Pellini N., 'Insurance, New Technologies, and Data: Challenges and Opportunities' (2026) 1 EJPLT.
DOI: https://doi.org/10.57230/EJPLT261NP

EJPLT
ISSN 2704-8012



Insurance, New Technologies, and Data: Challenges and Opportunities

Assicurazione, nuove tecnologie e dati: sfide ed opportunità

NICCOLÒ PELLINI
PhD Student in Economic Law
University of Florence

Abstract

This paper analyzes and addresses the challenges and opportunities presented by algorithmic profiling systems in the insurance sector, with a particular focus on the processing of policyholders' personal data. After reviewing the most significant regulatory measures, recent developments in case law, and certain compliance aspects of the insurance industry, the paper focuses on the phenomenon of automated decision-making processes and the related protection of policyholders through 'intelligible' information.

Il presente contributo analizza ed affronta sfide e opportunità del dei sistemi di profilazione algoritmica in ambito assicurativo, con particolare interesse rispetto al trattamento dei dati personali degli assicurati. Dopo aver passato in rassegna gli interventi normativi di maggiore rilevanza, i recenti sviluppi giurisprudenziali ed alcuni profili di compliance nell'attività assicurativa, il paper si concentra sul fenomeno dei processi decisionali automatizzati e la relativa tutela dell'assicurato attraverso un'informazione "intelligibile".

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Insurance; law; automated decision-making processes; GDPR; AI ACT.

Summary: 1. Introduction and state of the art – 2. The 'problem' of algorithmic profiling – 3. European legislation – 4. The insurance sector – 5. Conclusions.

1. Introduction and state of the art**

Insurance contract has undergone a process of evolution, metamorphosis and adaptation strongly influenced by the - initially growing, now relentless - advance of technology, which in itself heralds new risks to be insured, managed and compensated for through insurance techniques[1].

Within these dynamics, between a regulated market and technical-scientific progress, the figure 'seeking' effective safeguards, particularly in terms of information and transparency, is therefore clearly identifiable as the policyholder[2] .

Indeed, whilst it is true that in the relationship between insurer and insured, it has always been the latter who could decide whether and on what terms to provide the former with all the information in their possession regarding the risk to be insured – whilst insurers ended up being *'innocent victims of their own good faith'* who *'committed themselves to this contract so to speak blindly'*[3] – nowadays, it is the insurance companies that have at their disposal methods, tools and data[4] which place them at an advantage, capable even of overturning and subverting the typical concept of information asymmetry.

The insurance sector, too, is navigating the transition from analogue to digital operations, facing a number of challenges, *both* in terms of bringing companies' internal *compliance systems* into line with the regulations

**La presente pubblicazione è stata realizzata con il cofinanziamento dell'Unione europea – Next Generation EU, nell'ambito del progetto di ricerca di rilevante interesse nazionale, bando PRIN 2022 – prot. 2022W2Y8ES - CUP J53D23005970006, '*Insurtech e sostenibilità. Per un'evoluzione sostenibile, nell'uso della tecnologia e nel ruolo dell'informazione, nelle assicurazioni*'.

[1] For an account of the history of insurance, see A La Torre, *L'assicurazione nella storia delle idee* (2nd ed., Giuffré Milano 2000); M Rossetti, *Diritto delle assicurazioni* (1st ed., Padova 2011); A Donati, *Tratt. dir. ass.* (vol I, Milano 1952); F Melis, *Origini e sviluppi delle assicurazioni in Italia: secoli XIV-XVI* (Roma 1975); WR Vance, *Handbook on the law of insurance* (St. Paul 1904).

[2] The protection of the insured is an issue that highlights the strongly international nature of insurance contracts. Indeed, wherever an insurance contract is entered into, the need to protect the weaker party – subject to the specific legal frameworks of each state and system – remains the same. In this case, it is the phenomenon of the use of new technologies against which we must assess whether the scope of the protection afforded to the insured, as conceived by national and supranational legislators, can be considered a valid safeguard against abuses by the contracting party.

[3] A Baldasseroni, *Delle assicurazioni marittime* (Firenze 1786) 18. B McGurk, '21: Data: The growth of risk-related data in insurance and protecting privacy' in *Research Handbook on International Insurance Law and Regulation* (Cheltenham 2023) 590.

[4] See M Rabitti, 'Credit scoring via machine learning e prestito responsabile' (2023) Riv. dir. banc., 175

introduced as a result of digitalisation (e.g. GDPR[5] , DORA[6] , NIS2[7] etc.), where the sector often seems to have found itself *'playing catch-up with scientific discoveries'*[8] , and in terms of the safeguards to be put in place to protect end consumers grappling with the new digitalised market[9] .

