

Artificial Intelligence Governance in the Insurance Market: Legal Risks, Regulatory Challenges and Policyholder Protection

Assistant professor **Maricica TUDOSE**¹

Associate professor **Ion BÎTCĂ**²

Abstract

The rapid development of artificial intelligence in the insurance market is driving a profound transformation of traditional underwriting, pricing, and claims management mechanisms. However, the use of algorithmic systems in these areas raises significant legal and ethical issues, particularly regarding the transparency of automated decisions, the risk of discrimination, and the identification of the party liable for any resulting damages. This article examines the concept of ethical governance of artificial intelligence as applied to the insurance market, from the perspective of insurance law and the protection of the fundamental rights of the insured and the beneficiary. In this context, the main ethical principles with legal relevance – legality, transparency, non-discrimination, accountability, and human oversight – are examined, as well as the regulatory instruments capable of ensuring the responsible use of artificial intelligence. The analysis highlights the limitations of the current legal framework and the need to integrate ethical governance into the regulatory architecture of the insurance sector as a mechanism for preventing contractual imbalances and strengthening trust in digital systems. Finally, proposals are put forward for the development of a legal-ethical governance model tailored to the specific characteristics of the insurance market.

Keywords: artificial intelligence; ethical governance; insurance law; automated decision-making; beneficiary protection; legal liability; Insurtech.

JEL Classification: K24, K32

DOI: 10.62768/PLPA/2026/15/2/11

Please cite this article as:

Tudose, Maricica & Ion Bîtcă, „Artificial Intelligence Governance in the Insurance Market: Legal Risks, Regulatory Challenges and Policyholder Protection”, *Perspectives of Law and Public Administration* 15, no. 2 (June 2026): 358-372.

Article History

Received: 15 January 2026
Revised: 27 April 2026
Accepted: 25 May 2026

1. Introduction

Technological changes over the past few decades have brought about visible transformations in nearly every field, and the insurance market has been no exception.

¹ Maricica Tudose - Danubius International University of Galati, Romania, <https://orcid.org/0009-0007-7929-3692>, maricicatudose@univ-danubius.ro. **Corresponding author.**

² Ion Bîtcă - Moldova State University; Institute for Legal, Political, and Sociological Research. Center for Legal Research, Republic of Moldova, <https://orcid.org/0000-0001-8479-479X>, ionbitcapantelimon@yahoo.es.

If we think about it, we can no longer even conceive of underwriting or risk assessment without the help of increasingly sophisticated IT systems. The integration of artificial intelligence into everything related to claims processing, premium calculation, or even fraud detection has led to the emergence of operational models that, just a few years ago, we might have considered science fiction³.

But, as expected, things aren't all rosy. The use of these complex algorithms raises serious questions, both from a legal and an ethical perspective⁴. Let's take a simple example: a decision made by an automated system can profoundly affect an insured person – whether it's the denial of a claim or the setting of a premium much higher than that of another person. When the algorithm is a black box, when even experts can't explain exactly how it arrived at that result, how can you challenge the decision? How do you know if you were treated fairly?

Therefore, the issue I will examine below is how we might establish a system of ethical governance for artificial intelligence in the insurance sector that considers both the need for innovation and the effective protection of policyholders' rights. I believe this is an important topic precisely because it brings technology face to face with the fundamental values of the law. And perhaps it is precisely this interdisciplinary approach – which combines financial regulations with technology ethics and traditional insurance norms – that can bring something new to the discussion.

2. Conceptual Framework: Artificial Intelligence and the Insurance Market. What We Mean Today by Artificial Intelligence in Insurance

Before we can discuss regulation, it would be helpful to first clarify what we mean when we say, “artificial intelligence”. There are many definitions, but in short, it refers to technologies that enable systems to do things we typically associate with the human mind: learning from examples, making predictions, and making decisions⁵. In insurance, these technologies are used primarily to process vast amounts of data and to build models that anticipate future behaviors.

