

Opening the Black Box or Responding to Demands? Rethinking and Reconstructing the European Standard of Algorithmic Explanation

feng zhi

lexcausae@163.com

XXXXXXXXXX

Article

Keywords: Algorithmic explanation, Risk governance, Algorithmic trust, Explanation standard

Posted Date: October 12th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11093106/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

The European Union's current standard of algorithmic explanation emphasises the disclosure of a model's internal decision logic and related information. This normative premise was plausible in an era of code-based automated decision-making, but when confronted with complex algorithmic models such as neural networks, even where existing techniques can offer a degree of explanation, their fidelity and implementation costs make it difficult to satisfy the requirements of the current standard. Against this backdrop, the mitigation approach to the explanation standard, which focuses on particular audiences and scenarios in order to reduce the amount of explanatory information required in different contexts, fails to resolve the underlying technical limitation because the technical logic by which explanatory information is obtained remains unchanged. By contrast, the substitution approach, while recognising these technical limitations and seeking to replace the existing explanation standard and regime with technical trustworthiness, algorithmic controllability, and other institutions or content, yields solutions of limited practical scope because it does not fully identify and generalise explanation demands. Building on these limitations, this article advances a demand-oriented analytical framework. It proposes that the temporal nodes at which developers, deployers, and other actors retain control over a model should provide the basis for identifying and generalising the demands of algorithmic explanation, thereby fixing the categories of such demands. Having identified these categories of explanation demands, this article focuses on the realisation of these demands and reconstructs the current European standard of algorithmic explanation through equivalent and feasible substitute schemes.

Introduction

In the governance of algorithms, Articles 13, 15 and 22 of the European Union's General Data Protection Regulation (GDPR), together with Recital 71 thereof, are widely regarded as provisions on algorithmic explanation (Bryce Goodman and Seth Flaxman 2017). Beyond the United Kingdom, which has left the EU, non-EU countries such as China and Brazil have also largely taken these provisions as a reference, enacting corresponding rules on the right to object to automated decision-making and on explanatory disclosure (e.g., China, 2021-Personal Information Protection Law, art. 24(3); Brazil, 2018-Lei Geral de Proteção de Dados [LGPD], art. 20). Nevertheless, although the regime of algorithmic explanation has been adopted by many countries, its institutional practice is far from satisfactory, and the resistance of some market actors to algorithmic explanation is fairly pronounced. For instance, in the SCHUFA credit-scoring case, the scoring agency restricted the disclosure of scoring factors and their weights on the ground of trade secrets (OQ v. Land Hessen); in the case concerning the deactivation of Uber drivers' accounts, the platform invoked human review as a defence against algorithmic explanation (App Drivers & Couriers Union v. Uber B.V.). At the commercial level, it can likewise be confirmed that, although disclosures such as "Why am I seeing this ad" and System Cards disclose the decision logic, operating mechanisms and other information of algorithms, such disclosures are mostly standardised compliance templates, with the explanatory content of different platforms being highly convergent and of low relevance to existing problems such as algorithmic bias and information cocoons.

Analysing the causes of this phenomenon, this article holds that it results principally from the disjunction between the earlier explanation standard and existing algorithmic technology. The EU's regime of algorithmic explanation was set out in Articles 12 and 15 of the 1995 Data Protection Directive, whose regulatory object at the time of its enactment was primarily computer automation based on database encoding. At that time, although automated decision-making fields such as credit scoring had already exhibited black-box features, the traceability of decision logic remained an objective fact, so that the legislature's requirement of disclosing decision logic was technically feasible. Today, however, algorithmic technology has undergone wholesale iteration: mainstream algorithms such as neural networks follow the logic of high-dimensional non-linear mapping and distributed representation, and the impossibility of fully opening the algorithmic black box has become a technical consensus. The application of the earlier explanation standard has thereby upset the original equilibrium between technology, cost and the explanation standard, instinctively prompting platforms and other explaining parties to engage in legal evasion.

In light of the mismatch between the existing explanation standard and current algorithmic technologies, this article develops a demand-oriented theory of algorithmic explanation to improve the EU standard. Part 1 examines existing proposals for improving the standard and identifies their limitations. Building on that analysis, Part 2 sets out the demand-oriented theory and explains its advantages. Part 3 proposes a temporal-node criterion that distinguishes stages by reference to control over the model. This criterion identifies and generalises the demands for algorithmic explanation at the normative level, while leaving room for appropriate explanatory techniques to meet those demands. Part 4 completes the reconstruction of the explanation standard on the basis of the demands identified, so as to overcome the existing technical limitations and restore the practical effect of algorithmic explanation to its legislative intent.

1. The Limitations of Existing Improvement Schemes

Scholars in various countries have also examined the technical and cost limitations of the current EU explanation standard, and studies have proposed a range of improvements. Drawing on the mainstream literature, this article broadly classifies the existing improvement schemes into two categories according to whether they replace the original explanatory content and regime: the mitigation approach to the explanation standard, and the substitution approach to the explanation standard.

1.1. The limitations of the mitigation approach

Despite these technical limitations, the mitigation approach does not abandon the current EU explanation standard; rather, while retaining an explanation of the model itself, it further refines the current EU standard according to the relevant audiences and scenarios, thereby seeking, through the provision of differentiated explanatory information, to reduce the volume of explanatory information required in different audience and scenario contexts and to ease the technical burden of providing it. According to the audience or context of explanation, the existing mitigation approach can be divided into

three types. The first, guided by actual explanatory effect, constructs different explanation standards for different audiences (Zhihang Yang 2024). The second focuses on different algorithmic application scenarios and proposes different explanation standards (Yu Su 2024; Xinxin He 2023). The third focuses on sociological interactivity and emphasises the interactive realisation of algorithmic explanation (Tim Miller 2019). Moreover, since audience and scenario belong to different dimensions of differentiation, a few studies combine several differentiating criteria such as scenario, audience and mode of interaction, thereby further refining the explanation standard (Pierre Dewitte 2025).

In practice, the mitigation approach—setting the content of explanation through scenarios, audiences and interactive explanation—does provide differentiated explanatory information: in ordinary scenarios only a general account of the decision logic is required, whereas in special scenarios more persuasive case-specific reasons must be provided. However, this differentiated supply does not change the technical process by which explanatory information is generated. Whether it is the account of general decision logic in ordinary scenarios or the in-depth interpretation of specific decisions in special scenarios, the methods used still require the algorithmic black box to be penetrated, and the techniques involved do not change with the difference in information demands. In fact, varying the depth of disclosure merely filters information according to scenarios and audiences; it may be more effective than the EU standard, but its improvement in terms of technical pressure and cost burden remains more an institutional aspiration than a technical reality.