With this in mind, the insurance industry has adopted a varied approach, gradually engaging with the *disruptive* innovations offered by new technologies. However, the digital transformation/transition initially focused on products (with a growing element of digital integration in customer relations and the management of insurance contracts), before subsequently moving on – thanks to in-house development or through the integration of innovative *start-ups* via acquisitions – to technologies supporting *governance*, production, *risk assessment*, *pricing* and the distribution of insurance products on the market[10] .

Consequently, to date, companies have invested substantial resources in enhancing innovative technologies to expand their potential and explore new commercial opportunities, such as identifying new products and improving those already on the market, as well as to manage the stages of insurance

---

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1 (GDPR).

[6] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L333/1.

[7] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union [2022] OJ L333/80.

[8] To quote G. Alpa, 'Fintech: un laboratorio per i giuristi', (2019), 2, Contr. e Impr., 377 ff.

[9] The intersection between insurance and technology has given rise to the term 'InsurTech', now widely used in practice and derived from the combination of the English terms 'insurance' and 'technology'. On this subject, see most recently S. Landini, *Insurance Law, Insurance Contract, Insurance Business*, (2026 Naples), 127; A. J. Pagano, A. Cappiello, E. Vannucci, and C. D'Elia, 'InsurTech Integration: Reshaping the Insurance Value Chain in the Digital Age', (2024), American Journal of Economics and Business Administration, 46 ff.; S. Landini, 'Insurtech: innovation in production, distribution, governance, and supervision in the insurance market' (2021), Assicurazioni, 3, 434; M. T. Paracampo, 'InsurTech e l'applicazione delle tecnologie nel settore assicurativo' in *FINTECH. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari* (Torino 2021) 259 ff.

[10] *'Where traditional banking practices have been challenged by the advent of digital platforms, mobile banking apps, and innovative payment solutions'*. Thus, A. J. Pagano, A. Cappiello, E. Vannucci, and C. D'Elia, 'InsurTech Integration', (9) 46. See also S. Landini, 'Insurtech: innovation in production', (9) 434; P. Marano, M. Siri, *Regulating Insurtech in the European Union*, 2021, available at the link https://www.um.edu.mt/library/oar/bitstream/123456789/109656/1/Regulating_insurtech_in_the_European_Union%282021%29.pdf. This is a relatively recent phenomenon. *The European Insurance and Occupational Pensions Authority* (hereinafter referred to more briefly as 'EIOPA') has, for example, only begun to address the issue comprehensively in recent years. It was 'only' in 2019 that the first proper report in which EIOPA addressed the InsurTech phenomenon was published, stating*: 'InsurTech has an impact across all steps of the value chain in the insurance and pension sectors, including through the emergence of start-ups, often in cooperation agreements with incumbent undertakings. The business models of undertakings and the consumer experience are being transformed because of the proliferation of financial innovations and technology. Based on the evidence gathered, the EU InsurTech market is at an early stage but evolving.'* Subsequently, in 2021, EIOPA also established an expert advisory group on digital ethics in the insurance sector, which concluded its mandate with the publication of a report on AI governance principles. Furthermore, in 2023, EIOPA published a survey on the monitoring of the digitalisation market to gather further empirical data on the progress of digitalisation in the European insurance sector and to keep pace with the rapid changes that innovation brings to the insurance sector. For an up-to-date overview of technological developments in the insurance sector, EIOPA has published the *Report on the digitalisation of the European insurance sector*, which states that *'EIOPA will continue to promote the financial inclusion of vulnerable customers, customer protection and the ethical use of data, including in relation to AI and digitalisation*'.

premium quotation, claims settlement, risk underwriting, fraud investigation and product distribution[11] .

The key stages of the insurance business where the most significant risks to the protection of policyholders' rights are evident are those relating to customer profiling, which aims to assess policyholders' risks with greater accuracy in order to calculate the amount of premiums due and determine the other terms of the contract at the time of signing[12] . We are, in fact, witnessing a shift in *the modus operandi* regarding the processing of policyholders' personal data and the emergence of new methods of *risk profiling* through, for example, automated processing, with potential risks and issues regarding the protection of data subjects. Reference is made to risks such as unfair pricing conditions or the exclusion of categories of potential policyholders who are marginalised due to *both biases* in the automated algorithms used for profiling and programming logic that fails to respect the rights and freedoms of data subjects.