You've probably heard of that buzzword, Insurtech. Well, it refers exactly to this phenomenon: insurance companies that embrace technology and use machine learning algorithms to optimize their risk assessments and create increasingly personalized products⁶. On paper, it sounds great: companies are more efficient, costs

³ Lukas Lorenz, Judith van Erp, and Albert Meijer, “Machine-Learning Algorithms in Regulatory Practice: Nine Organisational Challenges for Regulatory Agencies,” *Technology and Regulation* (2022): 1–11, <https://doi.org/10.71265/hznjkw26>; Martin Eling, Davide Nuessle, and Julian Staubli, “The Impact of Artificial Intelligence along the Insurance Value Chain and on the Insurability of Risks,” *The Geneva Papers on Risk and Insurance—Issues and Practice* 47 (2022): 205–241, <https://doi.org/10.1057/s41288-020-00201-7>

⁴ Anya E. R. Prince and Daniel Schwarcz, “Proxy Discrimination in the Age of Artificial Intelligence and Big Data,” *Iowa Law Review* 105, no. 3 (2020): 1257–1318, <https://ilr.law.uiowa.edu/print/volume-105-issue-3/proxy-discrimination-in-the-age-of-artificial-intelligence-and-big-data>.

⁵ Virginia Dignum, *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way* (Cham: Springer, 2019), <https://doi.org/10.1007/978-3-030-30371-6>.

⁶ Luciano Floridi et al., “AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks,

go down, and customers receive offers tailored to their actual needs.

However, in addition to the many benefits they offer, there are also several issues stemming primarily from the predictive models used. No matter how advanced these models may be, they are based on a series of statistical correlations that can obscure or even create discrimination⁷. Furthermore, the complexity of the algorithms used is directly proportional to the logic behind the decisions, making it difficult to ensure strict compliance with the law⁸. Given these considerations, there is an urgent need to develop a conceptual framework designed to help us understand and manage these challenges.

3. Ethical Governance of Artificial Intelligence: On Ethical Governance and Its Principles

Let's now talk a little about what ethical governance of artificial intelligence actually means. The term may sound pretentious, but the idea behind it is simple: we need a set of rules, procedures, and mechanisms to ensure that algorithms are developed and used responsibly. In recent years, researchers in the field have reached a consensus on several basic principles without which we cannot speak of the proper use of AI⁹. These are:

- Transparency – understanding how the system works and the criteria it uses to make decisions (for example, if a loan application is rejected, the person affected should be informed of the reasons for the decision; this helps eliminate the risk of abuse, mistrust, and the inability to correct errors).

- Accountability – who is responsible for any errors (in this context, ethical governance requires the existence of mechanisms for legal and professional accountability, such as audits, methods for tracking the traceability of decisions, and the ability to intervene when problems arise).

- Fairness – there should be no discrimination, not even unintentional (for an algorithm to be fair, it must be continuously tested on various groups, and its social impact must be constantly assessed).

- Security – data protection and restrictions on data handling (a system with weak security, especially in the insurance sector, can lead to massive data breaches or intentionally compromised decisions).

- Maintaining human oversight – automated decisions should be reviewed and validated by a person (this is a fundamental principle: AI should assist human staff, not replace them).

These principles are interdependent and work in a complementary manner, each

Principles, and Recommendations,” *Minds and Machines* 28, no. 4 (2018): 689–707, <https://doi.org/10.1007/s11023-018-9482-5>.

⁷ Brent Daniel Mittelstadt et al., “The Ethics of Algorithms: Mapping the Debate,” *Big Data & Society* 3, no. 2 (2016): 1–21, <https://doi.org/10.1177/2053951716679679>.

⁸ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press, 2015).

⁹ Dignum, *Responsible Artificial Intelligence*, 80.

contributing to ensuring consistent ethical governance of artificial intelligence.

If we apply these principles to the insurance industry, we conclude that robust oversight mechanisms are needed for the algorithms used. Companies should have clear internal policies, conduct regular audits of their systems, and assess potential negative effects in advance. It is not enough to simply claim that your algorithm is fair; you must also prove it.

4. The European Legal Architecture for Artificial Intelligence Governance in the Insurance Sector

Ethical governance in the insurance sector cannot be based exclusively on voluntary principles or internal corporate policies. Although ethical standards provide an important normative orientation, their effectiveness depends on their translation into binding legal obligations, supervisory mechanisms, and enforceable rights. Within the European Union, the governance of artificial intelligence in insurance is based on a multilayered regulatory structure combining the Artificial Intelligence Act, data protection law, insurance-sector legislation, consumer protection rules, and requirements concerning operational and technological resilience.

This regulatory architecture reflects the particular position of insurance activities. Insurers do not merely use artificial intelligence to improve internal efficiency. Algorithmic systems may determine whether a person obtains insurance coverage, the amount of the premium, the classification of the insured risk, the conditions of the contract, or the acceptance and value of a claim. Consequently, the use of artificial intelligence may directly affect access to essential services, equality of treatment, privacy, contractual fairness, and the effective exercise of the rights of insured persons and beneficiaries.