As for how the mitigation approach presents information, the filtering of information and the organisation of content depend on the explaining party. Given the extreme complexity of algorithms, which information to disclose and which to withhold is entirely controlled by the explaining party, which essentially constitutes an exercise of informational power (Hao Wang 2022). In interactive explanation in particular, the explaining party must also guide and respond to the audience's questions; leaving aside whether the audience possesses the professional knowledge and cognitive capacity to pose effective questions, the interaction itself creates a problem of information asymmetry. In interactive explanation, the explaining party has the capacity to adjust and guide the audience's questions, and through successive content guidance it will in fact also frame the cognitive boundaries of the audience, concentrating their attention on a local path preset by the explaining party while neglecting other potential causal chains in the model's decision. Therefore, on the basis of the existing technical and cost limitations of algorithmic explanation, the mitigation approach cannot be expected to ensure that the explaining party presents information accurately.

1.2. The substitution approach to the explanation standard

Unlike the mitigation approach, the substitution approach takes fuller account of the technical limits of the current EU standard; it therefore does not attempt to improve upon the current EU standard, but instead proposes to substitute standards such as technical trustworthiness, procedural fairness and contestability of outcomes for the current EU standard. Depending on the scope of substitution, the existing substitution approach can be further divided into the content-substitution approach and the regime-substitution approach. The content-substitution approach retains the existing regime of

algorithmic explanation, but advocates shifting the focus of explanation from decision logic, determining features and operating mechanisms to decision rules and technical trustworthiness (Chunye Wang 2024; Sandra Wachter and Brent Mittelstadt 2019). By contrast, the regime-substitution approach holds that algorithmic explanation cannot be achieved under existing technical conditions, so that contestability of outcomes and algorithmic controllability should replace the regime of algorithmic explanation (Reuben Binns 2018; Zeng Yuan 2025; Kaminski et al. 2021).

Regarding the content-substitution approach, although it resolves the technical limitation of algorithmic explanation, it is essentially a concession of law to technology, and it correspondingly produces a problem of diminished effect in governance. On the one hand, at the technical level, compliance in the training and operation of an algorithm does not imply that its outcomes are compliant. Algorithms have the capacity for autonomous evolution: even if an algorithmic model performs well before deployment, changes in data distribution or interference by adversarial samples after deployment may cause it to produce decisions that deviate from the preset rules. Moreover, the decision logic of most algorithms, such as reinforcement learning, is itself dynamic and cannot provide fixed *ex ante* rules for review. Furthermore, when elements such as technical trustworthiness and qualification trustworthiness are treated as making outcomes acceptable, this also weakens the incentive of developers and deployers to monitor and correct the model, and may even aggravate the phenomenon of formal compliance. On the other hand, in terms of accountability, the designer's qualifications and the technical architecture point only to the trustworthiness of the algorithmic system itself, whereas algorithmic accountability seeks the causal chain concerning a particular decision; treating qualification and technical trustworthiness as the basis for the legitimacy of a decision is, in essence, a logical category error.

Regarding the regime-substitution approach, although it builds on the content-substitution approach and resolves the logical category error at the level of accountability, it is still subject to limitations. First, contestability of outcomes is *ex post* and passive, dependent on an algorithmic decision having been made. With algorithms widely deployed across various fields, *ex post* remedial mechanisms cannot resolve the irreversibility of the outcomes produced by some decisions. Second, contestability of outcomes, as a case-specific remedial avenue, is discrete in nature and can scarcely address systemic problems in the algorithmic system. Contestability of outcomes is premised on case-specific decisions, and the correction of an individual outcome does not necessarily bring about the correction of the algorithmic system; in particular, where the impact of an individual case is limited, groups such as the low-income and ethnic minorities find it difficult to shake the injustice of the algorithmic system itself. Third, contestability of outcomes faces the problem of response costs. Case-specific contestation requires case-specific response, and such responses, whether manual or algorithmic, entail substantial costs against the backdrop of the extremely broad scope of algorithmic application. Furthermore, beyond contestability of outcomes, algorithmic controllability further resolves the problem that contestability of outcomes focuses too heavily on decision outcomes by advocating the embedding of mechanisms such as human supervision and process review in the operation of algorithms, so as to achieve process controllability; but it falls into the same logical category error of inferring the legality of outcomes from process controllability.

2. The Proposal of the Demand-Oriented Approach

The demand-oriented approach is not a special theory of positive law; it is markedly domain-specific. In the technical domain, for example, demands largely concern practical aims such as model iteration, performance optimisation and compliance auditing. At the legal level, if algorithmic technology were absolutely neutral, requiring an explanation would serve no purpose, and a demand acquires legal significance when a balance of interests is disrupted. Therefore, explanation demands in law encompass the objectives and rules of various algorithmic governance scenarios, aiming to protect legitimate interests such as rights protection, risk control and public accountability; they not only constitute a reasonable expectation of, and claim to, explanation information at the technical level, but also constitute the basis for the legitimacy of the algorithmic explanation regime and are among the premises of the construction of the explanation standard.

Judging by the existing EU explanation standard, although the *Ck v. Dun & Bradstreet* case has rejected the formal transparency of disclosing the algorithmic code, it still retains the model-priority structure of explanation, that is, presupposing the accessibility of the algorithm's procedures, principles and related information, and then extracting information meaningful to the individual from them (*Ck v. Dun & Bradstreet*). Similarly, although the existing mitigation approach recognises the differences among audiences, it still takes as its premise the existence of an information set within the algorithm that can be fully accounted for, and places the individual in a position of ex post understanding and filtering of information.

By contrast, the demand-oriented approach first determines the explanation demands, thereby deriving the information needed for explanation, and then selects technical and institutional means such as local attribution, counterfactual explanation and algorithmic audit accordingly. On this basis, a complete explanation is no longer equated with the maximum degree of penetration of the black box, but is expressed as evidence sufficient to meet particular demands; it can thereby avoid both information overload and false transparency, and allow explanatory methods to be assessed for correctness, stability and verifiability corresponding to their legal purposes. At the same time, it can convert the existing technical gaps of explanation into obligations of system design, manual review and use restriction, rather than into a diminution of individual rights.