There remains a degree of opacity and uncertainty regarding the protection of the insured person concerned in relation to: - the processing of their personal data, particularly where automated decision-making processes are used (unmonitored entities such as credit rating agencies and credit scoring firms that make decisions); a problem regarding the legal bases used by insurance companies – particularly in relation to data processing under Article 9 of the GDPR; a problem of discrimination and exclusion, particularly based on automated decision-making processes and data processing under Article 9.

2. The 'problem' of algorithmic profiling

In a market characterised by a constantly shifting balance of power among its key players, one of the phenomena that has radically altered the *modus operandi* of *the* major *players* in the insurance sector in recent years is undoubtedly the increasing use of so-called algorithmic profiling through, precisely, algorithms that perform fully automated processing and which, through decisions based solely on automated decision-making processes, have legally significant consequences for the data subject[13] . What is most significant in the insurance sector is the processing of data (particularly personal data, but not exclusively) relating to the policyholder in order to create risk profiles and *clusters*, which serve to carry out *risk pooling* that makes the decision to offer (and under what terms) or not to offer insurance cover as granular as possible,

[11] S. Landini, 'Insurtech: innovation in production', (9) passim. On this subject, see also E. Battelli, 'Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi', (2019), 12 Corr. Giur., 1522 ff., as well as Id., 'Insurtech' ed evoluzione dell'offerta di polizze sanitarie', (2022) 1, Contr. e impr. I, 52 ff.

[12] E. Giorgini, 'Profilazione automatizzata e contratto assicurativo', (2024) 4, Assicurazioni, 754.

[13] *'Referring in this sense to the phenomenon in terms of the introduction of a series of protocols based on rules pre-established by the programmer (or developed by the software itself) in order to produce a desired outcome (…) the specific characteristics of this process are far from allowing us to reduce the whole of these innovations to a single category: certainly, a common element can be found in the use of non-linear computational algorithms, capable of identifying unknown causal relationships to be traced back to systems of linear equations in order to incrementally develop evaluative heuristics through the comparison and integration of new information within the pre-established set of rules and by refining their evaluative capacity through training.*' The definition is given in these terms by A. Davola, *Algoritmi decisionali e trasparenza bancaria*, (Milan, 2020) in the introduction, XVI.

thereby optimising the *business* decisions of insurance companies. The latter is the starting point, as well as the primary activity, for insurance companies and serves as a guide for placing an individual within a specific *pool* of homogeneous risks, in which groups of customers with similar risk profiles are grouped together and attributed to the same risk class[14] . This entails various implications regarding the protection of the insured person's personal data in the context of their subjection to such automated processing and decision-making processes, as well as with regard to discrimination or exclusion of so-called individuals deemed structurally 'uninsurable' (on grounds of health, ethnic origin, gender, etc.)[15] .

This is, in fact, outright discrimination (to be understood as an insurance technique aimed at distinguishing risk at the outset, quantifying the premium in relation to the level of risk of the individual policyholder, which is then distributed amongst the body of policyholders[16]) following *'scoring'* processes carried out by insurance companies, with consequences that in some (extreme) cases affect the fundamental rights and freedoms of policyholders[17] .

Algorithmic *scoring* has come to the fore, in particular, in the banking sector, where *credit scoring* has taken on independent significance following a paradigm shift in the market, in which the activity of granting credit has come to regard the assessment of so-called 'creditworthiness' as its essential prerogative[18]. From this perspective, technological acceleration has led, in both the banking and insurance sectors, to the increasingly widespread use of systems (whether mere predictive algorithms or full-fledged artificial intelligence systems [19]) designed to generate 'scores' [20] based on the processing of the personal data of the credit applicant (or, for the purposes of this research, the insured person)[21] .

Similarly, in the insurance sector, the use of such automated decision-making processes highlights the need for *specific* safeguards for the insured person.

---

[14] U. Malvagna, 'Intelligenza artificiale e polizze long-term care: tra personalizzazione del rischio ed esclusione sociale'' (2026), 1, Dialoghi di diritto dell'economia, 91.

[15] In such cases, the term *'machine bias'* is used, meaning *'natural consequences arising from the use of large statistical* datasets *which, if not properly cleaned, reflect – and thus incorporate – social injustices and discriminatory dynamics already present in the social fabric that produced them'*; these include various types: *incorrect labelling*, *sampling bias*, *proxy discrimination*, *and ad hoc groups*. See E. Pelino, *Art. 22 GDPR* in L. Bolognini and E. Pelino (eds.) *Codice della disciplina privacy*, (Milan, 2024) 160. On this subject, see also J. Knetsch, 'Data Protection Rights and Automated Decision-Making in the Field of Insurance', in C. Poncibò and P. Tereszkiewicz (eds.), *European Insurance Law within the Digital Age* (Cham, 2025), 167 ff.