4.1. The Artificial Intelligence Act and the Classification of Insurance Systems

Regulation (EU) 2024/1689 establishes a horizontal and risk-based framework for artificial intelligence systems placed on or used within the European Union market. Its relevance to the insurance sector is particularly significant because Annex III, point 5(c), expressly classifies as high-risk those artificial intelligence systems intended to be used for risk assessment and pricing in relation to natural persons in life and health insurance¹⁰.

This classification reflects the potentially serious consequences of algorithmic decisions in these fields. Risk assessment and pricing may determine not only the economic conditions under which insurance is offered, but also whether individuals can obtain meaningful access to protection against health-related, biometric, or mortality

¹⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689, July 12, 2024, annex III, point 5(c), <http://data.europa.eu/eli/reg/2024/1689/oj>.

risks. An apparently neutral model may generate indirect discrimination if it relies on variables that correlate with age, disability, gender, genetic characteristics, socio-economic status, geographical location, or other protected or vulnerable conditions.

The classification must nevertheless be interpreted precisely. The AI Act does not automatically designate every artificial intelligence system used by an insurer as high-risk. Systems used for administrative support, document classification, customer communication, general fraud detection, or certain forms of claims management may fall outside Annex III, depending on their purpose and effects. Such systems remain subject, however, to the general provisions of the AI Act, data protection legislation, insurance regulation, consumer protection law, and the prohibition of discriminatory practices.

Where an insurance undertaking develops an artificial intelligence system itself or places it on the market under its own name, it may assume the obligations of a provider under the AI Act. Where it purchases and uses a system developed by another entity, it will ordinarily act as a deployer. This distinction is important because responsibility cannot be transferred entirely to the technology supplier. An insurer using a third-party algorithm remains responsible for the manner in which the system is integrated into its underwriting, pricing, claims, or customer-management processes.

High-risk systems must comply with requirements concerning risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, and cybersecurity.¹¹ These requirements transform ethical principles into concrete compliance duties. Fairness requires the examination of the quality and representativeness of training, validation, and testing data. Accountability requires technical documentation and traceable logs. Transparency requires sufficient information for insurers to understand the capacities and limitations of the systems they use. Security requires resilience against errors, manipulation, and cyberattacks.

Human oversight is especially important in insurance decisions. It should not be reduced to the formal confirmation of an algorithmic recommendation. The person entrusted with oversight must possess the competence, authority, and practical capacity to understand the system's limitations, identify abnormal outputs, disregard an automated recommendation, reverse a decision, or interrupt the operation of the system. A model in which employees routinely approve algorithmic outputs without substantive verification would not provide meaningful human oversight and could reinforce automation bias.

For systems used in life and health insurance risk assessment and pricing, Article 27 of the AI Act also requires the deployer to perform a fundamental rights impact assessment before the system is first used.¹² The assessment should identify the categories of persons likely to be affected, the specific risks to their rights, the applicable human oversight mechanisms, and the measures available if those risks materialize. In the insurance context, this assessment should examine, *inter alia*, the potential exclusion

¹¹ Regulation (EU) 2024/1689, Articles 9–15 and 26.

¹² Regulation (EU) 2024/1689, Article 27.

of vulnerable persons, discriminatory pricing effects, the use of proxy variables, the consequences of inaccurate health-related predictions, and the accessibility of complaint and review mechanisms.

Article 86 further strengthens the position of affected persons by providing a right to obtain clear and meaningful explanations regarding the role of certain high-risk AI systems in individual decision-making and the principal elements of the decision.¹³

In practice, an insurer should therefore be able to explain why an algorithm contributed to a higher premium, an unfavourable risk classification, or another decision producing legal or similarly significant effects. Merely stating that the result was generated by a proprietary model cannot satisfy the requirements of meaningful explanation.

4.2. Data Protection, Profiling, and Automated Insurance Decisions

The use of artificial intelligence in insurance is inseparable from the processing of personal data. Insurance models may rely on financial information, medical records, lifestyle data, online behaviour, geolocation, data generated by connected devices, driving behaviour, or information collected through wearable technologies. Some of these categories, particularly health and biometric data, are subject to enhanced protection under Regulation (EU) 2016/679.

