

CHAPTER 11

UNITED KINGDOM

*Gordon Anthony**

I. Is there a national act containing a legal definition of Automated Administrative Decisions?

There is not – as yet – any national Act in the UK¹ that contains a legal definition of automated administrative decisions. While the need for legislation has been acknowledged – draft legislation was introduced into the UK Parliament in Spring 2025 but has not been enacted – the approach to automated decision-making so far has tended to focus upon soft law means of regulation and the use of guiding principles rather than formal rules. Working definitions have been found in that context. For instance, a government White Paper published in 2023 defined AI with reference to “2 characteristics ... the ‘adaptivity’ of AI [which] can make it difficult to explain the intent or logic of the system’s outcomes” and “the ‘autonomy’ of AI [which] can make it difficult to assign responsibility for outcomes”². While the White Paper acknowledged that there are different ways of defining AI, it said that defining “AI with reference to these functional capabilities and designing our approach to address the challenges created by these characteristics [would] future-proof our framework against unanticipated new technologies that are autonomous and adaptive ... We will, however, retain the ability to adapt our approach to defining AI if necessary, alongside the ongoing monitoring and iteration of the wider regulatory framework” (see paragraphs 39-41). That framework – which is intended to be “pro-innovation” – centres upon 5 principles of: (i) safety, security and robustness; (ii) appropriate transparency and explainability; (iii) fairness; (iv) accountability and governance; and (v) contestability and

* Professor of Public Law, Queen’s University, Belfast; Barrister-at-Law.

¹ The reference to the UK is made for ease of reference and also because the same general principles of law tend to apply in England, Wales, Northern Ireland, and Scotland. An analysis of the law in those jurisdictions can be found in, respectively, H. Woolf *et al.*, *De Smith’s Judicial Review* (2020), G. Anthony, *Judicial Review in Northern Ireland* (2024); and *The Laws of Scotland: Stairs Memorial Encyclopaedia* (2000).

² Available at <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#section321>.

redress (these are further analysed under “IV” below). Initial Guidance on the principles was published in February 2024³.

It remains to be seen whether any legislation that might be introduced in the UK Parliament will incorporate the above definition or whether it might draw upon one that has been used elsewhere. For instance, an earlier Private Members Bill in the UK Parliament defined AI as: “*technology enabling the programming or training of a device or software to (a) perceive environments through the use of data; (b) interpret data using automated processing designed to approximate cognitive abilities; and (c) make recommendations, predictions or decisions; with a view to achieving a specific objective*” (AI was for these purposes said to include “*generative AI, meaning deep or large language models able to generate text and other content based on the data on which they were trained*”)⁴. This definition apparently focused upon AI primarily in terms of generated outcomes, whereas other definitions, such as that in Article 3(1) of the EU’s AI Act, include an express mention of autonomy. Article 3 thus defines an AI system as “*... a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*”. Either, or a mix of both, of these definitions may well influence any future definition in UK statute law.

II. Is there a general legal basis (either at the constitutional level or in the Administrative Procedure Act) for the use of algorithmic automation and/or artificial intelligence (AI) by public authorities (government, agencies, local authorities, and specialised bodies)? If no such legal basis exists, are there any legislative provisions that permit public authorities to experiment with algorithmic automation or AI?

There is no specific legal basis that positively authorises the use of AI – the use of resources is a normal function of expenditure by public bodies when exercising powers, taking decisions, and so on. The use of AI is, however, subject to (what might be termed) negative authorisation, which takes three forms. The first is through the application of “*hard law*” rules that are enforced by the courts and are found in, for instance, the Human Rights Act 1998 and the Data Protection Act 2018 (as read with UK GDPR). Local authorities (to take that example) are public authorities

³ Available at https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d0013c821a0-/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf.

⁴ Available at <https://bills.parliament.uk/publications/53068/documents/4030>.

within the meaning of section 6 of the Human Rights Act 1998, and they must act compatibly with rights under the ECHR in all that they do, including the use of AI. The Data Protection Act 2018 would also impose constraints on public bodies (and on private actors): information either absorbed within and/or generated by AI would be required to be processed in accordance with the data protection principles contained in sections 34 – 42 of the 2018 Act. Those principles are largely at one with the principles of the EU’s GDPR⁵.

