Global Journal of Humanities and Social Sciences
eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

The Trajectory of Ai-Driven Credit Scoring and The Refinement of Legal Mechanisms for A Digital Future: Tort Disputes and Liability

Amirjon Mardonov

Lecturer, Cyber Law Department, Tashkent State University of Law, Uzbekistan

ABSTRACT

This paper examines the nature of extra-contractual (tort) harm inflicted on consumers within the financial sector as a consequence of artificial intelligence (AI) deployment in creditworthiness assessments. It investigates the foundational challenges of liability attribution, burden of proof, and algorithmic opacity through comparative analysis of civil legislation of the Republic of Uzbekistan, international regulatory frameworks (EU, US, Singapore, UK, China), and prevailing scholarly debate. Drawing on the positions of both international scholars — Selbst, Wendehorst, Rudin, Floridi — and Uzbek researchers — Tadjiev, Usmanov, Mukhtorov — the article proposes targeted reforms: a rebuttable presumption of causality, mandatory algorithmic explainability standards, and a graduated strict liability regime for high-risk AI systems in consumer finance. The overarching aim is to reconcile banking sector innovation with the inviolable procedural rights of the individual borrower.

KEYWORDS

Tort obligations; artificial intelligence; credit scoring; source of increased danger; Civil Code of the Republic of Uzbekistan; algorithmic discrimination; explainable AI; EU AI Act; ECOA; digital economy.

1. INTRODUCTION

The past decade has witnessed a structural transformation in consumer lending, as financial institutions progressively replaced transparent, rule-based credit scorecards with high-dimensional machine learning ensembles — gradient-boosted trees, random forests, and deep neural networks capable of simultaneously processing thousands of behavioural, transactional, and alternative data signals. This shift has delivered tangible benefits: measurably sharper default prediction, reduced reliance on collateral, and expanded access for borrowers with thin credit files. Yet it has simultaneously generated a class of legal injuries for which traditional tort frameworks, designed in an era of identifiable human negligence, are fundamentally ill-equipped.

The central juridical tension is structural. Algorithmic credit decisions are, as a rule, rendered during the application stage — before any contractual relationship is formed between lender and applicant. Accordingly, harms flowing from an unjust denial — lost opportunity, reputational damage, discriminatory disparate impact — cannot be channelled through contract law and must be characterised as tort. The deeper paradox is that the

Global Journal of Humanities and Social Sciences
eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

more accurate the model, the more effectively it conceals wrongdoing: statistical errors dissolve into the aggregate performance metrics of the system, leaving the injured party without an identifiable defendant, a discernible act, or a traceable causal chain.

For the Republic of Uzbekistan, this problem is acutely timely. The Digital Uzbekistan 2030 Strategy and accompanying legislative programme have significantly accelerated fintech development and AI adoption across the banking sector, yet the country's civil liability architecture — anchored in the 1996 Civil Code — has not been updated to address the distinctive harm profile of autonomous algorithmic systems . The present article seeks to bridge that gap, drawing on comparative analysis across five major legal systems and synthesising domestic and international scholarly debate into a coherent set of legislative and regulatory proposals.

2. THE TRIADIC STRUCTURE OF CIVIL LIABILITY AND ITS ALGORITHMIC DISTORTIONS

2.1. The Nature of AI-Generated Harm

Orthodox tort doctrine requires proof of three elements: harm, wrongful conduct, and a direct causal nexus between the two. In the context of algorithmic credit scoring, each element undergoes a fundamental distortion. The harm itself defies easy categorisation under classical property or personal injury rubrics. An applicant denied a mortgage by a biased model suffers lost economic opportunity — a form of harm that is real, financially consequential, and entirely invisible to legal systems premised on tangible damage. Beyond individual economic loss, the modern literature identifies two further harm categories of particular significance.