The GDPR requires personal data to be processed lawfully, fairly, and transparently, for specified purposes and in a manner limited to what is necessary. Data must also be accurate, securely stored, and retained only for the period required by the relevant purpose. These principles are directly relevant to artificial intelligence because the accuracy and legality of algorithmic outputs depend on the provenance, quality, relevance, and representativeness of the underlying data.¹⁴

The fact that data are technically accessible does not mean that they may lawfully be used for underwriting or pricing. Insurers must establish an appropriate legal basis for processing and, where special categories of data are involved, satisfy the additional conditions imposed by Article 9 GDPR. Consent should not be treated as a universal solution, particularly where the contractual position of the individual creates an imbalance or where refusal would effectively prevent access to an insurance product. Article 22 GDPR addresses decisions based solely on automated processing, including profiling, that produce legal effects or similarly significantly affect an individual. An automated refusal to conclude an insurance contract, the determination of a substantially higher premium, or the rejection of an important claim may fall within this framework when the decision is made without meaningful human participation.

Even where automated decision-making is permitted because it is necessary for entering into or performing a contract, is authorised by law, or is based on explicit

¹³ Regulation (EU) 2024/1689, Article 86.

¹⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, May 4, 2016, 1–88, arts. 5, 6, 9, 13–15, 22, and 35, <http://data.europa.eu/eli/reg/2016/679/oj>.

consent, appropriate safeguards remain necessary. These safeguards include the possibility of obtaining human intervention, expressing one's point of view, and contesting the decision. Human review must be genuine. The reviewer should examine the relevant evidence, assess the appropriateness of the model's output in the individual case, and possess the authority to modify the initial result.

The transparency duties under Articles 13–15 GDPR also require meaningful information about the logic involved in automated processing, together with the significance and foreseeable consequences of such processing. This does not necessarily require disclosure of source code or commercially sensitive mathematical details. It does, however, require information that enables the insured person to understand the principal factors influencing the decision, the manner in which those factors affected the outcome, and the available means of contesting it.

A data protection impact assessment under Article 35 GDPR may also be required when artificial intelligence entails systematic profiling, large-scale processing of sensitive data, or other processing likely to result in a high risk to individual rights and freedoms. In cases involving high-risk insurance systems, the data protection impact assessment and the fundamental rights impact assessment required by the AI Act should be coordinated rather than conducted as unrelated formal exercises. The former focuses primarily on risks arising from personal-data processing, while the latter addresses the broader effects of the system on equality, access to services, contractual fairness, and other fundamental rights.

4.3. Insurance Regulation, Consumer Protection, and Supervisory Responsibility

The Artificial Intelligence Act and the GDPR operate alongside the sector-specific rules applicable to insurance undertakings and distributors. Directive (EU) 2016/97 on insurance distribution requires distributors to act honestly, fairly, and professionally in accordance with the best interests of their customers. It also requires insurance products to correspond to the customer's demands and needs.¹⁵

The use of artificial intelligence does not displace these obligations. An insurer or intermediary cannot justify an unsuitable recommendation, unfair product differentiation, or deficient information by relying on the output of an algorithm. Where artificial intelligence is used to personalise insurance offers or recommend products, the system must be designed and monitored in a manner consistent with the customer's actual needs and interests.

Product oversight and governance requirements are equally relevant. Insurance products must be designed for an identified target market, tested before distribution, and periodically reviewed. Algorithmic systems used to define target markets or distribute products may narrow access in ways that were not initially apparent. Continuous

¹⁵ Directive (EU) 2016/97 of the European Parliament and of the Council of January 20, 2016, on insurance distribution (recast), OJ L 26, February 2, 2016, 19–59, arts. 17 and 20, <http://data.europa.eu/eli/dir/2016/97/oj>.

monitoring is therefore necessary to determine whether a model produces systematic exclusion, excessive premiums, or unsuitable product recommendations for particular categories of customers.¹⁶

The governance framework established by Directive 2009/138/EC, commonly known as Solvency II, also requires insurance undertakings to maintain effective systems of governance, risk management, internal control, and oversight of outsourced activities.¹⁷ These obligations extend to technological systems that materially affect underwriting, pricing, claims management, or compliance. The management body of an insurer remains ultimately responsible for the use of artificial intelligence, even where development, hosting, data processing, or model maintenance is outsourced.

This principle is particularly important when insurers rely on external Insurtech companies, cloud providers, or general-purpose artificial intelligence models. Contractual outsourcing cannot eliminate regulatory responsibility. Insurance undertakings should retain access to documentation, audit rights, information concerning model changes, incident-reporting mechanisms, and the technical capacity necessary to evaluate the provider's compliance.

