



Eagle International Journal of Science, Technology and Innovation

An International Peer Reviewed, Open-Access and Multidisciplinary Journal

Volume 1 | Issue 1 | August 2026 |

Website: <https://ejrihs.com/index.php/eijsti/index>

**WHEN THE ALGORITHM DECIDES: ARTIFICIAL INTELLIGENCE,
DIFFUSED LIABILITY, AND THE EMERGING ACCOUNTABILITY GAP IN
AUTOMATED DECISION-MAKING**

Majebi Samuel Amune, Ph.D

LL.B. (University of Benin); LL.M., M.Phil., Ph.D (Obafemi Awolowo University)

Senior Lecturer, College of Law, Joseph Ayo Babalola University, Ilesa, Osun State,
Nigeria & Principal Partner, LawDigital Consult.

Email: nobleheirs@yahoo.com

ABSTRACT

Decisions that once turned on human judgement are now routinely produced by artificial intelligence: who receives credit, who is flagged to the police, whose application survives the first cut of a recruitment process. Legal liability, however, was built around a different picture of the world, one in which an identifiable actor commits a fault that can be traced to a harm. Against the distributed and frequently anonymous reality of how algorithmic systems are designed and deployed, that architecture strains badly. This article examines the lacuna that opens as a result, where harm has plainly occurred and a system is plainly implicated, yet no single actor can be made to answer under existing rules of tort, contract or data protection law. Taking the problem of many hands as its analytical frame, the article traces how responsibility for an automated decision fragments across data suppliers, model developers, fine-tuners and deployers, and how that fragmentation defeats the causal reasoning on which fault-based liability rests. It then surveys the comparative responses, among them Article 22 of the EU General Data Protection Regulation, the Court of Justice's ruling in *Schufa*, the EU Artificial Intelligence Act and the English case law on automated policing, before turning to Nigeria's fragmented position under the Nigeria Data Protection Act 2023 and orthodox tort principles. Nigeria, having no statute directed at algorithmic harm, is acutely exposed. The article proposes a layered legislative response built on mandatory algorithmic traceability, an operator-centred presumption of liability, and a compensation mechanism for residual harm, and concludes that closing the gap calls for deliberate legislative recalibration rather than further stretching of inherited common law doctrine.

Keywords: Artificial Intelligence; Automated Decision-Making; Accountability Gap; Data Protection Law; Diffused Liability.

1. Introduction

A commercial bank in Akoka declines a loan application in a matter of seconds. A recruitment platform quietly removes a candidate from a shortlist before any human recruiter has opened the file. In both instances a decision carrying real consequences for a real person has been generated, wholly or in part, by a system trained on historical data and calibrated by engineers who will never meet the person on the receiving end. The question this article puts is simple to state and considerably harder to answer: when a decision of that kind causes harm, who answers for it, and who bears the liability?

The answer the law has traditionally given presupposes a single identifiable actor whose conduct can be measured against a standard of care and connected causally to the injury complained of. Automated decision-making unsettles that presupposition at every stage. Such a system is conceived by one set of engineers, trained on data assembled by another, fine-tuned towards a particular purpose by a third, and finally deployed by an operator who may understand very little about how outputs are actually reached. When harm follows, it is commonly the product of the chain in its entirety rather than of any identifiable link within it.

The argument advanced here is that Nigerian law is not yet equipped to say who answers for the algorithm, and that Nigerian legislation lacks the specificity needed to address wrongs of this character. Part 2 explains automated decision-making and the opacity characteristic of it. Part 3 develops the account of diffused liability through the problem of many hands. Part 4 surveys the comparative responses; Part 5 turns to Nigeria's fragmented position. Part 6 sets out a proposed legislative response, and Part 7 concludes.

2. Automated Decision-Making and the "Black Box" Problem

Automated decision-making, or ADM, refers to any process in which an outcome affecting a person is generated wholly or substantially by a computational system rather than by unaided human judgement. It exists along a spectrum. At one end sit systems that merely offer a human decision-maker a recommendation which can be rejected; at the other, systems that settle the outcome with no meaningful human involvement at all. The hardest

cases for legal responsibility cluster around the point where oversight has become formal rather than genuine, where a human signs off on what the machine has already determined.

Much of the difficulty flows from the opacity of the underlying systems, a phenomenon generally labelled the black box problem. A complex machine-learning system can be interrogated after the event, though usually only by a narrow class of specialists, within a limited window, and with no assurance that the behaviour in question was foreseeable in advance by anyone who designed, trained or deployed it. Cooper and colleagues, writing on accountability in algorithmic society, make the further and more uncomfortable point that transparency does not convert neatly into culpability: a system may be technically explainable and still frustrate every attempt to trace a harmful output back to a particular human failure. That opacity is often a by-product of how these systems come into being, assembled as they typically are from openly available toolkits repurposed for high-stakes applications their original developers never contemplated.

