair. The UK is actively grappling with these issues – through thought leadership (e.g., Law Society and SRA guidelines), through cross-sector initiatives (LawtechUK and academic collaborations), and through incremental regulatory updates. There is recognition that building public trust in legal tech is as important as the technology itself.

In conclusion, the UK’s lawtech sector, as with AI as a whole, stands at an important juncture. The trends are overwhelmingly positive: growing market adoption, enthusiastic support from both private and public sectors, and the potential for technology to greatly enhance access to justice and the quality of legal services. At the same time, achieving that potential will depend on navigating the regulatory and ethical maze, ensuring that innovation does not outpace the legal frameworks needed to manage risk.

With respect to AI in general, the next few years can be expected to bring clearer answers on issues which are as yet unresolved, including the data protection and copyright implications of web-scraping. Product safety rules are likely to evolve in the light of emerging hazards, and AI-related risks in the workplace will receive growing scrutiny. The need to maintain open markets alongside innovation is likely to be a recurring issue in competition policy.

Whether the UK's approach of dealing with AI-related risks as they emerge, rather than through anticipatory measures of the kind adopted in the EU, remains to be seen. The UK's current position by no means represents a legal or policy vacuum, since pre-existing regulations address AI usages in various ways. There is also something to be said for taking a wait-and-see attitude on the risks associated with more advanced or 'frontier' AI. Our, by its nature, can only be an interim account of a fast-developing field.

References

UK legislation

Health and Safety at Work etc. Act 1974 (UK Public Acts 1974 c. 37)

<https://www.legislation.gov.uk/ukpga/1974/37/contents>.

Consumer Protection Act 1987 (UK Public Acts 1987 c. 43)

<https://www.legislation.gov.uk/ukpga/1987/43>.

Copyright, Designs and Patents 1988 (UK Public General Acts 1988 c. 48)

<https://www.legislation.gov.uk/ukpga/1988/48/section/29A>.

Computer Misuse Act 1990 (UK Public General Acts 1990 c. 18)

<https://www.legislation.gov.uk/ukpga/1990/18/contents>.

Employment Rights Act 1996 (UK Public Acts 1996 c. 18)

<https://www.legislation.gov.uk/ukpga/1996/18/contents>.

Copyright and Rights in Databases Regulations 1997 (SI 1997 No. 3032)

<https://www.legislation.gov.uk/uksi/1997/3032/contents/made>.

Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003 No. 2426)

<https://www.legislation.gov.uk/uksi/2003/2426/contents>.

General Product Safety Regulations 2005 (SI 2005 No. 1803)

<https://www.legislation.gov.uk/uksi/2005/1803/contents>.

ISO Standard 62304: 2006 Medical device software – software life cycle processes'

<https://www.iso.org/standard/38421.html>.

Supply of Machinery (Safety) Regulations 2008 (SI 2008 No. 1597)

<https://www.legislation.gov.uk/uksi/2008/1597/contents>.

Equality Act 2010 (UK General Acts 2010 c. 15)

<https://www.legislation.gov.uk/ukpga/2010/15/contents>.

Toys (Safety) Regulations 2011 (SI 2011 No. 1881)

<https://www.legislation.gov.uk/uksi/2011/1881/contents>.

Consumer Rights Act 2015 (UK General Acts 2015 c. 15)

<https://www.legislation.gov.uk/ukpga/2010/15/contents>.

Electrical Equipment (Safety) Regulations 2016 (SI 2016 No. 1101)

<https://www.legislation.gov.uk/uksi/2016/1101/contents>.

Radio Equipment Regulations 2017 (SI 2017 No. 1206)

<https://www.legislation.gov.uk/uksi/2017/1206/contents>.

Data Protection Act 2018 (UK General Acts 2018 c. 12)

<https://www.legislation.gov.uk/ukpga/2018/12/contents>.

UK GDPR <https://www.legislation.gov.uk/eur/2016/679/contents>.

Automated and Electric Vehicles Act 2018 (UK General Acts 2018 c. 18)
<https://www.legislation.gov.uk/ukpga/2018/18/contents>.

Online Safety Act 2023 (UK General Public Acts 2023 c. 50)
<https://www.legislation.gov.uk/ukpga/2023/50>.

Automated Vehicles Act 2024 (UK General Acts 2024 c. 10)
<https://www.legislation.gov.uk/ukpga/2024/10/contents>.

Digital Markets, Competition and Consumers Act 2024 (UK General Public Acts 2024 c. 13)
<https://www.legislation.gov.uk/ukpga/2024/13/contents>.

Cyber Security and Resilience (Network Information and Systems) Bill 2025
<https://bills.parliament.uk/bills/4035>.

Data (Use and Access) Act 2025 (UK Public Acts 2025 c. 18)
<https://www.legislation.gov.uk/ukpga/2025/18/contents>.

Employment Rights Bill 2025 <https://bills.parliament.uk/bills/3737>.