Regulation (EU) 2022/2554 on digital operational resilience complements these requirements by imposing rules concerning information and communication technology risk, incident management, resilience testing, and third-party service providers.¹⁸ An artificial intelligence system may be ethically designed yet still create substantial risks if it is vulnerable to data corruption, cyberattacks, unauthorised access, model manipulation, or operational failure. Ethical governance must therefore include technological resilience and continuity, not merely fairness and transparency.

The European Insurance and Occupational Pensions Authority has also identified governance principles for trustworthy artificial intelligence in insurance, including proportionality, fairness and non-discrimination, transparency and explainability, human oversight, data governance and record-keeping, and robustness and performance.¹⁹ These principles are particularly valuable because they translate general ethical requirements into the operational context of insurance undertakings.

The coexistence of several regulatory regimes nevertheless creates a risk of fragmented supervision. An AI-based insurance system may simultaneously fall within

¹⁶ Commission Delegated Regulation (EU) 2017/2358 of September 21, 2017, supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors, OJ L 341, December 20, 2017, 1–7, http://data.europa.eu/eli/reg_del/2017/2358/oj.

¹⁷ Directive 2009/138/EC of the European Parliament and of the Council of November 25, 2009, on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (recast), OJ L 335, December 17, 2009, 1–155, arts. 41, 44, and 49, <http://data.europa.eu/eli/dir/2009/138/oj>.

¹⁸ Regulation (EU) 2022/2554 of the European Parliament and of the Council of December 14, 2022, on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014, and (EU) 2016/1011, OJ L 333, December 27, 2022, 1–79, <http://data.europa.eu/eli/reg/2022/2554/oj>.

¹⁹ European Insurance and Occupational Pensions Authority, *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector* (June 17, 2021), https://www.eiopa.europa.eu/publications/artificial-intelligence-governance-principles-towards-ethical-and-trustworthy-artificial_en.

the competence of an insurance supervisory authority, a data protection authority, and an AI market-surveillance authority. Effective enforcement therefore requires institutional cooperation, information exchange, coordinated inspections, and clear rules for determining which authority should lead investigations involving overlapping legal issues.

4.4. Towards an Integrated Compliance Model for Insurers

A coherent governance model should integrate ethical principles and legal obligations throughout the entire lifecycle of an artificial intelligence system. At a minimum, an insurance undertaking should establish the following mechanisms:

First, the undertaking should maintain a comprehensive inventory of the artificial intelligence systems it develops or uses. Each system should be classified according to its purpose, the persons affected, the categories of data processed, its degree of autonomy, and its potential legal and fundamental-rights effects.

Second, ex ante assessments should be conducted before deployment. Depending on the system, these may include a data protection impact assessment, a fundamental rights impact assessment, a product-governance assessment, and an evaluation of operational and cybersecurity risks. These assessments should be coordinated and approved at an appropriate level of management.

Third, insurers should implement data-governance and fairness-testing procedures. The datasets used to train and operate the system should be examined for accuracy, representativeness, historical bias, and the use of proxy variables. The performance of the system should be tested across relevant demographic and social groups, and significant disparities should trigger corrective measures. Such statistical testing should not, however, be treated as a complete substitute for the contextual legal assessment required under non-discrimination law²⁰.

Fourth, explanations should be designed from the perspective of the policyholder. Information should identify the principal factors affecting a decision and should be sufficiently clear to permit meaningful contestation. A general reference to statistical risk or proprietary technology is not enough.

Fifth, human-review mechanisms should be accessible, independent, and effective. Reviewers should have sufficient expertise and authority to depart from the automated result. Decisions involving the refusal of coverage, significant premium increases, or the rejection of substantial claims should receive enhanced human scrutiny. Sixth, insurers should establish continuing monitoring, logging, audit, and incident-reporting mechanisms. Governance should not end when the system is placed into operation. Models may deteriorate, datasets may change, and previously neutral variables may acquire discriminatory effects over time.

Finally, affected persons must have access to effective complaint and redress

²⁰ Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI," *Computer Law & Security Review* 41 (2021): 105567, <https://doi.org/10.1016/j.clsr.2021.105567>.

mechanisms. The insurer should provide a clear channel for challenging automated decisions and should preserve the records required to reconstruct the decision-making process. Supervisory authorities should also possess the technical expertise and legal powers necessary to investigate the system rather than relying exclusively on the insurer's own description.

Accordingly, ethical governance should be understood as an integrated legal and institutional process rather than as a collection of abstract values. Its purpose is to ensure that artificial intelligence remains subordinate to the insurer's legal obligations and to the rights of policyholders and beneficiaries. The use of technology may support risk assessment and improve efficiency, but it cannot replace legal responsibility, individualised assessment, or effective human judgment.