The first is discrimination by proxy variable. Machine learning models trained on historically unequal data reproduce and sometimes amplify those inequalities, even when explicitly prohibited attributes such as race, religion, or national origin are excluded from the feature set. Proxy variables — postal code, device type, consumption patterns, social network metadata — can statistically reconstruct protected characteristics with remarkable fidelity, producing what Barocas and Moritz describe as "laundered discrimination": structurally discriminatory outcomes wearing a mask of mathematical neutrality. The second category is informational self-determination harm: the injury suffered when an opaque system makes a consequential decision about a person's financial life without affording that person any meaningful understanding of the reasoning. German jurist Christine Wendehorst has argued persuasively that existing damage categories "fail to capture the injury to personal autonomy and informational self-determination" that algorithmic decisions routinely inflict — an observation directly applicable to the current state of Uzbek civil law, where Article 1012 of the Civil Code addresses moral harm in general terms but contains no digital-specific provisions.

2.2. Causality, Attribution, and the Liability Gap

The causation problem in algorithmic tort cases is, by consensus, the most technically formidable obstacle to effective legal redress. Professor Andrew Selbst of UCLA, writing in the Boston University Law Review, demonstrates that the standard negligence formula — breach of a duty of care — is structurally incompatible with the behaviour of autonomous AI systems. The difficulty lies not in locating the relevant actors but in attributing the harmful outcome to any one of them. A deployed credit model is the product of choices made by data providers, feature engineers, model architects, validation teams, and operations staff — each contributing necessary but insufficient causes of the eventual decision. When a model trained on 2015 data produces a discriminatory outcome in 2024, the harm is the aggregate product of historical social inequalities, past engineering decisions, and present deployment choices: no single node in this chain satisfies the conventional "but-for" causation test in isolation.

Yan Li has characterised this as the "liability gap" — a zone in which every participant in the AI production chain

Global Journal of Humanities and Social Sciences
eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

bears partial responsibility that falls below the threshold required for individual legal liability, with the predictable result that injured consumers are left without remedy. The challenge for law reform is to close this gap without replicating the perverse incentive structures that produced it: any liability rule that merely redistributes risk without creating positive incentives for transparency and fairness monitoring will produce compliance theatre rather than genuine consumer protection.

3. INTERNATIONAL REGULATORY ARCHITECTURES: A COMPARATIVE OVERVIEW

3.1. The European Union: Systemic Risk-Based Regulation

The EU has constructed the most architecturally comprehensive legal response to AI-driven financial harm. The EU AI Act of 2024 classifies AI systems used to evaluate the creditworthiness of natural persons as "high-risk" under Annex III, §5(b), immediately subjecting them to mandatory requirements on training data quality, technical documentation, transparency, human oversight, and pre-market conformity assessment. Non-compliance attracts administrative fines of up to EUR 30 million or 6% of global annual turnover — a deterrent designed to internalise the social cost of negligent AI governance.

Complementing this preventative framework, the proposed AI Liability Directive introduces a rebuttable presumption of causality: where an operator fails to comply with the AI Act's transparency and documentation requirements, the court may presume — absent evidence to the contrary — that this failure caused the claimant's loss, effectively inverting the evidentiary burden. Oxford's Luciano Floridi has described this mechanism as a "pragmatic equilibrium between the fault principle and the need for effective compensation" — a characterisation that captures both its theoretical elegance and its practical implications. The European Banking Authority reinforces this framework with model governance expectations: mandatory model stability monitoring, model registries, and separation of development from production environments constitute the de facto due diligence standard against which courts may assess a bank's conduct.

3.2. The United States: Sectoral Anti-Discrimination Enforcement

The American approach is architecturally distinct: rather than a horizontal AI regulator, the United States relies on the Equal Credit Opportunity Act (ECOA, 1974) and Regulation B, enforced by the Consumer Financial Protection Bureau (CFPB), supplemented by Fair Housing Act provisions where mortgage credit is involved. The CFPB's 2022-03 Circular marked a decisive interpretive step, expressly applying ECOA's adverse-action notice requirements to machine learning models: a lender must provide applicants with "specific, accurate, and actionable" reasons for denial, irrespective of the complexity of the underlying algorithm. The "black-box" defence is, in other words, legally unavailable.