The second form is common law principles that have been developed by the courts and which include fairness, rationality, and legality. Many of the principles are synonymous with administrative law and the workings of judicial review, and they have been developed by the courts over the past 50 years, in particular⁶. They potentially apply when any public law decision is taken by a public body, including through the use of AI. The point is illustrated in the context of the problem scenarios that have been prepared for this special issue of the journal.

The third form is “*soft law*” and, in particular, the five regulatory principles that were noted under question number 1 above. These are principles that guide regulators as they seek to monitor the use and development of AI across public and private sectors, where regulatory approaches will have implications for the manner and extent to which public decision-makers include AI within their decision-making processes. The content and significance of those principles – where there is a degree of overlap with common law principles – are also returned to below (see heading IV).

III. Do public authorities rely on algorithmic automation/AI in their daily operations? If yes, to what extent? Which areas are most affected by automation (e.g., security, policing, immigration, transport, tax management, welfare, health and employment services, education, justice, or digital identity)?

The answer to this question – or certainly the first part of it – can be answered in the affirmative. Public authorities in the UK, as elsewhere, now make use of AI and, moreover, do so on a regular and

⁵ See also the Data Use and Access Act 2025.

⁶ See H. Woolf *et al.*, *De Smith’s Judicial Review*, cit. at 1; G. Anthony, *Judicial Review in Northern Ireland*, cit. at 1; and *The Laws of Scotland: Stairs Memorial Encyclopaedia*, cit. at 1.

increasing basis⁷. Doing so is routinely regarded as a means to maximise efficiency in public decision-making, albeit AI is (of course) also regarded as challenging what might be termed traditional public law values⁸. An insight into that tension can be seen in some of the factual scenarios addressed in this special issue.

More difficult to answer is the question of which areas are the most affected by automation, as that would require an audit of all areas of public service and access to data sets. However, a compromise answer can be found in the government White Paper noted above. The paper makes it clear that AI is now permeating all areas of decision-making; indeed, it is written on the assumption that it will come to suffuse many areas of public and private decision-making. That is why the approach in the UK to date has been centred upon adaptability and flexibility – the ability to respond to AI on an iterative basis is seen as imperative to the current and future regulatory approach (and, as above, it may inform any legislative intervention in the area).

IV. What legal requirements – e.g. in terms of privacy, cybersecurity, quality of the datasets, impact assessments, transparency obligations, access to codes, the right to explanations, compulsory human involvement, and the right to obtain a review or remedy – apply to the use of algorithmic automation or AI by public authorities? Are there sector-specific regulations on Automated Administrative Decisions (e.g., public procurement, taxation etc.)?

It has been noted above that legal requirements take form at three main levels in the UK: “*hard law*” rules found in legislation (as applied by the courts); common law principles; and “*soft law*” regulatory principles identified by the government. Little need be said about the hard law rules as apply under the Human Rights Act 1998 and the Data Protection Act 2018. While these are domestic Acts of Parliament and have been interpreted by the courts on that basis – Brexit has also weakened the link between the Data Protection Act 2018 and EU law⁹ – much of the law here will be similar to that which applies elsewhere in Europe. The right to privacy is an example: it applies under both pieces

⁷ See, e.g., *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058 (on the use of automated facial recognition technology: use of the technology found to be in breach of, *inter alia*, privacy rights).

⁸ See, e.g., P. Craig, *Administrative Law* (2025), especially Chapter 10.

⁹ Though see also section 106(3) of the Data Use and Access Act 2025.

of legislation and is applied in the light of the rulings of the European Court of Human Rights in particular¹⁰.