5. Legal Risks Arising from the Use of Artificial Intelligence in the Insurance Market. What Legal Risks Arise in Practice

Now let's see what could go wrong. Because, unfortunately, there are quite a few potential problems.

Probably the most talked-about issue is algorithmic discrimination. And I'm not referring to someone intentionally programming an algorithm to be racist or sexist. Often, the problem is much more subtle. The algorithm learns from existing data, and that data may already contain biases²¹. Or it may use variables that, while not explicitly prohibited, strongly correlate with sensitive characteristics – such as gender, ethnicity, or religion²². The result? People in certain categories end up being treated differently, without any objective justification.

Then there is the issue of a lack of transparency. Complex algorithms, especially those based on deep neural networks, are notoriously difficult to interpret. You may have the result but be unable to explain how it was achieved. Yet, in law, the principle of providing reasons for decisions is fundamental. If you cannot tell someone why their claim for compensation was rejected, how can they be considered to have been properly informed?²³

Finally, there is the thorny question of liability. When an algorithm makes a mistake and someone suffers as a result, who pays?²⁴ The insurance company that used it? The firm that developed the software? The team that trained the model? The programmer who wrote a line of faulty code? The answer is far from simple, and current legislation – designed for a world where decisions were made solely by humans – does not offer clear solutions.

²¹ Mittelstadt et al., "Ethics of Algorithms," 15.

²² Pasquale, *The Black Box Society*, 27; Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," *California Law Review* 104, no. 3 (2016): 671–732, <https://doi.org/10.15779/Z38BG31>.

²³ Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law* 7, no. 2 (2017): 76–99, <https://doi.org/10.1093/idpl/ixp005>.

²⁴ Prince and Schwarcz, "Proxy Discrimination," 1260.

6. Legal Protection Mechanisms. How Can We Better Protect Policyholders?

In the face of these risks, we cannot sit idly by. We need legal tools that are adapted to the realities of technology. And here I would like to mention a few areas that I consider essential.

First and foremost, the requirement for algorithmic transparency. It's not enough to simply say, "The system decided". You must be able to provide an explanation that the average person can understand²⁵. Of course, there's no need to explain every single mathematical operation, but at the very least, the general criteria and basic logic should be accessible.

Next, the right to human intervention and appeal. Anyone affected by an automated decision should be able to request that their case be reviewed by a human. And not just as a formality, but in earnest – meaning that person should have the authority to change the decision, if necessary, not just go through the motions.

Last but not least, algorithmic auditing. I think it's an excellent idea for the algorithms used to be periodically reviewed by independent experts who can identify potential biases, errors, or legal violations²⁶.

In this context, insurance market supervisory authorities should adopt a proactive and preventive approach, engaging in the continuous monitoring and periodic evaluation of algorithmic systems through audit and control mechanisms, rather than limiting their intervention to situations where malfunctions or violations of the legal framework have already been identified²⁷.

7. Policy Recommendations. What Could Be Done at the Legislative Level

Beyond best practices, I believe legislative action is also needed. Because, let's be honest, companies won't always do the right thing voluntarily, especially if it involves additional costs.

A first step could be to require an algorithmic impact assessment before any artificial intelligence system is put into operation in the insurance sector. This would be like the privacy impact assessments already in place under data protection regulations. In practice, the company would have to demonstrate that it has analyzed the potential risks and taken steps to prevent them.

Next, it would be helpful to establish minimum transparency standards. What does it mean for an algorithm to be explainable? What level of detail should be provided to policyholders? How often should the tests be repeated? All these issues could be clarified through guidelines or even regulations.

And, of course, supervisory authorities should be given both the authority and

²⁵ Wachter, Mittelstadt, and Floridi, "Why a Right to Explanation," 78.

²⁶ Cary Coglianese and David Lehr, "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era," *Georgetown Law Journal* 105 (2017): 1147–1223.

²⁷ Joshua A. Kroll et al., "Accountable Algorithms," *University of Pennsylvania Law Review* 165, no. 3 (2017): 633–705, <https://pennlawreview.com/2017/02/23/accountable-algorithms/>.

the resources to effectively monitor this sector. You can't regulate something you don't understand, so these institutions need to have technology experts on staff.