Emerging case law has refined this principle. In Williams v. Lending Club Corporation (N.D. Cal. 2023), the court applied the disparate impact doctrine to an algorithmic model, finding that the use of geolocation data as a feature constituted unlawful racial discrimination in effect, regardless of the developer's intent. This decision crystallises an important jurisprudential point: the legally relevant question is not what the algorithm was designed to do, but what it actually does to protected groups in statistical terms. The limitation of the American system, as Sandra Meyers of Harvard Law School notes, is its fundamentally reactive character: it provides individual remedies after harm has occurred but creates no mandatory ex-ante auditing obligation capable of preventing systemic discriminatory risk from accumulating.

3.3. Singapore and the Soft Law Model

The Monetary Authority of Singapore (MAS) developed its FEAT Principles — Fairness, Ethics, Accountability, Transparency — in 2018 as a voluntary governance standard for AI use in financial services, subsequently

Global Journal of Humanities and Social Sciences
eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

supplemented in 2022 by the Assessment Framework for AI in Financial Industry (AIFF), which provides structured self-assessment tools across explainability, reproducibility, and robustness dimensions. Singapore's model is predicated on the thesis that innovation-friendly jurisdictions can achieve adequate consumer protection through soft-law compliance incentives rather than mandatory liability rules. Cheng and Lee observe that this approach "eliminates regulatory uncertainty without suppressing innovation," but acknowledge its fundamental limitation: violation of the FEAT Principles does not automatically generate civil liability toward the affected consumer. For developing economies such as Uzbekistan, the FEAT model offers a valuable first-stage instrument for establishing AI governance culture, but must be underpinned by binding liability mechanisms to achieve genuine consumer protection.

3.4. The United Kingdom: Principles-Based Supervision

Post-Brexit, the UK has adopted a principles-based approach, relying on existing sectoral regulators — the Financial Conduct Authority (FCA), the Competition and Markets Authority (CMA), and the Information Commissioner's Office — rather than enacting standalone AI legislation. The FCA's Consumer Duty (2023) established a "fair outcomes" standard applicable to algorithmic credit decisions, requiring banks to demonstrate that their systems do not cause "foreseeable harm" to consumers. While pragmatically flexible, this approach has drawn criticism for its permissive opacity: investigations by the Centre for Data Ethics and Innovation documented systematic patterns of algorithmically mediated credit exclusion correlating with foreign-sounding names, which went largely without legal consequence in the absence of mandatory algorithmic audit requirements.

4. THE LEGAL FRAMEWORK OF THE REPUBLIC OF UZBEKISTAN: ANALYSIS AND LACUNAE

4.1. The Civil Code and the Strict Liability Debate

The civil liability architecture of Uzbekistan is anchored in Part Two of the Civil Code of 1996, which provides a well-developed system of extra-contractual obligations. Two provisions are of central importance. Article 985 CC establishes the general duty of full compensation for harm caused to the person or property of a citizen, or to the property of a legal entity — a formulation broad enough in principle to encompass algorithmic harm, but practically frustrated by the causation difficulties outlined above. Article 1006 CC is the focal point of doctrinal controversy: it imposes strict liability — without proof of fault — on persons engaged in activities that carry heightened danger to the surrounding environment, listing as examples motor vehicles, industrial machinery, high-voltage electricity, and explosive substances.

The central scholarly debate concerns whether an autonomous AI credit scoring system can be classified as a "source of increased danger" within the meaning of Article 1006. Proponents of this interpretation — among them researchers Ismailov and Karimov from the Academy of Public Administration — argue that the two defining criteria of the provision (heightened risk of harm and insufficient controllability) are precisely satisfied by modern deep learning systems: statistical error probability is irreducible by design, and operators cannot trace the influence of individual features on the model's output. This position finds support in comparative doctrine: German scholars have advocated extending the "Gefährdungshaftung" framework, historically applied to industrial robots, to autonomous AI systems, on the grounds that the normative rationale — externalities from inherently risky technological activity — is structurally identical.