UK case law

Bandla v. Solicitors Regulation Authority [2025] EWHC 1167
[https://uk.practicallaw.thomsonreuters.com/D-110-6255?transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/D-110-6255?transitionType=Default&contextData=(sc.Default)&firstPage=true).

Bodrul Zzaman v. HMRC [2025] UKFTT 00539 <https://www.rossmartin.co.uk/sme-tax-news/8457-ai-fails-to-help-taxpayer-in-hicbc-appeal>.

BHB v. William Hill [2005] EWCA Civ 863 <https://www.wipo.int/wipolex/en/judgments/details/1485>.

Cresswell v. Board of Inland Revenue [1984] IRLR 190
https://en.wikipedia.org/wiki/Cresswell_v_Board_of_Inland_Revenue.

Crypto Open Patent Alliance v. Wright [2024] EWHC 3135
<https://www.judiciary.uk/judgments/crypto-open-patent-alliance-v-wright-order/>.

Getty Images (US) Inc v. Stability AI Ltd [2025] EWHC 2863 <https://www.judiciary.uk/wp-content/uploads/2025/11/Getty-Images-v-Stability-AI.pdf>.

HMRC v. Gunnarsson [2025] UKUT 247 <https://www.gov.uk/tax-and-chancery-tribunal-decisions/the-commissioners-for-hm-revenue-and-customs-v-marc-gunnarsson-2025-ukut-00247-tcc>.

Independent Workers Union of Great Britain v. CAC and Rooffoods Ltd t/a Deliveroo [2023] UKSC 43
<https://www.supremecourt.uk/cases/uksc-2021-0155>.

Ms (Bangladesh) v. Secretary of State for the Home Department [2025] UKUT 305
<https://tribunalsdecisions.service.gov.uk/utiac/ui-2025-001831>.

Newspaper Licensing Agency Ltd v Meltwater Holding BV [2013] UKSC 18
https://web.archive.org/web/20160308062504/https://www.supremecourt.uk/decided-cases/docs/UKSC_2011_0202_Judgment.pdf.

Olsen v. Finansiel Stabilitet A/S [2025] EWHC 42 <https://www.judiciary.uk/wp-content/uploads/2025/01/Approved-Judgment-Olsen-v.-Finansiel-Stabilitet-AS.pdf>.

Online sales of posters and frames, Competition and Markets Authority Decision, Case 50223 (August 2016) <https://assets.publishing.service.gov.uk/media/57ee7c2740f0b606dc000018/case-50223-final-non-confidential-infringement-decision.pdf>.

Pro Health Solutions Ltd v. ProHealth Inc BL O/0559025 <https://www.ipo.gov.uk/t-challenge-decision-results/o055925.pdf>.

Public Relations Consultants Association Ltd v. The Newspaper Licensing Agency Ltd [2013] UKSC 13
<https://www.supremecourt.uk/cases/uksc-2011-0202>.

UB v. Secretary of State for the Home Department UI-2025-000834
<https://tribunalsdecisions.service.gov.uk/utiac/ui-2025-000834>.

Uber BV v. Aslam [2021] UKSC 5 <https://www.supremecourt.uk/cases/uksc-2019-0029>.

UK official reports (White Papers, Policy Papers and others)

HM Government (2017) *Industrial Strategy. Building a Britain Fit for the Future*
<https://assets.publishing.service.gov.uk/media/5a8224cbcd915d74e3401f69/industrial-strategy-white-paper-web-ready-version.pdf>.

HM Government (2019) *AI Sector Deal* <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal>

HM Government (2019) *AI Council* <https://www.gov.uk/government/groups/ai-council>.

HM Government (2021) *National AI Strategy* <https://www.gov.uk/government/publications/national-ai-strategy>.

HM Government (2023) *A Pro-Innovation Approach to AI Regulation* Command Paper Number: 815
<https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>.

HM Government (2023) *Independent Review of the Future of Compute*
<https://www.gov.uk/government/publications/future-of-compute-review>.

HM Government (2024) *A Pro-Innovation Response to AI Regulation: Government Response*
<https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response#annex-a-method-and-engagement>.

HM Government (2024) *Implementing the UK's AI Regulatory Principles: Initial Guidance for Regulators* <https://www.gov.uk/government/publications/implementing-the-uks-ai-regulatory-principles-initial-guidance-for-regulators/implementing-the-uks-ai-regulatory-principles-initial-guidance-for-regulators>.

HM Government (2024) 'UK signs first international treaty addressing risks of artificial intelligence' press release 5 September 2024 <https://www.gov.uk/government/news/uk-signs-first-international-treaty-addressing-risks-of-artificial-intelligence>.

HM Government (2024) 'Copyright and AI: Consultation' <https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence/copyright-and-artificial-intelligence>.

HM Government (2025) *AI Opportunities Action Plan* <https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan>.

HM Government (2025) 'Investment in British AI companies hits record levels as Tech Sec pitches UK as global magnet' press release 3 September 2025 <https://www.gov.uk/government/news/investment-in-british-ai-companies-hits-record-levels-as-tech-sec-pitches-uk-as-global-magnet>.