8. Conclusion

Artificial intelligence is becoming an integral component of contemporary insurance activities, transforming underwriting, risk assessment, premium calculation, product distribution, fraud detection, and claims management²⁸. These technologies can improve operational efficiency, facilitate more accurate risk evaluation, reduce administrative costs, and support the development of personalised insurance products. Nevertheless, the same capabilities may also intensify existing contractual and informational imbalances between insurance undertakings and policyholders. When algorithmic systems influence access to coverage, determine premiums, or contribute to the rejection of claims, their use can directly affect individual rights, economic interests, and access to essential forms of financial protection.

The analysis undertaken in this article demonstrates that the governance of artificial intelligence in insurance cannot be reduced to the voluntary application of abstract ethical principles. Transparency, fairness, accountability, security, and human oversight acquire practical significance only when they are translated into binding legal duties, internal governance structures, supervisory competences, and effective remedies. Ethical governance should therefore be understood as a legally structured and institutionally enforceable process that applies throughout the entire lifecycle of an artificial intelligence system.

The European regulatory framework provides the foundations for such an approach. The Artificial Intelligence Act introduces a risk-based system and subjects certain AI applications used in life and health insurance risk assessment and pricing to the legal regime governing high-risk systems. The GDPR complements this framework by regulating profiling, automated decision-making, sensitive personal data, transparency, and data protection impact assessments. At the same time, insurance-sector legislation requires undertakings and intermediaries to act honestly, fairly, and professionally in the best interests of customers, while Solvency II and the Digital Operational Resilience Act reinforce governance, risk-management, outsourcing, cybersecurity, and operational-continuity obligations.

The coexistence of these instruments nevertheless creates a complex and potentially fragmented regulatory environment. A single algorithmic system may simultaneously fall within the competence of insurance supervisors, data protection authorities, and AI market-surveillance authorities. Effective protection therefore depends not only on the existence of legal rules but also on institutional coordination, exchange of technical information, coordinated inspections, and the development of specialist expertise within supervisory bodies. Authorities must be capable of

²⁸ Lázaro Cuesta Barberá, "Artificial Intelligence and the Insurance Industry: Regulatory and Market Perspectives," *Consorcio de Compensación de Seguros* (2024), <https://www.consorsegurosdigital.com/almacen/pdf/artificial-intelligence-and-the-insurance-industry-regulatory-and-market-perspectives.pdf>.

independently examining the design, data sources, performance, and effects of algorithmic models rather than relying exclusively on information supplied by insurers or technology providers.

The responsibility of insurance undertakings remains central. An insurer cannot avoid accountability by arguing that an automated decision was generated by software developed by an external provider. The undertaking that integrates an AI system into underwriting, pricing, distribution, or claims management remains responsible for ensuring that the system complies with applicable legal standards. Outsourcing arrangements should therefore guarantee access to technical documentation, audit rights, incident-reporting procedures, information concerning model modifications, and the possibility of effective intervention where risks are identified.

A coherent internal governance model should include an inventory and legal classification of AI systems, coordinated impact assessments, appropriate data-governance procedures, regular testing for discriminatory outcomes, detailed record-keeping, independent algorithmic audits, and continuous monitoring after deployment. Particular attention should be paid to proxy variables capable of reproducing discrimination indirectly, as well as to changes in datasets or market conditions that may cause a previously acceptable model to produce unfair or inaccurate results.

Meaningful transparency and human oversight are essential components of this governance structure. Policyholders should receive intelligible information concerning the principal factors that influenced an automated decision and the practical consequences of the use of artificial intelligence. Transparency does not necessarily require disclosure of source code or proprietary mathematical formulas, but it must enable affected persons to understand and contest decisions. Similarly, human intervention must not become a merely formal confirmation of algorithmic outputs. Reviewers must possess the necessary competence, independence, information, and authority to reconsider and, where appropriate, reverse the automated result.

The protection of policyholders also requires accessible complaint and redress mechanisms. Individuals affected by the refusal of coverage, an excessive premium, an unfavourable risk classification, or the rejection of a claim should be able to request substantive human review and obtain a reasoned response. The insurer must preserve sufficient records to reconstruct the decision-making process, while supervisory and judicial authorities must be able to examine whether the algorithmic outcome complied with legal requirements.

Ultimately, artificial intelligence should remain an instrument supporting insurance decision-making rather than an autonomous substitute for legal responsibility and professional judgment. Innovation and policyholder protection are not necessarily conflicting objectives. A predictable and coherent governance framework can promote technological development while strengthening trust, contractual fairness, and legal certainty. The principal regulatory challenge is therefore not to prevent the use of artificial intelligence in insurance, but to ensure that its development and deployment remain subordinate to fundamental rights, consumer interests, sector-specific obligations, and effective public supervision. Only under these conditions can artificial intelligence contribute to a more efficient insurance market without undermining

equality, accountability, and confidence in the institutions responsible for providing financial protection.