3. The Dual Structure of Algorithmic Explanation Demands

The demand-oriented approach works backwards to determine the information that should be provided, and then selects matching explanation techniques and institutional mechanisms. Therefore, the structuring of algorithmic explanation demands should complete the abstraction of demands at the normative level and match them to techniques at the implementation level. On the one hand, explanation demands should be capable of being fixed, to establish why an explanation is required, to whom it is owed, and how detailed it should be. On the other hand, explanation demands should be adapted to existing technical and institutional means. The demand-oriented approach does not simply adapt

demands to technical capacity, but seeks to further convert normative demands into concrete information tasks that can be realised by technical and institutional mechanisms, and therefore requires a means of connecting those tasks to technical and institutional measures.

3.1. An analysis of the structuring of existing explanation demands

In existing research on algorithmic explanation, many studies also consider explanation demands, which can be roughly classified into two types: scenario-specific structuring of explanation demands, and abstract structuring of explanation demands derived from particular values.

Regarding scenario-specific structuring, although it basically covers the typical scenarios of algorithmic application such as medical diagnosis, finance, the judiciary and public administration, and thereby extends the scope of explanation demands under the current provisions, it remains open-ended and dynamic and cannot satisfy the fixity of demands required by the demand-oriented approach. At the same time, from the existing research, the scenario-specific treatment of explanation demands can become excessively detailed. In the judicial application scenario, for instance, different scholars further distinguish between the judicial scenario and the criminal-justice scenario of algorithmic application, yet the explanation demands of the two are in fact similar (Xianjun Sang 2025; Zhongyang Wang 2024). Under such excessive scenario-specific treatment, on the one hand it tends to cause inconsistency within the legal order, making the explanation standards under similar demands diverge and making it difficult for developers, deployers and even regulators to form clear compliance expectations; on the other hand it tends to produce regulatory arbitrage, enabling the explaining party of algorithms to evade explanation obligations by exploiting the unclear boundaries between scenarios, or to apply selectively the lower standards favourable to it.

Regarding the abstract structuring of explanation demands, although it establishes fixed categories of explanation demand, it does not consider the problem of adaptation to explanation techniques, and remains an abstraction at a purely normative level, of limited significance for the construction of dynamic explanation standards. First, the explanation demands induced by existing research remain relatively fragmented and lack consensus. With demands unclear, it is difficult to adapt them directly to explanation techniques. Second, existing efforts to identify demands mainly seek to justify the legitimacy or necessity of algorithmic explanation, none of which has reserved space for technical adaptation, so that the interactive problem between technology and explanation demands cannot be resolved, and the explanation provisions are liable to be hollowed out again. Consider the demand for accountability, under the current state of affairs in which existing techniques can hardly fully open the black box to complete the attribution of responsibility, what technique should be matched with it and which component of the model should be explained remain unclear.

3.2. The proposal of the dual-structure scheme for algorithmic explanation demands

In light of existing classifications of explanation demands, the scenario-specific structuring can hardly satisfy the requirement of fixity under the demand-oriented approach, while the value-guided abstract structuring fails to adapt to technical and institutional means. How, then, should the demands of algorithmic explanation be structured? First, it is important to recognise that the structuring of explanation demands should still be based on application scenarios; a structuring of demands divorced from social facts can neither represent users' legal interests nor contribute to the realisation of normative purposes, and can hardly be justified even in terms of legitimacy and feasibility. However, such application scenarios should not be overly narrow individual scenarios, but representative typical scenarios. Representative scenarios can encompass similar cases. At the same time, in similar scenarios, the manner in which algorithmic decisions intrude upon the rights and interests of counterparties and the resulting harm are broadly similar, so that explanation demands exhibit homogeneity.

On this basis, the abstraction of explanation demands should use the temporal node as its organising standard, dividing algorithms into the behaviour stage and the outcome stage. The temporal-node standard is not an existing standard in technology or law; rather, it is a stage-based distinction developed for the induction and technical adaptation of explanation demands, taking the point of transfer of the main control over the model among actors as its basis and the operational stages of the model's development, deployment and application as the stages being distinguished. The behaviour stage concerns the development of the model and its deployment configuration before it is put into specific application, mainly corresponding to the control exercised by developers and deployers over the inside of the model. The outcome stage concerns the result-generation stage of the algorithm, it corresponds to the users outside the model and resolves the question of whether the outcome is appropriate and what corrective measures can be taken.

As for the significance of this distinction, it can provide a relatively fixed framework of demands for the demand-oriented explanation standard. From the continuity of control over the model, and subject to the autonomy of algorithms, existing explanation demands mainly fall between the behaviour stage, in which developers and deployers still possess complete control, and the outcome stage, in which control is basically lost after the model is put into application. Therefore, even if algorithmic application scenarios and technical forms continue to renew, new demands can still be classified under the existing categories of demand on the basis of control. More importantly, the temporal-node standard can also leave room for the use of explanation techniques in schemes for realising demands. Setting aside technical feasibility, existing schemes of demand induction can also complete the abstraction of demands, and the temporal-node standard does not differ from them at a purely normative level. The mismatch affecting the existing explanation standard arises from the limitation of explanation techniques, which is why the construction of the explanation standard begins to consider the problem of technical

adaptation. In this regard, the temporal-node standard induces demands by control, and in so doing also completes the assessment of the feasibility of information provision by control. The information supply of algorithmic explanation is constrained by the explaining party's control over the model; when the model exceeds control, obtaining information also becomes difficult. At the same time, from a technical perspective, the research and practice of explanation techniques have gone beyond the early stage of comprehensively dissecting the model as a whole under traditional expert systems, and have formed multi-dimensional technical classification standards such as the timing of explanation, model dependence, the scope of explanation and the mode of interaction (Sami Kabir et al. 2025). Among them, the technical classification of explanation based on ex ante model internals and ex post input-output results can already confirm that the logic of demarcation according to the temporal node conforms to technical fact.

3.3. The content of the dual structure of algorithmic explanation demands

Existing research on algorithmic explanation suggests that, explanation demands broadly include the protection of user rights, the regulation of power, decision trust, fairness and justice, algorithmic accountability, the regulation of algorithmic discrimination and the examination of big-data evidence. Under the temporal-node standard, how can the two stages of behaviour and outcome accommodate all existing demands, and under what higher-level concepts should they be abstracted? This requires further clarification to enable technical adaptation and guide the construction of the explanation standard.

3.3.1. Risk governance demand at the behaviour stage

From the existing explanation demands, demands such as rights protection and the regulation of power concern specific legal interests, and legal interests cannot be protected through legal declarations alone; regulation must address the acts or omissions of particular actors, so as to guide, constrain and evaluate the conduct of actors and prevent harm to legal interests. At the same time, because the law has not yet recognised the legal personhood of artificial intelligence, the conduct of protecting the legal interests corresponding to the existing explanation demands mainly points to the technical activities of developers, deployers and other actors throughout model research and development, integration into particular settings, operation and maintenance. Therefore, demands such as rights protection and power regulation, as legal interests under the limited control of developers and deployers, mainly correspond to the behaviour stage of the algorithm.