HM Government (2025) *Artificial Intelligence Playbook for the UK Government* <https://www.gov.uk/government/publications/ai-playbook-for-the-uk-government/artificial-intelligence-playbook-for-the-uk-government-html>.

HM Government (2025) *Trusted Third-Party AI Assurance Roadmap* policy paper <https://www.gov.uk/government/publications/trusted-third-party-ai-assurance-roadmap>.

HM Government (2025) *Explanatory Notes. Data (Use and Access) Act 2025* https://www.legislation.gov.uk/ukpga/2025/18/pdfs/ukpgaen_20250018_en.pdf.

HM Government (2025) *Data (Use and Access) Act 2025: Data Protection and Privacy Changes* <https://www.gov.uk/guidance/data-use-and-access-act-2025-data-protection-and-privacy-changes>.

HM Government (2025) *Make Work Pay* <https://www.gov.uk/government/collections/make-work-pay>.

UK Parliamentary debates

Hansard 'AI technology regulations' <https://hansard.parliament.uk/lords/2024-07-30/debates/C1541E2E-0AE3-486C-9077-42CBA1785164/AITechnologyRegulations>.

Other UK official documents

AI Security Institute (2025) 'Rigorous AI research to enable advanced AI governance' <https://www.aisi.gov.uk/>.

Alan Turing Institute (2025) 'AI for science and government (ASG)' <https://www.turing.ac.uk/about-us/impact/asg>.

BridgeAI (2025) 'Empowering UK organisations to harness the power of AI through support and funding, bridging the AI divide for a more productive UK' <https://iuk-business-connect.org.uk/programme/bridgeai/>.

BSI (2019) *The Emergence of Artificial Intelligence and Machine Learning Algorithms in Healthcare: Recommendations to Support Governance and Regulation* <https://www.bsigroup.com/globalassets/localfiles/en-gb/about-bsi/nsb/innovation/mhra-ai-paper-2019.pdf>.

CMA (2018) 'Pricing algorithms: economic working paper on the use of algorithms to facilitate collusion and personalised pricing' https://assets.publishing.service.gov.uk/media/5bbb2384ed915d238f9cc2e7/Algorithms_econ_report.pdf.

CMA (2023) 'Cloud services market investigation' <https://www.gov.uk/cma-cases/cloud-services-market-investigation>.

CMA (2024) 'AI foundation models: update paper' <https://www.gov.uk/government/publications/ai-foundation-models-update-paper>.

CMA (2024) 'CMA AI strategic update' <https://hai.stanford.edu/ai-index/2025-ai-index-report>.

CMA (2025) 'How the UK's digital markets competition regime works' <https://www.gov.uk/guidance/how-the-uks-digital-markets-competition-regime-works>.

CMA (2025) 'SMS investigation into Google's general search and search advertising services' <https://www.gov.uk/cma-cases/sms-investigation-into-googles-general-search-and-search-advertising-services>.

CMA (2025) 'SMS investigation into Google's mobile platform' <https://www.gov.uk/cma-cases/sms-investigation-into-googles-mobile-platform>.

CMA (2025) 'SMS investigation into Apple's mobile platform' <https://www.gov.uk/cma-cases/sms-investigation-into-apples-mobile-platform>.

CMA (2025) 'CMA takes first steps to improve competition in search services in the UK' press release <https://www.gov.uk/government/news/cma-takes-first-steps-to-improve-competition-in-search-services-in-the-uk>.

DBT (2024) 'Product Regulation and Metrology Bill – Artificial Intelligence' https://data.parliament.uk/DepositedPapers/Files/DEP2024-0804/Lord_Leong_to_Lord_Holmes_of_Richmond-PRAM_Bill_AI.pdf.

Department of Education (2015) 'Keeping Children Safe in Education' <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>.

Department of Education (2022) 'Meeting digital and technology standards in schools and colleges' <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>.

Department of Education (2025) 'Generative AI: product safety expectations' <https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations#:~:text=Generative%20AI%20products%20must%20effectively,top%20of%20an%20AI%20product.>

Government Equalities Office (2022) 'Public Sector Equality Duty: guidance for public authorities' <https://www.gov.uk/government/publications/public-sector-equality-duty-guidance-for-public-authorities>.

HMCTS (2025) 'Modernising courts and tribunals: benefits of digital services' <https://www.gov.uk/guidance/modernising-courts-and-tribunals-benefits-of-digital-services#:~:text=Through%20the%20programme%20we%3A>.

ICO (2023) 'Guidance on AI and data protection' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/>.

ICO (2023) 'AI and data protection risk toolkit' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/>.

IPO (2023) 'Intellectual property: an overview' <https://www.gov.uk/intellectual-property-an-overview>.

IPO (2023) 'Intellectual property: copyright' <https://www.gov.uk/government/collections/intellectual-property-copyright>.

IPO (2024) 'Copyright and artificial intelligence' <https://www.gov.uk/government/consultations/copyright-and-artificial-intelligence>.

ICO (2024) 'ICO consultation series on generative AI and data protection' <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/2024/09/ico-consultation-series-on-generative-ai-and-data-protection/>.