The common law principles that potentially apply to the use of AI are sometimes said to be three-fold and can be summarized as follows (these apply most immediately in judicial review proceedings but also take form in administrative law more broadly):

i. **Illegality.** At its most simple, this principle means that a public decision-maker will act unlawfully if it does not “*understand correctly the law that regulates [its] decision-making power and ... give effect to it*”¹¹. The application of this principle can become multi-faceted in practice, but the main point to be made here is that it gives effect to the hard law rules contained in, among other pieces of legislation, the Human Rights Act 1998 and the Data Protection Act 2018. It would also give effect to any legislation that might be enacted specifically in relation to AI.

ii. **Procedural fairness.** This principle requires decision-makers to give effect to the rules of fairness, which may either be found in statute law (the principle thus overlaps here with illegality, above) and/or the common law. The common law rules are famously divided into the right to a fair hearing and the rule against bias, where the manner in which they apply always depends upon context. It should, however, be noted that the rules potentially apply whenever “(anyone) decides anything”¹² – and that “anyone”, for these purposes, might be said to include an automated decision-maker.

iii. **Wednesbury unreasonableness.** This principle – which overlaps with, and can be displaced by, the proportionality principle in human rights cases – renders decisions unlawful where the decisions are “*so unreasonable that no reasonable decision-maker*” could have taken them¹³. The principle is ultimately concerned with controlling the exercise of discretion by administrative decision-makers, and it has, in that way, historically focused on decisions taken by humans. This is

¹⁰ Human Rights Act 1998, s. 2.

¹¹ *Council of Civil Service Unions v Minister for the Civil Service* [1985] AC 374, 408, Lord Diplock.

¹² *Board of Education v Rice* [1911] AC 179, 182, Lord Loreburn.

¹³ *Associated Provincial Picture Houses v Wednesbury Corporation* [1948] 1 KB 223, 233. On the relationship between *Wednesbury* and proportionality see G. Anthony, *Judicial Review in Northern Ireland*, cit. at 1, especially Chapter 6.

plainly where AI can present some of its greatest challenges: while exercises of discretion can perhaps easily be assessed when they are based upon human reasoning, the qualities of unreasonableness (or proportionality) assume a different dimension in the context of automated decision-making.

The regulatory principles identified by the government fall under the five headings that have been noted under question 2.1 above, and they are perhaps most relevant to the sub-question about sector-specific regulation. In its Initial Guidance on how the principles ought to operate, the government emphasised that they are about promoting transparency around the use of AI and that, while different principles may have more obvious relevance in certain regulatory remits, all are potentially relevant in a particular sector and should be considered as such. The government said the following about the principles¹⁴:

i. Safety, security and robustness. This principle is intended to help regulators “*Understand and communicate the level of safety related risk in their regulatory remit*” and also to “*Stress the importance of AI developers and deployers (within regulators’ remits) undertaking safety risk assessments and implementing appropriate mitigations to identified risks*”. The principle should also prompt consideration of “*how AI developers and deployers should mitigate and build resilience to cybersecurity related risks throughout the AI life cycle*”.

ii. Appropriate transparency and explainability. This principle is intended to foster trust in AI and its use, and it ought to “*Encourage AI developers and deployers to implement appropriate transparency and explainability measures*”. The principle is also to be understood as foundational to the other principles; indeed, it is said to be “*necessary for the proper implementation of the other four principles*”.

iii. Fairness. According to this principle, there is a need to “*develop, publish descriptions or signpost to existing descriptions of fairness that apply to AI systems’ outcomes within their regulatory remit*” and also to “*Consider how AI systems that are used in their regulatory remit are designed, developed, deployed and used considering this description of fairness*”. The government has moreover said that it is important to align “*descriptions*

¹⁴ All quotes below at https://assets.publishing.service.gov.uk/media/65c0b6bd63a23d-0013c821a0/implementing_the_uk_ai_regulatory_principles_guidance_for_regulators.pdf.

of fairness and [that] developing joint tools and guidance is particularly important in cross-cutting regulatory remits”.

iv. Accountability and governance. This principle seeks to *“Place clear expectations for compliance and good practice on appropriate actors in the AI supply chain (within regulators’ remits), including expectations for what appropriate internal accountability and governance frameworks might look like”*. It also requires that regulators, *“Consider whether existing powers that place accountability on decision makers are applicable in the context of AI and to AI developers and AI deployers”*. Lastly, the principle seeks *“to foster accountability through promoting appropriate transparency and explainability”*.

v. Contestability and redress. This final principle seeks, where appropriate, to *“encourage AI developers and AI deployers (within regulators’ remits) to provide clarity to users on”* how they may challenge AI outcomes or decisions. Moreover, it highlights *“that appropriate transparency and explainability is key to ensuring that AI deployers or end users can contest outcomes and are aware of routes to redress”*.