On this basis, these demands can be grouped under the concept of risk governance, for the following reasons. First, from the definition of risk itself, risk in law mainly refers to harm or loss with the possibility of occurrence, characterised by abstraction, potentiality and uncertainty as to whether it will materialise (Huanmin Lin 2025). In this regard, demands such as rights protection all correspond to particular legal interests in law, and, following the application of algorithms, may suffer harm or loss, thus corresponding to the feature of potential damage in risk. At the same time, in algorithmic

application, although the algorithmic black box is not the direct cause of the risk of algorithmic application, it obscures the process of algorithmic decision-making, making infringements of rights and interests difficult to identify and control, and even making it difficult to determine whether algorithmic conduct will actually realise the risk; such demands therefore also correspond to the feature of uncertainty in risk and can be fully subsumed under the category of risk in law.

Second, existing normative demands in algorithmic application, such as accountability and rights protection, correspond to attribution and the allocation of obligations within risk, and jointly fall within the scope of risk governance. In their treatment of risk, sociology and law are not wholly opposed: both link responsibility to decisions (Entscheidung). At the sociological level, Luhmann completed the conceptual shift from “security” to “danger”, resolving the problem that “security”, as the conceptual opposite of “risk”, obscures the role of the decision-maker in risk, thereby interpreting future negative consequences as the logical extension of present decisions and ensuring that responsibility can be anchored to the decision-maker (Niklas Luhmann 1993). On this basis, legal doctrine further develops the transformation from sociological attribution to normative obligations, projecting the attribution structure onto the dimensions of the urgency and probability of the occurrence of harm, forming the tripartite structure of “danger–risk–residual risk” (Gefahr–Risiko–Restrisiko), placing harms with different probabilities within the framework of the decision-maker’s obligations, corresponding to different contents of obligation. Under this analytical framework, the existing normative demands in algorithmic application, as the counterpart to risk, reveal the decisions of developers and deployers that are obscured by the traditional “algorithmic black box–algorithmic explanation” structure; at the same time, the existing demands, as obligations in law, further complete the transformation of obligations after attribution, embedding the actors at the behaviour stages of algorithmic development and deployment into the system of legal obligations.

In sum, the risk-governance demand for explanation differs from the risk-prevention requirement within existing AI governance frameworks: it seeks to realise the allocation of risk control and the attribution of responsibility for harm, that is, to anchor algorithmic risks to specific technical links and responsible actors through algorithmic explanation, to implement risk-prevention obligations, and to allocate responsibility after harm occurs. Whether they are principled demands such as fairness and justice, rights protection and power regulation, or specific scenario-based rule demands such as algorithmic accountability and the regulation of algorithmic discrimination, they all concern risk control and the attribution of responsibility, and can be subsumed under the demand of risk governance, corresponding to the behaviour stage of the algorithm.

3.3.2. Algorithmic trust demand at the outcome stage

Under the temporal-node standard, what demand does the outcome stage correspond to? From a technical perspective, because the outcome-output stage has externality and uncontrollability, the explanatory demand at this point should no longer focus on the risks associated with particular conduct, but on the trustworthiness of outcomes. However, it must be made clear that risk governance at the behaviour stage can also foster algorithmic trust; the account of trust at the outcome stage should

therefore distinguish between trust at the behaviour and outcome stages, assigning expectations of external reliability at the behavioural level to risk governance and distilling the algorithmic trust of the outcome stage.

Trust, as a demand of algorithmic explanation and even as a goal of AI governance, is already a basic consensus (Tae Wan Kim and Bryan R. Routledge 2022; Alison T. Lui et al. 2025), but what exactly is algorithmic trust? Existing research offers several accounts, which can be roughly classified into two types: the first treats algorithmic trust in the exercise of public power as an extension of trust in public authority (Junlin Yi 2025; Borong Wang and Yuanshui Lai 2024); the second, from a psychological perspective, analyses trust in terms of subjective feelings and perceived technical efficacy in human–machine interaction (Wei Dai and Xixin Wang 2025; Weiwen Huang 2025). Turning to the ways in which such trust is established, however trust is defined, existing proposals for building trust essentially take the form of computational reliabilism (Juan Manuel Durán 2025), namely, when confronted with the essential opacity caused by the complexity of algorithmic technology, not demanding a full understanding of the algorithm’s internal logic, but instead inferring its trustworthiness from external technical indicators such as the safety and stability of the algorithmic system. Externalist accounts of technical trustworthiness do address the existing technical predicament of algorithmic explanation, but external reliability assessment in essence still belongs to the scope of risk governance at the behaviour stage of the algorithm; at a time when algorithmic technology cannot be fully controlled, computational reliabilism cannot reach and eliminate problems at the outcome level such as algorithmic hallucination. Moreover, existing algorithms have already comprehensively intervened in social life; algorithmic trust that lacks an effective verification mechanism for outcomes can easily lead to the unnoticed reshaping of the ways in which social groups understand decisions by algorithmic logic, and even form an “algorithmic discipline”.

In response, the algorithmic trust demand at the outcome stage should not be the external technical indicators of computational reliabilism, but the ability to assess whether outcomes conform to empirical expectations, and the possibility of remedying outcomes that deviate from those expectations. Trust is a cross-disciplinary concept spanning politics, management, psychology, sociology and other fields; although its functions and definitions vary across disciplines, all disciplines basically regard it as a form of behavioural expectation within a particular relation, and the formation of such expectation relies on fixed and reliable experience within that relation. For example, in psychology, Rotter defines trust as an individual’s generalised expectation that the words, promises and verbal or written statements of others can be relied upon, formed from the reinforcement history of others honouring commitments acquired in early socialisation (Julian B. Rotter 1971). In sociology, Luhmann divides trust into personal trust and institutional trust, both of which likewise derive from reliable experience within the relation (Niklas Luhmann 2017). On this basis, an account of trust at the outcome stage should also be based on the particular relation in which trust resides.