ICO (2024) 'Regulating AI: the ICO's Strategic Approach' <https://ico.org.uk/media2/migrated/4029424/regulating-ai-the-icos-strategic-approach.pdf>.

ICO (2025) 'The UK GDPR' <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/>.

ICO (2025) 'Preventing harm, promoting trust: our AI and biometrics strategy' <https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/artificial-intelligence-and-biometrics-strategy/>.

ICO (2025) 'The Data Use and Access Act 2025 (DUAA) - what does it mean for organisations?' <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/the-data-use-and-access-act-2025-what-does-it-mean-for-organisations/>.

ICO (2025) 'ICO launches consultations for Data (Use and Access) Act 2025 amendments' <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/08/ico-launches-consultations-for-data-use-and-access-act-2025-amendments/>.

ICO (2025) 'What does the UK GDPR say about automated decision-making and processing?' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/>.

ICO (2025) 'Rights related to automated decision making including profiling' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/rights-related-to-automated-decision-making-including-profiling/>.

ICO (2025) 'Parental controls' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/11-parental-controls/>.

ICO (2025) 'Introduction to the Children's code' <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/>.

Law Commission (2025) 'Product liability' <https://www.legislation.gov.uk/ukpga/2025/20>.

Law Commission (2025) 'Artificial intelligence and the law: a discussion paper' <https://lawcom.gov.uk/publication/artificial-intelligence-and-the-law-a-discussion-paper/>.

Legal Services Board (2025) 'Reserved legal activities' <https://legalservicesboard.org.uk/enquiries/frequently-asked-questions/reserved-legal-activities#:~:text=Reserved%20legal%20activities%20,right%20of%20audience%2C%20litigation%2C>.

Ministry of Justice (2022) 'Further investment in digital transformation of UK's legal sector' press release <https://www.gov.uk/government/news/further-investment-in-digital-transformation-of-uk-s-legal-sector#:~:text=LawtechUK%20is%20a%20government,legal%20services%20via%20digital%20solutions>.

Ministry of Justice (2025) 'AI action plan for justice' <https://www.gov.uk/government/publications/ai-action-plan-for-justice/ai-action-plan-for-justice>.

NHS England (2025) 'NHS Lab AI Lab ethics initiative' <https://digital.nhs.uk/services/ai-knowledge-repository/nhs-lab-ai-ethics-initiative>.

Office for Product and Safety Standards (2025) 'AI's evolving role in product safety' <https://opss.blog.gov.uk/2025/07/14/ais-evolving-role-in-product-safety/>.

RIO (2025) 'Regulatory Innovation Office: One Year On' https://assets.publishing.service.gov.uk/media/68f7548ffd57416292f12d9a/regulatory_innovation_office_one_year_on.pdf.

SRA (2018) 'Technology and legal services' <https://www.sra.org.uk/sra/research-publications/technology-legal-services/#:~:text=The%20legal%20market%20faces%20challenges,work%20quicker%20and%20more%20efficient>.

SRA (2022) 'Lawtech providers Q&A'

<https://www.sra.org.uk/solicitors/resources/innovate/common-queries-answered/#:~:text=The%20SRA%20cannot%20provide%20a,free%20to%20give%20such%20advice.>

SRA (2022) 'Compliance tips for solicitors regarding the use of AI and technology'

<https://www.sra.org.uk/solicitors/resources/innovate/compliance-tips-for-solicitors/#:~:text=To%20ensure%20there%20is%20senior,the%20risks%20of%20technology%20failure.>

European Union legal and official documents

Product Liability Directive (1985) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374>

European Commission (2019) 'Ethics guidelines for trustworthy AI' <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

Artificial Intelligence Act <https://artificialintelligenceact.eu/ai-act-explorer/>.

Product Liability Directive (2024) <https://eur-lex.europa.eu/eli/dir/2024/2853/oj/eng>.

Platform Work Directive (2024) <https://eur-lex.europa.eu/eli/dir/2024/2831/oj/eng>.

European Commission 'Adequacy decisions' https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Code of Practice for General-Purpose AI <https://artificialintelligenceact.eu/introduction-to-code-of-practice/>.

Draft Directive on Algorithmic Management

https://www.europarl.europa.eu/doceo/document/EMPL-PR-774283_EN.pdf.

European Commission (2025) 'Commission opens antitrust investigation into Meta's new policy regarding AI providers' access to Whatsapp' press release

https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2896.

EU Digital Omnibus https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2718.

Official documents from other countries

ACM (2020) 'Research on monitoring of algorithmic applications'

<https://www.acm.nl/nl/publicaties/onderzoek-naar-toezicht-op-algoritmische-toepassingen>.

CNIL (2025) 'AI and GDPR: the CNIL publishes new recommendations to support responsible innovation'

<https://www.cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-support-responsible-innovation>.

IEEE (2019) 'White Paper – ethically aligned design – a vision for prioritising human well-being with autonomous and intelligent systems' <https://ieeexplore.ieee.org/document/9398613>.