It is apparent from this summary of the government’s principles that they overlap in part with some of the logic and content of the common law principles that apply in judicial review (and administrative law more broadly). For instance, the government’s emphasis on accountability is consistent with much of the underlying rationale for judicial review of public authority decisions; and the principle of contestability and redress is evocative of internal review rights/and or rights of recourse to tribunals and courts. There would also appear to be some commonality at the level of fairness, albeit the government’s principle of fairness appears to be more substantive in nature than procedural. If that is so, any overlap would perhaps arise with *Wednesbury* unreasonableness rather than procedural fairness – the idea of procedural fairness might, in turn, complement the principle of accountability and the need *“to foster accountability through promoting appropriate transparency and explainability”*.

V. Who builds the algorithmic technologies used by public authorities? Are these developed by public entities, private companies, or a hybrid body?

There is no simple answer to this question, and, again, it would require an audit to understand who develops the AI systems used by the

public administration. Anecdotally, it can be said that the development of AI models is led by private companies, whose products will be used by public authorities as part of their ordinary work, subject to such use being compatible with the authorities' legal powers and duties. Indeed, while the government has sought to develop a strategy in relation to the development of AI, this has tended to be at the level of guiding and overseeing such developments rather than at a level of directing and controlling them. It is thus here that the government's five principles might be expected to have their maximum effects: if followed, they ought to act as *ex ante* considerations that will inform the development and release of AI technologies.

VI. Is there a centralised infrastructure for digital data management, or are there several infrastructures? If the latter is true, is interoperability guaranteed, and to what extent? Are there any rules or procedures governing the exchange of information between different administrative bodies?

The UK has a National Data Strategy, which seeks to maximise efficiencies in the public and private sectors by sharing data across a number of trusted sources¹⁵. The strategy rests upon four "pillars" – data foundations, data skills, data availability, and responsible data – and pursues five "missions", which include (as the third mission) "*transforming government's use of data to drive efficiency and improve public services*". The strategy here states:

"The coronavirus pandemic showed that there is massive untapped potential in the way government and public services use and share data to help and protect people. To sustain the high watermark set by the pandemic, the government will undertake an ambitious and radical transformation of its own approach, driving major improvements in the way information is efficiently managed, used and shared across government. To succeed, we need a whole-government approach that ensures alignment around the best practice and standards needed to drive value and insights from data; and the creation of an appropriately safeguarded, joined-up and interoperable data infrastructure to support this. We also need the right skills and leadership within the public sector to understand and unlock the potential of data".

¹⁵ All quotes in this section found at <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>.

The other missions make it clear that the move towards the use of centralised and/or shared data is an iterative process. For instance, the first two missions relate to *“unlocking the value of data across the economy”* and *“securing a pro-growth and trusted data regime”*, whereas missions four and five are titled *“ensuring the security and resilience of the infrastructure on which data relies”* and *“championing the international flow of data”*. Mission four would appear to be the one most immediately related to rules and procedures for the exchange of information. It reads:

“The use of data is now a central part of modern life, so we need to make sure that the infrastructure underpinning it is safe and secure. The infrastructure on which data relies is a vital national asset that needs to be protected from security risks and other concerns, such as service disruption. Interruption to data-driven services and activities can cause disruption to businesses, organisations and public services. While these are also commercial risks to manage, the government has a responsibility to ensure that data and its supporting infrastructure is resilient in the face of established, new and emerging risks, protecting the economy as it grows”.