At present, algorithmic technology has penetrated comprehensively into government services, resource allocation and the platform economy; relying on its data advantages and platform architecture, it moves

beyond the supporting role of traditional technological governance tools, transforms administrative rules and platform rules into automatically executed decision logic, and intervenes deeply in credit evaluation, judicial early warning, resource allocation and other links of the allocation of public resources and of rights and obligations, thereby gaining substantial power over individuals and markets in social life. In terms of the relationship underlying algorithmic trust, it should be an intermediate state between entrustment and social contract. Under this relation, the expectation of behaviour and outcomes is not simple interpersonal trust: the external reliability of an algorithm is not the most relevant basis for expectations about its behaviour, and the expectation of its behaviour in fact relies on social life experience, which derives from institutional trust and everyday common sense. For example, the expectation of the outcome of automated administrative punishment for speeding does not derive from simple external technical reliability, but from the social institutional experience of algorithms intervening in social governance. Therefore, trust at the outcome stage should not be merely the external trust of behaviour, but should involve a direct empirical assessment of behaviour and outcomes; and, given the quasi-power character of algorithms, algorithmic trust is not a simple empirical assessment, but must also possess the capacity for remedy.

4. The Reconstruction of the Explanation Standard under the Demand-Oriented Approach

4.1. The reconstruction of the standard under risk governance demand

Risk governance demand aims to allocate and implement risk-control obligations and to attribute responsibility for damage if the risk materialises. Under this goal, the explanation standard should shift from the disclosure of internal model information to the disclosure of information on risk-control conduct (hereinafter the “substitute standard”), thereby shifting the focus of explanation to the verification of the technical facts of risk mitigation measures. To this end, developers and deployers should each provide filing statements on risk assessment and the corresponding preventive and control measures, and deployers should disclose, on request, the input-, processing- and output-side logs of the algorithm, for technical verification.

4.1.1. The equivalence and economic efficiency of the substitute standard

In terms of explanatory equivalence, replacing the disclosure of internal model information with the verification of risk mitigation measures is an equivalent substitution for the realisation of risk governance demand, rather than a concession of legal demands to technology. At present, algorithmic explanation is not intended to open the algorithmic black box, but is premised on the realisation of risk governance demand; under this premise, equivalent verification is in essence the comparison of the effects of different standards at the dimension of demand. In this regard, disclosure of internal model

information can mainly reveal risk nodes and identify the actors responsible for them and, under idealised technology, assess the risk-control capacity of the responsible actors, thereby linking responsibility governance and realising risk governance demand. By comparison, under the substitute standard, existing techniques for identifying risks do not depend on decomposing the model internals, but rely mainly on technical schemes such as red-teaming; moreover, red-teaming at the market level mostly adopts the most cutting-edge AI models, and the risks discovered under such testing basically constitute the limit of human foreseeability. Therefore, judged by the effect of the verification of risk mitigation measures, it can also verify the boundaries of different actors' capacity to control risk, completing the reasonable allocation of risk among developers, deployers, users and other actors. As for implementation costs, the filing of information on risk mitigation measures and the retention of logs entail in fact only the storage cost of data records, and such costs have already been incurred under the current compliance requirements, so that the substitute standard basically adds no new cost.

4.1.2. The concrete content of the substitute standard

First, risk governance demand is premised on risk control, and such control is premised on the foreseeability of risk. Therefore, algorithmic explanation under risk governance demand should provide an account of the risk assessment for the model as applied, including the risks of abuse and malicious exploitation of the algorithm. Second, risk governance also links the attribution of responsibility upon the realisation of risk, so as to ensure the implementation of risk-control obligations; and the attribution of responsibility is premised on the boundaries of control. Once the risks have been identified, the boundaries of control can be examined through the mitigation measures adopted. At the same time, the boundaries of control do not exist a priori; technically, they should be inferred in reverse from the technical conduct actually performed by the responsible actors. Where the responsible actors have adopted risk mitigation measures conforming to the general standard and the foreseeable risk still materialises, this signifies that the risk is uncontrollable. Conversely, this signifies a failure to perform the risk-control obligation within the controllable scope. Therefore, algorithmic explanation under risk governance demand should also describe how responsibility for algorithmic safety is allocated among actors, the technical prevention and control measures, and the like. Finally, the specific risk-governance measures may differ across models and environments, which also affects the verification of risk mitigation measures, so that the basic information of the algorithm, the algorithmic model and the context in which the service is used should also be accounted for.

It should be noted, however, that an account of risk assessment and mitigation measures is also, in essence, a compliance statement, and existing practice has demonstrated that compliance statements can easily degenerate into template-based exercises that do not support the attribution of responsibility. For example, in the EU Dun & Bradstreet case, the information provided by D&B was in fact inconsistent with the facts (CK v Dun & Bradstreet Austria). In response, in addition to the compliance statement, the logs of the input, processing and output sides should also be disclosed, to provide a means of verifying that information and give courts and users a means of addressing information asymmetry.

4.1.3. The scheme for realising the explanation standard

Although the substitute standard is feasible in technical and cost terms, how should it be realised? For the explanatory content proposed above, implementing the explanation standard requires two steps: first, the explaining party should be identified, to ensure that an explanation is provided; second, the mode of explanation should be determined, to balance interests such as trade-secret and personal-data protection. Regarding the party responsible for providing the explanation, developers and deployers should each account for the basic information of the algorithm, the algorithmic model, the service situation, and the risk assessment and mitigation measures. In addition, deployers should account for the logs of the input, processing and output sides. Under the logic of allocating risks arising from algorithmic applications, the allocation of risk is premised on the conduct that creates the risk and the capacity to control it, and at the outset of the algorithm's development such risk-control actors have in fact been preliminarily determined. Among these, developers are mainly responsible for the safety training and value alignment of the base model, and constitute one of the risk-control actors, so that they should account for the risk assessment and mitigation measures they have adopted. Although deployers cannot intervene deeply in the training of the base model, can still implement limited safety reinforcement of runtime risk mitigation measures, such as adopting filtering mechanisms and safety guardrails for the "input-output" relation, so that they also constitute risk-control actors and should account for the risk assessment and mitigation measures such as safety guardrails. Furthermore, because deployers operate the model in its application setting and possess the capacity to record the operation of the model, they should also be responsible for retaining and disclosing the logs of the input, processing and output sides.

Regarding the form of explanation, the basic information of the algorithm, the algorithmic model, the service situation, and the risk assessment and mitigation measures should be provided through filing statements. First, this explanatory information is determined ex ante, having been generated during the development and deployment stages before the model enters commercial use, and its content is basically determined. Second, information such as risk mitigation measures contains, to some extent, trade secrets of developers and deployers; compulsory public disclosure would lead to the leakage of trade secrets and weaken enterprises' incentive to innovate, and would at the same time prompt hackers to engage in reverse engineering, giving rise to security risks.