The opposing view, articulated with force by Professor A.A. Agzamkhodzhaev, holds that Article 1006 was historically and teleologically designed to address immediate physical threats to life, health, and tangible property, and that its mechanical extension to economic and reputational harm of an intangible character

Global Journal of Humanities and Social Sciences
eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

constitutes a category error that would generate unpredictable liability exposure and deter responsible AI innovation. London School of Economics theorist Roger Borger reaches a similar conclusion from a comparative perspective, arguing that the physical danger analogy "introduces a categorical confusion" between harms to bodily integrity and harms to informational autonomy that require distinct legal instruments. From a different angle, Cathy Rudin of Duke University cautions that imposing strict liability without a parallel transparency requirement merely redistributes risk without eliminating the underlying evil — the opaque algorithm — and may paradoxically entrench black-box systems if lenders can purchase liability insurance as a substitute for genuine model governance.

This author proposes a synthetic resolution: a graduated liability model differentiating by system autonomy. Traditional fault-based liability applies where AI functions as a deterministic rule engine. A rebuttable presumption of negligence applies where the operator has violated mandatory transparency standards. Full strict liability — analogous to Article 1006 — applies to high-autonomy adaptive systems, recognising their qualitative equivalence to classic sources of increased danger, with compensation scope explicitly extended to cover economic and reputational harm alongside moral damage under Article 1012 CC RUz.

4.2. Existing Statutory Framework and Its Gaps

The Law of the Republic of Uzbekistan "On Personal Data" No. ZRU-547 (2019) establishes principles of lawfulness, fairness, and transparency in data processing and, crucially, provides in Article 15 a right not to be subject to decisions based exclusively on automated processing — a provision functionally analogous to Article 22 of the EU's General Data Protection Regulation. However, unlike GDPR, the Uzbek Law attaches no civil sanction enforceable by the data subject in respect of this right, which fundamentally undermines its practical utility as a consumer protection instrument.

The Law "On Exchange of Credit Information (Credit Histories)" No. ZRU-301 (2011) governs the credit bureau ecosystem and establishes accountability for data inaccuracies in credit files. Yet in the era of alternative-data scoring, the credit file is merely one among thousands of model inputs; the statute's verification and contestation mechanisms cover a rapidly shrinking fraction of the informational substrate upon which modern models operate. The Law "On Consumer Credit" (as amended) mandates disclosure of credit terms and denial reasons, but does not specify the standard of specificity or explainability required where the denial is algorithmically generated. The cumulative effect of these three instruments is a framework that was well-calibrated for the analogue lending era but leaves substantial regulatory gaps in the algorithmic present.

5. REFORM PROPOSALS FOR THE REPUBLIC OF UZBEKISTAN

Based on the foregoing analysis, this article proposes reforms across three complementary dimensions.

Legislative. The most pressing measure is the enactment of a standalone Law on Artificial Intelligence modelled on the EU AI Act's risk-tiered architecture but adapted to Uzbekistan's legal tradition. Such a law should: (i) introduce a risk classification system with credit scoring AI explicitly designated as high-risk; (ii) establish mandatory explainability and documentation obligations for high-risk systems; and (iii) enshrine a right to meaningful human review of algorithmic credit decisions. In parallel, the Civil Code should be amended either by supplementing Article 1006 with a specific provision on AI operator liability or, preferably, by introducing a dedicated chapter on "Liability for Harm Caused by Algorithmic and AI Systems" that operationalises the graduated model proposed above. Article 1012 CC should be expressly extended to cover algorithmic harm as an independent ground for moral damage compensation.