3. Diffused Liability: The "Problem of Many Hands" in the AI Pipeline

The phrase "the problem of many hands" originated well outside artificial intelligence, in Dennis Thompson's analysis of moral responsibility within public bureaucracies. Where a harmful outcome is the work of many hands, Thompson observed, it may be genuinely unclear who is to blame, because the causal antecedents lying closest to the harm have become detached from the place where decisions were actually taken. Helen Nissenbaum subsequently carried the insight into computerised systems, treating it as one among several structural barriers to accountability, standing alongside the difficulty of tracing a bug to its source and the ever-present temptation to blame the computer.

The common law of negligence was constructed to resolve precisely this difficulty in the context of physical products, and it did so by fixing responsibility on the manufacturer who puts a defective item into the stream of commerce. *Donoghue v Stevenson* established that a manufacturer owes a duty of care to the ultimate consumer, actionable notwithstanding the absence of any contract between them. Nigerian courts have applied the principle without hesitation. In *Nigerian Bottling Co Ltd v Ngonadi* the Supreme Court held the manufacturer of a defective refrigerator liable for injuries caused when it exploded, and in

Okwejiminor v Gbakeji it reaffirmed the duty against the manufacturer of a contaminated bottled drink, while exonerating the retailer who had done no more than sell the product in the condition it was received.

What makes that doctrine workable is exactly what an AI pipeline ordinarily lacks: a single identifiable manufacturer in control of the finished product before it reaches the consumer. An automated decision-making system passes through several independent pairs of hands. Data is collected and labelled by one group of actors. A base model is trained by another, frequently in a different jurisdiction. A third fine-tunes it. An operator who built none of it then deploys the result and either monitors it or does not. When harm follows, the question is no longer the one *Ngonadi* and *Okwejiminor* answered, namely whether the manufacturer took reasonable care, but the prior and much harder question of which among several actors, none possessing complete visibility of the whole, ought to be treated as the manufacturer in the first place. Causation grows correspondingly elusive, because a harmful output may emerge from the interaction of several design choices each of which was, taken alone, entirely reasonable.

4. Comparative Regulatory Responses to the Accountability Gap

The European Union has moved furthest in closing the accountability gap, and has done so through positive legislation rather than incremental common law development. Article 22 of the General Data Protection Regulation confers a right not to be subject to a decision based solely on automated processing, profiling included, where that decision produces legal effects or similarly significantly affects the person concerned. The exceptions are narrow, confined to contractual necessity, statutory authorisation and explicit consent, and even where one applies the controller must put safeguards in place: human intervention at a minimum, together with the right to express a view and to contest the outcome.

The Court of Justice has read Article 22 expansively, and in a way directly responsive to the diffusion described in Part 3. In *OQ v Land Hessen (Schufa Holding (Scoring))* the Court held that a credit reference agency which does no more than generate a probability score, neither granting nor refusing credit itself, is nonetheless engaged in automated decision-making where the lender leans heavily on that score. The effect of the ruling is to

pin responsibility on the actor holding the greatest informational control, instead of allowing it to evaporate into the space between the scorer and the nominal decision-maker. The Artificial Intelligence Act, in force since August 2024, builds this into a general risk-tiered regime. Crucially, it declines to treat developer and user as interchangeable, separating the provider who places a system on the market from the deployer who puts it into service and attaching distinct, non-delegable obligations to each.

England and Wales arrived at a comparable diagnosis by a narrower route. In *R (Bridges) v Chief Constable of South Wales Police* the Court of Appeal held the use of live automated facial recognition by a police force unlawful, in part because no adequate legal framework governed who could be placed on a watchlist, where the technology could be deployed, or how its use might be reviewed. To treat the absence of a framework as itself unlawful is to characterise the gap as a structural defect rather than merely a shortfall in after-the-fact redress. Wisconsin took a more permissive line in *State v Loomis*, holding that reliance on a proprietary recidivism-risk algorithm at sentencing did not offend due process so long as the score was not determinative and remained open to challenge. Yet a defendant invited to contest a score he cannot interrogate, the methodology being a protected trade secret, holds a right that is formally available and substantively hollow.

5. Nigeria's Fragmented Legal Landscape

Nigeria has enacted no statute addressed specifically to artificial intelligence or to algorithmic harm. The nearest analogue to Article 22 is the Nigeria Data Protection Act 2023, which establishes the Nigeria Data Protection Commission and, for the first time in Nigerian statute law, imposes obligations directed at automated processing. Section 27(1)(g) requires a data controller, before collecting personal data directly from a subject, to disclose the existence of automated decision-making together with its significance and consequences, and to inform the subject of the right to object. Section 37 goes further, granting a right not to be subject to a decision based solely on automated processing, profiling included, where that decision carries legal or similarly significant effects.