At the same time, log-retention information should be recorded and stored by deployers in real time and disclosed in response to a reasonable request by a relevant party. First, algorithmic log information is dynamic: it is generated in real time through the real-time processes involved in individual decisions, and its content is highly dependent on changes in specific inputs and the operational environment, so that filing measures are not feasible. Second, log information usually contains users' personal data, behavioural trajectories and even sensitive information; direct disclosure would infringe personal-data interests and is likewise not feasible. Therefore, log information should be stored by deployers and disclosed on request.

Furthermore, the proposed approach to explanation through filing and log retention should not be understood as an addition to the existing regime of algorithmic governance. Rather, it represents a

systematic application of existing EU legal provisions. EU law already provides a relatively well-established legal basis for documenting algorithmic systems and retaining logs. Article 30 of the GDPR expressly requires data controllers to maintain records of processing activities involving automated decision-making, while Article 35(3)(a) requires a data protection impact assessment for automated decision-making that produces legal effects or similarly significant effects. The demand for risk governance is, in essence, directed towards protecting the legal interests of natural persons and other actors. In the field of personal data, it therefore largely falls within the scope of data protection impact assessments. Moreover, Article 35(7) of the GDPR specifies at least four elements of such an assessment: a systematic description of the envisaged processing operations and their purposes; an assessment of the necessity and proportionality of those operations in relation to their purposes; an assessment of the risks to data subjects' rights and freedoms; and the measures envisaged to address those risks. The proposed approach to explanation through filing and log retention can thus be accommodated within the existing legal framework. Beyond the GDPR, Article 11 of the EU Artificial Intelligence Act requires technical documentation for high-risk AI systems to be drawn up before they are placed on the market or put into service and to be kept up to date, while Article 12 requires such systems to technically allow the automatic recording of events throughout their lifetimes. These provisions further extend the legal framework for documentation and log retention.

It is important to note that, although existing practice does not regard the current filing and log retention as provisions on algorithmic explanation but generally treats them as independent regimes, they do not constitute a regime substitute for algorithmic explanation; rather, they should fall within the scope of the explanation regime. In terms of their institutional effects, although the existing legislation anticipates the two as tools of risk governance, they generally lack effective means of verification in existing practice. In practice, the filing regime exhibits problems including arbitrary content, insufficient effective information, low intelligibility and incompleteness, and has basically failed to meet legislative expectations (Yuting Guo 2025). By contrast, when brought within the explanation standard, it not only provides substantive guidance for the content of algorithmic filing, but, through the interaction between filing information and log information, opens a channel for verifying the authenticity and effectiveness of filing information. Moreover, responsibility under the existing regimes is tied only to administrative liability and is mainly directed at the compliance measures themselves; under the regime of algorithmic explanation, however, responsibility is broadened, being used as a means of verifying risk-control capacity and linking civil and even criminal responsibility governance, which in turn strengthens the performance of compliance obligations.

4.2. The reconstruction of the standard under outcome trust

Algorithmic trust requires decisions to conform to experience and departures from experience to be remediable. The algorithm under such trust differs from the algorithm in the general commercial field: the decision outcomes of the former usually directly concern the legal rights and interests of the persons affected by those decisions and fall within the scope of legal regulation, whereas the latter must still act

on the basis of decision outcomes in order to produce legal effects, and is not an object of legal regulation. Under this premise, the explanation standard under algorithmic trust should have deployers and other operating actors complete the publicity of general social experience independent of the algorithmic decision logic, and, when outcomes deviate from experience, provide a fully reasoned report of human review.

4.2.1. The equivalence and economic efficiency of the publicity of general social experience

In terms of its function, it seeks to balance the different interests in social relations, and in essence exercises public power or quasi-public power as social management through the medium of algorithms, so that the output results and input content of such an algorithm should possess a causal link conforming to general empirical assessment. In fact, if current algorithms were merely rule-based algorithms that completely follow the logic of “input–rule–output”, then the algorithm could achieve absolute neutrality, and the algorithm itself could realise the trust demand. However, the function of current algorithms lies in extracting and organising the facts of a case, and finally extracting weights from the case facts to fit with established rules. Under this function, the standard of algorithmic intelligibility promoted by existing practice and research is in fact intended to ascertain the weights assigned by the algorithm in individual decisions, and finally to derive the trustworthiness of the outcome on the basis of the causality between decision weights and output results. However, because existing techniques can hardly fully open the algorithmic black box, the intelligibility standard can scarcely contribute to the realisation of algorithmic trust at present.

Under this limitation, the intervention of general experience can in fact equally realise algorithmic trustworthiness. In terms of the underlying reasoning, the logic of the existing intelligibility standard is to ascertain the weights applied by the algorithm from the “input–output” relation, thereby completing the assessment of empirical consistency and finally deriving whether the outcome is trustworthy. By comparison, on the basis of the combination of general social experience and input content, the output result can equally be inferred, completing a comparison with which to assess the trustworthiness of the output. In substance, under this logic, algorithmic explanation first presupposes the decision logic under general experience, and then, on the basis of the consistency assessment of the outcome, infers whether such weight extraction conforms to general experience. Therefore, under the existing technical limitations, the realisation of algorithmic trust can equally be replaced by the publicity of general experience.

It is worth noting that the disclosure of general social experience is intended, in essence, to address the cognitive limitations of users and other recipients of explanations. Where those recipients possess the relevant professional knowledge, there is no need to explain such experience to them. As to its source, platforms and other deployers, as professional actors operating in particular contexts, generally have an understanding of general social experience. Its disclosure can therefore be undertaken by deployers alone and does not entail substantial costs.

4.2.2. The concrete content of general social experience

The publicity of general social experience is in essence the external replacement of the content of the algorithm's internal decision logic. In current market practice, the publicity of decision experience is already fairly common, although such disclosures mostly consist of compliance statements focused on the model itself and remain, in essence, unilateral self-certification by platforms without a means of verification. How, then, should the publicity of general experience under algorithmic trust be set?

Under this definition of general social experience, it should refer to the basic, shared criteria for judgment formed by a particular social community on the basis of universal life experience, accumulated common sense and rational cognition, concerning the ordinary course of affairs, the normal causal relations, the benchmarks of behavioural norms and reasonable expectations about outcomes. On the one hand, general social experience belongs to consensual social judgement, and carries the function of a benchmark of consistency assessment in algorithmic trust; this benchmark in essence completes the transfer of trust: because general social experience conforms to trust expectation, outcomes conforming to general social experience also possess a trustworthy expectation. On the other hand, general social experience should be an empirical rule acceptable to ordinary members of society. Platform users, as the recipients of the explanation, are not professional technicians and generally lack the capacity to understand technical knowledge.