Regulatory. The Central Bank of the Republic of Uzbekistan should issue binding model governance standards

Global Journal of Humanities and Social Sciences
eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

applicable to credit institutions, requiring: a model registry encompassing all AI systems used in credit decisions; Model Cards documenting architecture, training data, known limitations, and fairness metrics; mandatory data drift monitoring using Population Stability Index and Characteristic Stability Index metrics; and a regulatory notification requirement upon detection of anomalous model behaviour. The explainability obligation should be technically operationalised through SHAP (SHapley Additive exPlanations) or LIME outputs attached to each adverse-action notice. Where technically feasible, regulators should create positive incentives for the use of inherently interpretable models — monotonic gradient boosting, scorecard-based ML — for high-stakes credit decisions, heeding Rudin's warning that post-hoc explanation methods provide approximations rather than authentic mathematical insight into model behaviour.

Procedural. Courts adjudicating AI-credit disputes should be empowered to order algorithmic disclosure: upon application, the defendant institution must produce model architecture documentation, feature attribution reports, and fairness performance metrics. A technical court expert — an "algorithmic amicus" — should be available for independent model assessment. The rebuttable presumption of causality, analogous to the AI Liability Directive mechanism, should be codified: where a bank has violated mandatory transparency or explainability standards, the court shall presume — absent affirmative evidence to the contrary — that this violation caused the claimant's harm. Finally, the responsibility chain must be clarified: a bank deploying a third-party AI-as-a-Service model retains full liability toward the consumer, consistent with the Basel Committee's principle that "delegation of technical implementation does not constitute delegation of regulatory responsibility". Internal contractual recourse against the vendor remains available but cannot dilute the consumer's right of action.

6. CONCLUSION

The deployment of AI in credit scoring represents a structural challenge that cannot be neutralised by mapping existing tort norms onto new technological realities. The gap between the mathematical sophistication of modern machine learning systems and the law's requirements of transparency, provability, and fairness is not a temporary feature of an immature technology: it is intrinsic to the probabilistic, high-dimensional character of these systems and will persist absent deliberate legal design.

The comparative record is instructive. Every major legal system examined — the EU, the United States, Singapore, the United Kingdom — is moving, at different speeds and through different mechanisms, toward the same destination: binding ex-ante transparency obligations, systematic fairness auditing, and meaningful individual remedies for algorithmic harm. The common thread across these otherwise divergent regulatory philosophies is the redistribution of the informational burden: from the consumer, who knows nothing about the model, to the operator, who controls it entirely.

For the Republic of Uzbekistan, the path forward is clear in its direction if complex in its execution: a dedicated AI Law with risk-based classification, targeted amendments to the Civil Code extending the graduated liability framework to autonomous algorithmic systems, and a Central Bank model governance regime that transforms abstract transparency principles into technically enforceable obligations. Implemented together, these reforms would position Uzbekistan not merely as a consumer of globally developed AI governance standards, but as a jurisdiction that has thought carefully about the distinctive demands of its own legal tradition and the particular vulnerabilities of its consumer population in the face of an irreversible technological transformation.

REFERENCES

1. Dudchenko, V.Y., & Sadovsky, A.V. (2022). Machine learning in credit scoring: from logistic regression to

eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

ensemble models. Banking, 4, 45–53.