Bibliography

1. Barocas, Solon, and Andrew D. Selbst. "Big Data's Disparate Impact." *California Law Review* 104, no. 3 (2016): 671–732. <https://doi.org/10.15779/Z38BG31>.
2. Coglianese, Cary, and David Lehr. "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era." *Georgetown Law Journal* 105 (2017): 1147–1223.
3. Commission Delegated Regulation (EU) 2017/2358 of September 21, 2017, supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors. OJ L 341, December 20, 2017, 1–7. http://data.europa.eu/eli/reg_del/2017/2358/oj.
4. Cuesta Barberá, Lázaro. "Artificial Intelligence and the Insurance Industry: Regulatory and Market Perspectives." *Consortseguros Digital*, 2024. <https://www.consortsegurosdigital.com/almacen/pdf/artificial-intelligence-and-the-insurance-industry-regulatory-and-market-perspectives.pdf>.
5. Dignum, Virginia. *Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way*. Cham: Springer, 2019. <https://doi.org/10.1007/978-3-030-30371-6>.
6. Directive 2009/138/EC of the European Parliament and of the Council of November 25, 2009, on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II) (recast). OJ L 335, December 17, 2009, 1–155. <http://data.europa.eu/eli/dir/2009/138/oj>.
7. Directive (EU) 2016/97 of the European Parliament and of the Council of January 20, 2016, on insurance distribution (recast). OJ L 26, February 2, 2016, 19–59. <http://data.europa.eu/eli/dir/2016/97/oj>.
8. Eling, Martin, Davide Nüesle, and Julian Staubli. "The Impact of Artificial Intelligence along the Insurance Value Chain and on the Insurability of Risks." *The Geneva Papers on Risk and Insurance—Issues and Practice* 47 (2022): 205–241. <https://doi.org/10.1057/s41288-020-00201-7>.
9. European Insurance and Occupational Pensions Authority. *Artificial Intelligence Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector*. June 17, 2021. https://www.eiopa.europa.eu/publications/artificial-intelligence-governance-principles-towards-ethical-and-trustworthy-artificial_en.
10. Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge, et al. "AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations." *Minds and Machines* 28, no. 4 (2018): 689–707. <https://doi.org/10.1007/s11023-018-9482-5>.
11. Kroll, Joshua A., Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. "Accountable Algorithms." *University of Pennsylvania Law Review* 165, no. 3 (2017): 633–705. <https://pennlawreview.com/2017/02/23/accountable-algorithms/>.
12. Lorenz, Lukas, Judith van Erp, and Albert Meijer. "Machine-Learning Algorithms in Regulatory Practice: Nine Organisational Challenges for Regulatory Agencies." *Technology and Regulation* (2022): 1–11. <https://doi.org/10.71265/hznjkw26>.

13. Mittelstadt, Brent Daniel, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. "The Ethics of Algorithms: Mapping the Debate." *Big Data & Society* 3, no. 2 (2016): 1–21. <https://doi.org/10.1177/2053951716679679>.
14. Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.
15. Prince, Anya E. R., and Daniel Schwarcz. "Proxy Discrimination in the Age of Artificial Intelligence and Big Data." *Iowa Law Review* 105, no. 3 (2020): 1257–1318. <https://ilr.law.uiowa.edu/print/volume-105-issue-3/proxy-discrimination-in-the-age-of-artificial-intelligence-and-big-data>.
16. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, May 4, 2016, 1–88. <http://data.europa.eu/eli/reg/2016/679/oj>.
17. Regulation (EU) 2022/2554 of the European Parliament and of the Council of December 14, 2022, on digital operational resilience for the financial sector and amending Regulations (EC) No. 1060/2009, (EU) No. 648/2012, (EU) No. 600/2014, (EU) No. 909/2014, and (EU) 2016/1011. OJ L 333, December 27, 2022, 1–79. <http://data.europa.eu/eli/reg/2022/2554/oj>.
18. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). OJ L 2024/1689, July 12, 2024. <http://data.europa.eu/eli/reg/2024/1689/oj>.
19. Wachter, Sandra, Brent Mittelstadt, and Chris Russell. "Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI." *Computer Law & Security Review* 41 (2021): 105567. <https://doi.org/10.1016/j.clsr.2021.105567>.
20. Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law* 7, no. 2 (2017): 76–99. <https://doi.org/10.1093/idpl/ix005>.