OECD (2025) 'OECD AI Principles' <https://oecd.ai/en/ai-principles>.

OECD (2025) 'Intellectual property issues in artificial intelligence trained on scraped data' OECD Artificial Intelligence Papers No. 39 June 2025

https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/the-effects-of-generative-ai-on-productivity-innovation-and-entrepreneurship_da1d085d/b21df222-en.pdf.

Secondary literature

Abraha, H. (2023) 'Regulating algorithmic employment decisions through data protection law' *European Labour Law Journal*, 14: 172-191

<https://journals.sagepub.com/doi/10.1177/20319525231167317>.

Adams-Prassl, J., Binns, R. and Kelly-Lyth, A. (2022) 'Directly discriminatory algorithms' *Modern Law Review*, 86: 144-175 <https://onlinelibrary.wiley.com/doi/10.1111/1468-2230.12759>.

Ahn Le, V. (2025) 'Copyright of photography and artificial intelligence: a tale of two technologies' *Journal of Intellectual Property Law and Practice*, 20: 562-569

<https://academic.oup.com/jiplp/article/20/8/562/8203364>.

Aloisi, A., Joppe, A. and Abraha, H. (2025) 'From "general" to "context-specific" data protection for workers: insights from the EU rules on platforms, algorithmic management and AI systems' *European Labour Law Journal* online first https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5273823.

Atkinson, J. and Collins, P. (2024) *Algorithmic Management and a New Generation of Rights at Work* (London: Institute of Employment Rights). Available at SSRN: <https://ssrn.com/abstract=4853536> or <http://dx.doi.org/10.2139/ssrn.4853536>.

Barocas, S. and Selbst, A. (2016) 'Big data's disparate impact' *California Law Review*, 104: 671-732.

Bishop, L., Carter, C., Deakin, S. and Pourkermani, K. (2025) 'Labour rights in the digital economy: A first look at the CBR Platform Work Index', Digit Data Commentary 06, Digital Futures at Work Research Centre, available at: https://digit-research.org/data_commentaries/labour-rights-in-the-digital-economy.

Bogg, A. (2021) 'For whom the bell tolls: "contract" in the gig economy' OxHRH blog <https://ohrh.law.ox.ac.uk/for-whom-the-bell-tolls-contract-in-the-gig-economy/>.

Buick, A. (2024) 'Copyright and AI training data – transparency to the rescue?' *Journal of Intellectual Property Law & Practice*, 20: 182-192 <https://academic.oup.com/jiplp/article/20/3/182/7922541>.

Collins, P. (2021) 'Automated dismissal decisions, data protection and the law of unfair dismissal' UK Labour Law Blog, 19 October 2021 <https://uklabourlawblog.com/2021/10/19/automated-dismissal-decisions-data-protection-and-the-law-of-unfair-dismissal-by-philippa-collins/>.

Countouris, N. and De Stefano, V. (2025) "'Not the usual gig": the personal scope(s) of application of Directive 2024/2831 on improving working conditions in platform work' (2025) *European Labour Law Journal* <https://journals.sagepub.com/doi/10.1177/20319525251375028>.

De la Durantaye, K. (2024) 'Control and compensation. A comparative analysis of copyright exceptions for training generative AI (June 17, 2024)'. 56 *International Review of Intellectual Property and Competition Law* (IIC) (2025), Available at SSRN: <https://ssrn.com/abstract=5021889> or <http://dx.doi.org/10.2139/ssrn.5021889>.

Deakin, S. (2020) 'Decoding employment status' *King's Law Journal*, 31: 180-193
<https://www.tandfonline.com/doi/full/10.1080/09615768.2020.1789432>.

Geiger, C. (2024) 'Elaborating a human rights friendly copyright framework for generative AI. (April 12, 2024). *International Review for Intellectual Property and Competition Law* 2024, Vol. 55, Issue 7, pp. 1129–1165. Available at SSRN: <https://ssrn.com/abstract=4634992> or <http://dx.doi.org/10.2139/ssrn.4634992>.

Hiessl, C. (2025) 'Case law on algorithmic management at the workplace: cross-European comparative analysis and tentative conclusions' (April 16, 2025). Available at SSRN: <https://ssrn.com/abstract=3982735> or <http://dx.doi.org/10.2139/ssrn.3982735>.

Hugenholz, P. and Quintais, J.P. (2021) 'Copyright and artificial creation: does EU copyright law protect AI-assisted output?' *International Review of Intellectual Property and Competition Law*, 52; 1190-1216 <https://link.springer.com/article/10.1007/s40319-021-01115-0>.

Kretschmer, M, Margoni, T. and Oruc, P. (2023) 'Copyright law, and the lifecycle of machine learning models' (December 20, 2023). Available at SSRN: <https://ssrn.com/abstract=4670563> or <http://dx.doi.org/10.2139/ssrn.4670563>.

Lin, Y. and Guan, T. (2025) 'From safe harbours to AI harbours: reimagining DMCA immunity for the generative AI era' *Journal of Intellectual Property Law & Practice*, 20: 606-616
<https://academic.oup.com/jiplp/article/20/9/605/8221820>.