These are real advances, and they close only a narrow portion of the gap. Both provisions bite only where personal data is in play, which leaves harms produced by systems operating

on non-personal or aggregated data entirely outside their reach. Nor is it clear whether an upstream model developer who never controls personal data at all, but whose design choices shape the eventual decision, falls within section 37 in any meaningful sense. What Nigeria has done, in substance, is import the vocabulary of automated decision-making without confronting the diffusion problem that vocabulary was developed in Europe to address.

Beyond data protection, a claimant is thrown back on the ordinary law of tort discussed in Part 3. That body of doctrine assumes an identifiable manufacturer capable of being measured against a single standard of care, and it has little to say where the wrong resides in the emergent interaction of several actors' individually defensible choices. Nigeria has nothing corresponding to the AI Act's provider–deployer distinction, and no pre-deployment certification regime of the kind whose absence proved fatal in *Bridges*. NITDA's guidance on artificial intelligence remains aspirational in character. The upshot is that a Nigerian whose loan application is declined by an opaque automated system may discover that no existing rule was drafted with that harm in contemplation.

6. Towards Closing the Accountability Gap

Closing the gap does not require Nigeria to discard the tort doctrine it has received. It does require legislation capable of adapting that doctrine to a pipeline occupied by many actors. Three measures, each drawn from the comparative material canvassed above, are proposed here.

The first is traceability. Any statute addressed to high-impact automated decision-making should impose a mandatory obligation on providers and deployers to maintain auditable logs of the data, the model version and the configuration underlying a given decision. Without a record of that kind, causation, which is the element the many-hands problem most directly threatens, is effectively unprovable by the time a dispute reaches a courtroom.

The second is an operator-centred presumption of liability, modelled loosely on the deployer obligations of the AI Act and on the reasoning in *Schufa*. The entity that deploys a system into a social context should carry a rebuttable presumption of liability, coupled

with a right of contribution against upstream developers whose components it can demonstrate were defective. The alternative, which is the present position, requires a claimant to identify precisely which actor was at fault, a burden the structure of the pipeline makes close to impossible to discharge. This reform should be paired with generalising the right in section 37 of the Nigeria Data Protection Act 2023 beyond personal-data processing, so that it reaches any automated decision producing legal or similarly significant effects, and with a right to human review that is meaningful rather than merely formal, *Loomis* having shown how easily such a right becomes illusory.

The third addresses the residual cases in which harm is demonstrable but no individual actor's fault can be proven, which is precisely the category the many-hands problem predicts will keep recurring. For those cases, a compensation mechanism funded by mandatory contributions from providers and deployers of high-risk systems, calibrated to risk tier, would ensure that victims are not left remediless simply because a responsibility that genuinely exists cannot be attributed to a single hand.

7. Conclusion

The accountability gap examined in this article is not a passing inconvenience that sharper litigation technique will eventually dissolve. It is a structural consequence of assembling decision-making systems out of components contributed by many hands, no one of which is, on its own, causally or morally sufficient to explain the harm that results. The common law of negligence, however capably it has handled defective refrigerators and contaminated soft drinks, was never built to answer a question of that shape, and section 37 of the Nigeria Data Protection Act 2023, welcome though it is as a first step, answers only a fraction of it. Comparative experience points consistently in one direction. *Schufa* fixes responsibility on the actor with the greatest informational control; *Bridges* insists that an adequate legal framework must exist before deployment and not merely afterwards. Both suggest that closing the gap is work for the legislature rather than for the slow accretion of judicial precedent. Nigeria's Data Protection Commission and National Assembly should legislate for the pipeline as it actually operates, and should do so while the many hands responsible for a harm can still be told apart.

Bibliography

Cases

1. *Donoghue v Stevenson* [1932] AC 562 (HL)
2. *Nigerian Bottling Co Ltd v Ngonadi* [1985] 1 NWLR (Pt 4) 739 (SC)
3. *Okwejiminor v Gbakeji* [2008] 5 NWLR (Pt 1079) 172 (SC)

4. *OQ v Land Hessen (Schufa Holding (Scoring))* Case C-634/21 EU:C:2023:957 (7 December 2023)
5. *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058
6. *State v Loomis* 881 NW2d 749 (Wis 2016)

Legislation

10. Nigeria Data Protection Act 2023
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation) [2016] OJ L119/1
12. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L1689

Books, Journal Articles and Conference Papers

13. Cooper, A Feder and others, 'Accountability in an Algorithmic Society: Relationality, Responsibility, and Robustness in Machine Learning' (2022) Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency 864
14. Nissenbaum, Helen, 'Accountability in a Computerized Society' (1996) 2 Science and Engineering Ethics 25
15. Thompson, Dennis F, 'Moral Responsibility of Public Officials: The Problem of Many Hands' (1980) 74 American Political Science Review 905