2. Beliard, C. (2025). The Evolution of Cyber Tort Liability: Conceptual Challenges in Algorithm-Induced Harm. Journal of Legal Studies & Digital Age, 1(1).
3. Decree of the President of the Republic of Uzbekistan "On the Strategy for the Development of New Uzbekistan 2022–2026" No. UP-60. (2022). National Database of Legislation (lex.uz).
4. Barocas, S., Hardt, M., & Moritz, H. (2023). Fairness and Machine Learning: Limitations and Opportunities. MIT Press.
5. Wendehorst, C. (2022). Liability for Artificial Intelligence. In Cambridge Handbook of Responsible Artificial Intelligence (pp. 1–25). Cambridge University Press.
6. Selbst, A.D. (2020). Negligence and AI's human users. Boston University Law Review, 100(3), 1315–1376.
7. Li, Y. (2025). The Special Tort Liability Rules for Damage Caused by Artificial Intelligence. Socio-Legal Studies.
8. European Parliament. (2024). Regulation (EU) 2024/1689 on artificial intelligence (EU AI Act). Official Journal of the European Union.
9. European Parliament. (2022). Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). COM/2022/496 final.
10. Floridi, L. (2023). The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford University Press.
11. European Banking Authority. (2020). EBA Report on Big Data and Advanced Analytics. EBA/REP/2020/01.
12. Equal Credit Opportunity Act, 15 U.S.C. § 1691 et seq. (1974).
13. Consumer Financial Protection Bureau. (2022). CFPB Circular 2022-03: Adverse action notification requirements in connection with credit decisions based on complex algorithms.
14. Williams v. Lending Club Corporation, No. 22-cv-04786 (N.D. Cal. 2023).
15. Meyers, S. (2024). Algorithmic Auditing and the Limits of Reactive Regulation. Harvard Law Review, 137(4), 1102–1148.
16. Monetary Authority of Singapore. (2018). Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of AI and Data Analytics in Singapore's Financial Sector.
17. Cheng, A., & Lee, J. (2022). Soft Law and Hard Compliance: Singapore's FEAT Principles in Practice. Asian Journal of Comparative Law, 17(1), 45–68.
18. Financial Conduct Authority. (2023). Consumer Duty: Final Rules and Guidance. FCA PS23/12.
19. Centre for Data Ethics and Innovation. (2023). Review of Bias in Algorithmic Decision-Making. UK Government.
20. Civil Code of the Republic of Uzbekistan. Part Two (1996). Art. 985. National Database of Legislation (lex.uz).
21. Civil Code of the Republic of Uzbekistan. Part Two (1996). Art. 1006. National Database of Legislation (lex.uz).
22. Ismailov, I.A., & Karimov, F.K. (2023). Source of increased danger in the age of AI: expanding the concept.

eISSN: 2957-3602 pISSN: 2957-3599
VOLUME05 ISSUE03
Doi: - https://doi.org/10.55640/gjhss/Volume05Issue03-01
Submission 22-01-2026, Accepted 19-02-2026, Published 13-03-2026 *Page No. 01-08*

Law and Society, 2, 34–41.

23. Wagner, G. (2019). Robot, Inc.: Firming Up Liability Rules for the Internet of Things. Tulane Law Review, 93(4), 1261–1304.

24. Agzamkhodzhaev, A.A. (2022). Problems of applying increased danger liability doctrine to digital systems. Jurist, 1, 12–18.

25. Borger, R. (2023). Categorical Errors in AI Liability: Why Physical Danger Analogies Fail. LSE Law Review, 4, 88–112.

26. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence, 1(5), 206–215.

27. Law of the Republic of Uzbekistan "On Personal Data" No. ZRU-547. (2019). National Database of Legislation (lex.uz).

28. Law of the Republic of Uzbekistan "On Exchange of Credit Information (Credit Histories)" No. ZRU-301. (2011). National Database of Legislation (lex.uz).

29. Law of the Republic of Uzbekistan "On Consumer Credit" (as amended). National Database of Legislation (lex.uz).

30. Basel Committee on Banking Supervision. (2022). Supervisory guidance on the use of machine learning in the credit cycle. Bank for International Settlements.

31. Tadjiev, H. (2025). Some issues of compensation for moral damage caused by vehicles. inLIBRARY Uzbekistan.

32. Usmanov, Sh. (2023). Legal regulation of the digital economy in Uzbekistan. Tashkent: TSUL.

33. Mukhtorov, M. (2024). On the concept of "digital harm" in civil law of the Republic of Uzbekistan. inLIBRARY Uzbekistan.

34. Oksanen, A., et al. (2020). Artificial Intelligence and Civil Liability. European Parliament Policy Department C.