O'Callaghan, M. (2023) 'Could output produced autonomously by AI systems enjoy copyright protection, and should it? An analysis of the current legal position and the search for the way forward' *Cornell International Law Journal*, 55: 306-350.

Pitt, G. (2024) "'The simple things you see are all complicated": thoughts on *Deliveroo*' *Industrial Law Journal*, 53: 784-795 <https://academic.oup.com/ilj/article/53/4/784/7903072>.

Quintais, J.P. (2025) 'Generative AI, copyright and the AI Act' *Computer Law and Security Review*, 56, 106107 <https://www.sciencedirect.com/science/article/pii/S0267364925000020>.

Matulionyte, R., Formosa, P., Strowel, A. and Montefiore, T. 'Data transparency and copyright: opportunities and challenges' (October 20, 2025). Available at SSRN: <https://ssrn.com/abstract=5629050> or <http://dx.doi.org/10.2139/ssrn.5629050>.

Militsyna, K. (2025) 'On the carrot and the stick that unfair competition law can offer to AI-based work-like output' *GRUR International*, 74: 834-844
<https://academic.oup.com/grurint/article/74/9/834/8214128>.

Rosati, E (2025) 'Copyright exceptions and fair use defences for AI training done for "research" and "learning", or the inescapable licensing horizon' (June 30, 2025) *European Journal of Risk Regulation*. Available at SSRN: <https://ssrn.com/abstract=5331405> or <http://dx.doi.org/10.2139/ssrn.5331405>.

Samuelson, P. (2024) 'Fair use defenses in disruptive technology cases' (November 8, 2023). 71 UCLA L. Rev. 1484 (2024). Available at SSRN: <https://ssrn.com/abstract=4631726>.

Sanders, A. (2025) 'Article 3 in the Platform Work Directive on intermediaries: joint liability or joint employment?' *European Labour Law Journal* online first
<https://journals.sagepub.com/doi/full/10.1177/20319525251375025>.

Sheard, N. (2025) 'Algorithm-facilitated discrimination: a socio-legal study of the use by employers of artificial intelligence hiring systems' *Journal of Law and Society* 52: 269-291.

Zhang, J. (2025) 'Input out, output in: towards positive-sum solutions to AI-copyright tensions' *Journal of Intellectual Property Law & Practice*, 20: 594-604
<https://academic.oup.com/jiplp/article/20/9/594/8220785>.

Blogs

A&O Shearman (2025) 'UK AI: existing regulators take the lead'
<https://www.aoshearman.com/en/insights/ao-shearman-on-data/uk-ai-existing-regulators-take-the-lead>.

A&O Shearman (2025) 'FCA summary of AI Sprint' <https://finreg.aoshearman.com/FCA-summary-of-AI-Sprint>.

A&O Shearman (2025) 'UK Information Commissioners Office launches AI and biometrics strategy'
<https://www.aoshearman.com/en/insights/ao-shearman-on-data/uk-information-commissioners-office-launches-ai-and-biometrics-strategy>.

Ada Lovelace Society (2025) 'Will the UK AI Bill protect people and society?'
<https://www.adalovelaceinstitute.org/blog/uk-ai-bill/>.

Alan Turing Institute (2025) '7 out of 10 say laws and regulations would increase their comfort with AI amid rising public concerns, national survey finds' <https://www.turing.ac.uk/news/7-10-say-laws-and-regulations-would-increase-their-comfort-ai-amid-rising-public-concerns>.

Bird & Bird (2021) 'Legal weapons in the fight against data scraping'
<https://www.twobirds.com/en/insights/2021/global/legal-weapons-in-the-fight-against-data-scraping#:~:text=recourse%20against%20data%20scrapers,criminal%20offence%20in%20some%20circumstances>.

Bird & Bird (2024) 'The Digital Markets, Competition and Consumer Bill passes: a new era begins'
<https://www.twobirds.com/en/insights/2024/uk/the-digital-markets-competition-and-consumer-bill-passes-a-new-era-begins>.

CREATe (2025) 'The law of data scraping: a review of UK law on text and data mining'
<https://www.create.ac.uk/blog/2021/03/30/new-working-paper-the-law-of-data-scraping-a-review-of-uk-law-on-text-and-data-mining/#:~:text=Those%20looking%20to%20the%20law,to%20removing%20some%20of%20the>.

Deloitte (2024) 'The UK's framework for AI regulation'
<https://www.deloitte.com/uk/en/blogs/ecrs/the-uks-framework-for-ai-regulation.html>.

Digicon (2024) 'The need to update the Artificial Intelligence Act to make it Human Rights Act compliant' <https://digi-con.org/the-need-to-update-the-artificial-intelligence-act-to-make-it-human-rights-compliant/>.