On this basis, general social experience should be kept relatively isolated from the technical explanatory content of the model itself. At the same time, the publicity of such experience should enable recipients of the explanation to compare it with, and draw inferences from, individual outcomes, that is, the disclosed experience should provide a basis for assessing empirical consistency. Finally, the publicised experience should be open to public scrutiny and independent professional review, so as to avoid the use of new templates for disclosed information. For example, in the credit-scoring scenario, the publicity of general social experience should include: (1) the commonly recognised factors associated with credit evaluation, such as income level and debt ratio; (2) the scoring logic of each factor; and (3) how the score is used.

4.2.3. The mode of human review upon deviation from general social experience

It is important to note that, apart from the assessment of empirical consistency, an ineffective remedy for outcomes that depart from general social experience cannot establish algorithmic trust either. In current market practice, under some algorithmic decisions, even if the assessment of general social experience is completed, when affected persons request review, the process is still largely driven by the algorithm, and the reasons given after review often repeat the reasons given at the time of the algorithmic decision.

In response, when outcomes deviate from general social experience, deployers and other operating actors should provide a means of obtaining human review and a fully reasoned justification. In fact, the

mechanism of human review under algorithmic decision-making already exists, but in existing practice it has often been used as a defence against algorithmic explanation, such as the formalised human review in the case of the deactivation of Uber drivers' accounts. Therefore, human review should provide a complete, externally verifiable argument addressing the outcome of the algorithmic decision, at least comprising fact-finding, the application of general social experience, and discretionary reasoning. Among these, fact-finding should restore the input information underlying the decision by relying on the input-side log under risk governance; the application of general social experience should include legal norms, business rules or platform conventions—experience, customs and rules commonly recognised by social groups; and discretionary reasoning should substantively apply general experience to the input facts.

Conclusion

The SCHUFA credit-scoring case and the series of cases concerning the dismissal of Uber drivers by robots, which have formed in recent years around the obligation of explanation in automated decision-making, indicate that EU market actors have a tendency to evade this explanation standard. Analysing the reasons, this article holds that the root of the problem lies in the fact that the current state of explanation techniques is not adapted to the EU explanation standard. The current EU explanation standard was formed in an environment of rule-based and code-based automated decision-making, and its basic premise was that the explanation demands of counterparties could be satisfied by disclosing the algorithmic logic or the determining factors. Yet, against the backdrop of neural networks and other complex models becoming important decision-making tools, explanation of the model internals may face simultaneously the limitations of insufficient faithfulness and excessively high disclosure cost.

Accordingly, this article proposes a demand-oriented framework of algorithmic explanation to address the difficulties of applying the EU explanation standard under modern explanation techniques. On the basis of this framework, explanation demands should first be induced and abstracted, according to the temporal-node standard of whether the explaining parties retain actual control over the model, into the risk governance demand at the behaviour stage and the algorithmic trust demand at the outcome stage. The former seeks to realise, through explanation and records, the allocation, performance and tracing of responsibility for risk-control obligations; the latter seeks to enable affected persons to judge whether automated decisions conform to general social experience, and to obtain an effective remedy when an outcome deviates abnormally. As to the former, this article advocates relying on existing governance mechanisms such as algorithmic filing, risk assessment and log retention, and replacing the universal disclosure of internal model information with the filing statements of risk assessment and mitigation measures, and the retention and disclosure of decision logs on request. As to the latter, it advocates taking the verifiable general social experience and the degree of deviation between it and case-specific decisions as the benchmark of explanation, and configuring a human-review mechanism in cases of significant deviation.

Of course, the scope and extension of the explanation framework proposed here remain to be tested. First, the temporal-node standard is premised on the existence of a clear boundary of control between developers, deployers and other actors, and its applicability to current intelligent agents and other AI systems that do not produce a single decision as their final output requires further examination. Second, supporting designs such as the probative effect of filing information in attribution, the procedural structure of on-application disclosure of retained logs, and the formation and updating mechanism of general social experience, require clarification through detailed institutional design. In sum, this article maintains that the future development of the regime of algorithmic explanation should not continue to focus on the black box itself, but should turn further towards “at which node, for which demand, by which actor, what kind of information sufficient to realise accountability and remedy should be provided”.

Declarations

Author Contribution

F.Z. is the sole author of this work and contributed to all aspects of the study, including conceptualization, methodology, analysis, and the writing and revision of the manuscript.

Data Availability

This article is based on an analysis of publicly available legislation, judicial decisions and published literature. It does not include any empirical analysis and is not based on any dataset.

References

1. A. Secondary Sources
2. An J (2023) Hierarchy of algorithmic transparency. *Chin J Law* 2:54–57 (in Chinese)
3. Biedermann A, Lau T (2024) Decisionalizing the problem of reliance on expert and machine evidence. *Law Probab Risk* 23:mga007
4. Binns R (2018) Algorithmic accountability and public reason. *Philos Technol* 31:543–556
5. Carnat I (2024) Addressing the risks of generative AI for the judiciary: the accountability framework(s) under the EU AI Act. *Comput Law Secur Rev* 55:106067
6. Chapdelaine P (2024) Algorithmic price personalization and the limits of anti-discrimination law. *McGill Law J* 69:489–513
7. Dai W, Wang X (2025) The limitations of algorithmic transparency mechanisms and their overcoming. *ECUPL J* 1:39–43 (in Chinese)
8. Dewitte P (2025) AI meets the GDPR: navigating the impact of data protection on AI systems. In: Smuha NA (ed) *The Cambridge handbook of the law, ethics and policy of artificial intelligence*. Cambridge University Press, pp 133–157