DLA Piper (2025) 'Digital protection laws in the UK' <https://www.dlapiperdataprotection.com/?c=GB#:~:text=Following%20the%20UK%E2%80%99s%20exit%20from%20EU%20Exit%29%20Regulations%202019.>

Eve Legal (2025) 'Disclosing AI usage to your clients: best practices for legal teams' <https://www.eve.legal/blogs/disclosing-ai-usage-to-your-clients-best-practices-for-legal-teams#:~:text=Disclosing%20AI%20Usage%20to%20Your,of%20providing%20competent%2C%20fair%20representation.>

Frontier Economics (2025) 'Evaluation of HMCTS digital reform programme finds improvements for many' <https://www.frontier-economics.com/uk/en/news-and-insights/news/news-article-i21883-evaluation-of-hmcts-digital-reform-programme-finds-improvements-for-many/#:~:text=Evaluation%20of%20HMCTS%20digital%20reform,better%20ensure%20it%20is.>

Global Legal Post (2025) 'Legal AI startup Luminance, backed by Slaughter and May, raises \$75m' <https://www.globallegalpost.com/news/legal-ai-start-up-luminance-backed-by-slaughter-and-may-raises-75m-897378499#:~:text=Luminance%E2%80%99s%20latest%20round%20was%20led,Partners%20and%20Slaughter%20and%20May.>

Guardian (2024) 'UK arts and media reject plan to let AI firms use copyrighted material' <https://www.theguardian.com/technology/2024/dec/19/uk-arts-and-media-reject-plan-to-let-ai-firms-use-copyrighted-material.>

Guardian (2025) 'Labour MPs to demand more concessions on workers' rights after government climbdown' <https://www.theguardian.com/politics/2025/nov/28/labour-mps-to-demand-more-concessions-on-workers-rights-after-government-climbdown.>

HFS Kramer (2023) 'UK withdraws plans for broader Text and Data Mining (TDM) copyright and database right exception' <https://www.hsfkramer.com/notes/ip/2023-03/uk-withdraws-plans-for-broader-text-and-data-mining-tdm-copyright-and-database-right-exception#:~:text=Text%20and%20data%20mining%20,copyright%20or%20database%20right%20infringement.>

HFW (2024) 'UK's Automated Vehicles Act 2024' <https://www.hfw.com/insights/uks-automated-vehicles-act-2024/>.

Hogan Lovells (2024) 'An overview of the new EU Product Liability Directive: businesses beware' <https://www.hoganlovells.com/en/publications/new-eu-product-liability-directive-businesses-beware.>

Hogan Lovells (2025) 'New CNIL's guidance on AI models: a practical approach amidst EU's regulatory tangles' <https://www.hoganlovells.com/en/publications/new-cnils-guidelines-on-ai-models-a-practical-approach-amidst-eus-regulatory-tangles.>

Hunton (2024) 'CNIL publishes new guidelines on the development of AI systems' <https://www.hunton.com/privacy-and-information-security-law/cnil-publishes-new-guidelines-on-the-development-of-ai-systems>.

Hunton (2025) 'UK (Data Use and Access) Bill to become law' <https://www.hunton.com/privacy-and-information-security-law/uk-data-use-and-access-bill-to-become-law#:~:text=became%20entangled%20in%20debates%20over,data%20inputs%20for%20AI%20models>.

IBA (2025) 'Liability for software under the new European product liability directive' https://www.ibanet.org/European-Product-Liability-Directive-liability-for-software?utm_source=chatgpt.com.

Inview (2024) 'The 2024 In-house legal technology report' <https://inview.lawvu.com/2024-in-house-legal-technology-report/#:~:text=The%20Report%20signals%20an%20overwhelming,risk%20routine%20tasks>.

Kennedys Law (2025) 'The Artificial Intelligence (Regulation) Bill: closing the UK's AI regulation gap?' <https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-artificial-intelligence-regulation-bill-closing-the-uks-ai-regulation-gap/>.

King & Spalding (2025) 'EU and UK AI round-up – July 2025' <https://www.kslaw.com/news-and-insights/eu-uk-ai-round-up-july-2025>.

Law Society (2024) 'How AI is reshaping the future of legal practice' <https://www.lawsociety.org.uk/topics/ai-and-lawtech/partner-content/how-ai-is-reshaping-the-future-of-legal-practice>.

Law Society (2025) 'Changes to GDPR – what solicitors need to know' <https://www.lawsociety.org.uk/topics/gdpr/changes-to-gdpr-solicitors>.

Legal Geek (2025) 'London lawtech incubators' <https://www.legalgeek.co/may-14th-day-london-lawtech-incubators/#:~:text=On%2014%20May%2C%20the%20international,to%20open%20in%20September%202017>.

Legal Innovation Zone (2025) 'Welcoming more UK tech solutions to Canada' <https://www.torontomu.ca/zone-learning/legal-innovation-zone/news/press-releases/2025/09/welcoming-more-uk-legal-tech-solutions-to-canada/#:~:text=TORONTO%2C%20September%202nd%2C%202025%20%E2%80%94,and%20explore%20the%20Canadian%20Market>.

Loyens and Loeff (2025) 'AI: redefining the boundaries of competition (law)' <https://www.loyensloeff.com/insights/news--events/news/ai-redefining-the-boundaries-of-competition-law/>.

Mayer Brown (2023) 'The UK government's approach to regulating the use of Artificial Intelligence' <https://www.mayerbrown.com/en/insights/publications/2023/07/uks-approach-to-regulating-the-use-of-artificial-intelligence>.

Mayer Brown (2024) 'UK government response to AI consultation regulation'
<https://www.mayerbrown.com/en/insights/publications/2024/03/uk-government-response-to-ai-regulation-consultation>.

Mayer Brown (2024) 'AI challenges in competition law: how are regulators responding?'
https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2024/04/ai-challenges-in-competition-law_mar24.pdf%3Frev=55168f8e10a64e458c3fc1ac7af179df.

Natural and Artificial Law (2025) '12 false citations/AI hallucinations incidents in UK courts: the complete legal timeline before and after Ayinde and how pervasive is the problem?'
<https://naturalandartificiallaw.com/false-citations-ai-hallucinations-uk/>

Natural and Artificial Law (2025) 'The 8 most common types of AI hallucinations /false citations in case law'
<https://naturalandartificiallaw.com/ai-hallucinations-in-case-law/>.

Non-Billable (2024) 'The UK's hottest legal tech companies in 2024'
<https://www.nonbillable.co.uk/posts/hottest-legal-tech-companies#:~:text=The%20UK%20is%20a%20great,and%20most%20prestigious%20law%20firms>.

Osborne Clarke (2023) 'Generative AI: can intellectual property infringements in training data be prevented?'
<https://www.osborneclarke.com/insights/generative-ai-can-intellectual-property-infringements-training-data-be-avoided>.

Pinsent Masons (2025) 'UK AI action plan provides for shift in regulatory approach'
<https://www.pinsentmasons.com/out-law/news/uk-ai-action-plan-regulatory-shift>.

Pinsent Masons (2025) 'Getty Images v Stability AI: Getty's copyright case against Stability AI fails'
<https://www.pinsentmasons.com/out-law/news/gettys-copyright-case-against-stability-ai-fails>.

Paul Weiss (2025) 'EU Commission publishes its Code of Practice for General Purpose AI: what you need to know'
<https://www.paulweiss.com/insights/client-memos/eu-commission-publishes-its-code-of-practice-for-general-purpose-ai-what-you-need-to-know>.

RPC Legal (2013) 'Copyright: Supreme Court considers "browsing defence"'
<https://www.rpclegal.com/thinking/ip/copyright-supreme-court-considers-browsing-defence/#:~:text=Comment>.

Slaughter and May (2023) 'Competition and regulatory newsletter: CMA clears Microsoft's acquisition of Activision Blizzard'
<https://www.slaughterandmay.com/insights/importedcontent/competition-regulatory-newsletter-cma-clears-microsoft-s-acquisition-of-activision-blizzard/>.

Stanford AI Index (2025) <https://hai.stanford.edu/ai-index/2025-ai-index-report>.

Taylor Wessing (2024) 'AI and competition law: the next frontier?'
<https://www.taylorwessing.com/en/insights-and-events/insights/2024/08/ai-and-competition-law-the-next-frontier>.

Taylor Wessing (2025) 'Game, set and match! UK's Data (Use and Access) Act passes'
<https://www.taylorwessing.com/en/insights-and-events/insights/2025/06/game-set-and-match>.

The Lawyer (2025) 'Value of Thomson Reuter's HighQ purchase revealed'
<https://www.thelawyer.com/value-of-thomson-reuters-highq-purchase-revealed/#:~:text=Value%20of%20Thomson%20Reuters%27%20HighQ,considerable%20growth%20for%20the>.

Think Digital Partners (2025) 'MOJ to use AI to overhaul UK justice system'
<https://www.thinkdigitalpartners.com/news/2025/08/04/moj-to-use-ai-to-overhaul-uk-justice-system/#:~:text=Partners%20www,increase%20prison%20capacity%20and>.

Thomson Reuters (2025) 'How AI is transforming the legal profession'
<https://legal.thomsonreuters.com/blog/how-ai-is-transforming-the-legal-profession/#:~:text=>.

Thomson Reuters Institute (2024) '2024 report on the state of the UK legal market: positivity amidst volatility'
<https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2024/04/State-of-UK-Legal-Market-2024.pdf#:~:text=Let%E2%80%99s%20take%20a%20look%20at,these%20professionals%20to%20spend%20their>.

TLT (2022) 'CJEU determines that the supply of computer software is "sale of goods"'
<https://www.tlt.com/insights-and-events/insight/cjeu-determines-that-the-supply-of-computer-software-is-sale-of-goods>.

UCL (2022) 'Measures to address "unregulated" legal services will enhance consumer protection'
<https://www.ucl.ac.uk/news/2020/jun/measures-address-unregulated-legal-services-will-enhance-consumer-protection#:~:text=Professor%20Mayson%20,online%20advice%20and%20bespoke%20documents>.