9. Ding X (2022) Automatic decision-making based on trust: principle reflection and system reconstruction of the right to algorithm interpretation. *China Legal Sci* 1:99–118 (in Chinese)
10. Durán JM (2025) Beyond transparency: computational reliabilism as an externalist epistemology of algorithms. *Philosophy of science for machine learning: core issues and new perspectives* (pp. 55). Synthese Library, vol 527. Springer
11. Goodman B, Flaxman S (2017) European Union regulations on algorithmic decision-making and a right to explanation. *AI Magazine* 38:50–57
12. Guo Y (2025) Constructing a risk-graded artificial intelligence system filing system. *Orient Law* 6:87–88 (in Chinese)
13. He X (2023) The justification and limitations of the algorithm interpretation rights. *J Dalian Univ Technol (Social Sciences)* 3:72 (in Chinese)
14. Huang W (2025) The legal nature of algorithmic trust. *Global Law Rev* 3:126–132 (in Chinese)
15. Kabir S, Hossain MS, Andersson K (2025) A review of explainable artificial intelligence from the perspectives of challenges and opportunities. *Algorithms* 18:10
16. Kaminski ME, Urban JM (2021) The right to contest AI. *Columbia Law Rev* 121:1957–2047
17. Kim TW, Routledge BR (2022) Why a right to an explanation of algorithmic decision-making should exist: a trust-based approach. *Bus Ethics Q* 32:75–102
18. Lei Y (2026) Operational risks and regulatory system of reputational penalty in the digital age. *Tribune Political Sci Law* 2:148 (in Chinese)
19. Lin H (2025) Governing artificial intelligence: navigating the divide between risk and danger. *J Comp Law* 6:175–176 (in Chinese)
20. Liu Q (2026) The limits of protection for procedural rights in automated administration. *Jurist* 1:125–139 (in Chinese)
21. Luhmann N (1993) *Risk: a sociological theory* (Barrett R, Trans). Walter de Gruyter
22. Luhmann N, Davis H, Raffan J, Rooney K (2017) Trans.). *Polity*
23. Lui AT, Lamb G, Durodola L, Law (2025) *Innov Technol* 17:289–317
24. Miller T (2019) Explanation in artificial intelligence: insights from the social sciences. *Artif Intell* 267:1–38
25. Rotter JB (1971) Generalized expectancies for interpersonal trust. *Am Psychol* 26:443–452
26. Sang X (2025) System construction and operation of judicial algorithm explanation mechanisms. *Law Modernization* 3:158–175 (in Chinese)
27. Su Y (2020) The genealogy of regulation on algorithms. *China Legal Sci* 3:167–168 (in Chinese)
28. Su Y (2024) On the system establishment of algorithm interpretation. *Orient Law* 1:89–95 (in Chinese)
29. Wachter S, Mittelstadt B (2019) A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Bus Law Rev* 2019:494–620

30. Wang B, Lai Y (2024) Legal incentives and formation of algorithmic trust in the digital-intelligent society. *J Nanning Normal Univ (Philosophy Social Sci Edition)* 6:132–133 (in Chinese)
31. Wang C (2024) The predicament and relief of algorithm interpretation in automated administration. *Law Sci Magazine* 3:75–86 (in Chinese)
32. Wang H (2022) Transparency as manipulation? Uncovering the disciplinary power of algorithmic transparency. *Philos Technol* 35:69. <https://doi.org/10.1007/s13347-022-00564-w>
33. Wang Z (2024) The institutional choices for algorithmic interpretation in criminal justice. *J China Univ Political Sci Law* 6:251–261 (in Chinese)
34. Xie Z (2020) Regulating algorithmic decision: focusing on the right to explanation of algorithm. *Mod Law Sci* 1:179 (in Chinese)
35. Yang Z (2024) Another possibility to realize the algorithm transparency: explainable artificial intelligence. *Administrative Law Rev* 3:158–160 (in Chinese)
36. Yi J (2025) On the trust building of human-machine collaborative trial. *China Legal Sci* 2:159 (in Chinese)
37. Yuan Z (2025) Should algorithms be interpreted? The governance dimension of controllable AI. *Legal Forum* 1:130 (in Chinese)
38. Zhang E (2023) Theoretical reflection and institutional construction of algorithmic transparency. *J Huazhong Univ Sci Technol (Social Sci Edition)* 6:30–31 (in Chinese)
39. Zhao L (2024) A study of technical due process regulation of automated administration. *Legal Sci* 3:94 (in Chinese)
40. Legislation B International Instruments & Official Reports
41. Brazil (2018) General Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais. Law No. 13.709/2018)
42. China (2021) Personal Information Protection Law of the People's Republic of China
43. European Union (1995) Directive 95/46/EC (Data Protection Directive). *Official J Eur Union L* 281:31–50
44. European Union (2016) Regulation (EU) 2016/679 (General Data Protection Regulation). *Official J Eur Union L* 119:1–88
45. European Union (2024) Regulation (EU) 2024/1689 (Artificial Intelligence Act). *Official Journal of the European Union. L* 2024/1689
46. C Case Law
47. App D (2023) & *Couriers Union v. Uber B.V.*, ECLI:NL:GHAMS:2023:796 *Gerechtshof Amsterdam*
48. CK v (2025) *Dun & Bradstreet Austria GmbH and Magistrat der Stadt Wien*, Case C-203/22. CJEU
49. SCHUFA Holding and Others (Scoring) (2023) Case C-634/21. CJEU

Tables

Tables 1 and 2 are available in the Supplementary Files section.

Figures

Figure 1. Model-First Process of Conventional Algorithmic Explanation

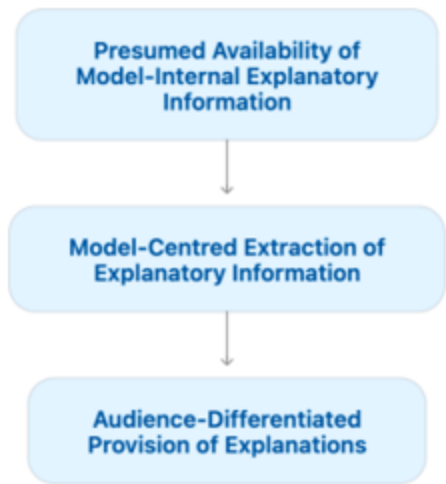


Figure 1

See image above for figure legend

Figure 2. Demand-Oriented Process of Algorithmic Explanation

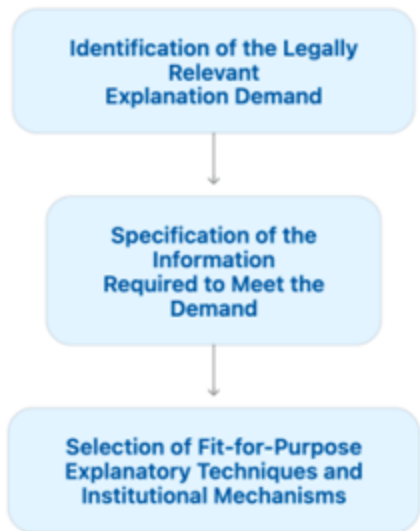


Figure 2

See image above for figure legend

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [Table1.png](#)
- [Table2.png](#)
- [SupplementaryInformation.docx](#)