[16] S. Landini, 'Assicurazioni e salute' in F Capriglione (ed), *Sanità, Finanza, Etica* (Milano 2025) 201.

[17] In this context, F Petrosino, 'Scoring assicurativo algoritmico e rischio di discriminazione. Spunti per una riforma' (2023) V Riv Dir Banc 443 ss, 453. ff., in particular 453, and U. Malvagna, 'Intelligenza artificiale', (14) 71.

[18] P Gaggero e C Valenza, 'Le moderne tecniche di credit scoring tra GDPR, disciplina di settore e AI Act' (2024) Rivista di diritto bancario 825 ff.

[19] As defined by Regulation (EU) 2024/1689 as *'an automated system designed to operate with varying levels of autonomy and which may exhibit adaptability after deployment and which, for explicit or implicit purposes, derives from the input it receives how to generate outputs such as predictions, content, recommendations or decisions that may affect physical or virtual environments*'. On the subject of the first applications in the insurance sector, see F Ioannoni Fiore, 'Applicazioni dell'intelligenza artificiale e nuovi strumenti di governo del rischio nei contratti assicurativi' (2022) Riv dir impr 112 ff.

[20] On the basis of which to decide whether or not to grant credit or, as far as insurance contracts are concerned, whether or not to issue a policy.

[21] See also N M Faraone, 'Spunti ricostruttivi in materia di profilazione e valutazione del merito creditizio nella nuova strategia europea dei dati' (2025) I Analisi Giuridica dell'Economia 267 ff.

3. European legislation

Having identified the scope of the study, it is necessary to outline the regulatory framework provided by European legislation, which grants insured persons[22] the most significant safeguards in this area. Alongside supranational regulation, of course, legislation dictated by national law also plays a fundamental role, and in particular the multi-level legislation applicable to insurance matters within the Italian legal system . Here, in discussing the impact of personal data processing using new technologies on the insurance sector, we shall focus in particular on European legislation on the protection of personal data, specifically with regard to the use of automated decision-making processes.

Firstly, it is considered appropriate to begin with Regulation (EU) 679/2016, commonly known as the 'GDPR'[23] , which was designed to protect 'rights' and 'freedoms' in relation to the right to the protection of personal data and to harmonise national legislation by aligning it with EU standards on this matter[24] . Finally, Regulation (EU) 1689/2024, better known as the 'AI ACT'[25] , was introduced to address the issue of so-called automated decision-making processes, was Regulation (EU) 1689/2024, better known *as the 'AI* ACT' , which advocates a risk-based approach and represents a significant step towards the development and responsible use of artificial intelligence systems, introducing a *'horizontal'* framework for artificial intelligence systems based on *a 'risk-based graduated regulatory approach*[26] .

As mentioned, one of the main points of intersection between these regulations and the *Insurtech* sector concerns the safeguards afforded to the insured in the event of decisions based exclusively on automated processing algorithms (i.e. on substantial 'algorithmic processing' of data)[27] , *i.e.* the

[22] *'Insured parties-data subjects'*, as these are both parties entering into the insurance contract and so-called 'data subjects' under Article 4 of the GDPR, which *defines 'personal data' as 'any information relating to an identified or identifiable natural person ('data subject')*'.

[23] On this subject, AA Vv, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford Academic 2020); AA Vv, *Guida al trattamento e alla sicurezza dei dati personali* (G Comandé e G Malgieri eds, Milano 2018).

[24] To use the terminology set out in Article 1 of the GDPR, entitled *'Subject matter and purpose*'.

[25] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, hereinafter referred to more briefly as the 'AI ACT'.

[26] See U. Malvagna, 'Intelligenza artificiale', (14), 49 ff. See also A.J. Pagano, C. Cappiello, C. D'Elia, AJ Pagano, C Cappiello e C D'Elia, 'AI ACT between selectivity and discrimination. The state of the art of National and EU Regulation' (2025) Business Law Review, *passim*; G Malgieri e F Pasquale, 'Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology' (2024) Computer Law & Security Review 1. Safeguards regarding *credit scoring* are also found in the so-called CCD2, Directive (EU) 2023/2225 on consumer credit agreements. On these topics, see V Notarangelo, 'La protezione dei dati degli interessati nell'accesso al credito: la valutazione del merito creditizio tra normativa e decisioni algoritmiche' in R Floreani e S Petrussi (eds), *Il GDPR in ambito assicurativo* (vol II, Milano 2025) 121 ff., which also discusses developments regarding the 'right to be forgotten' in relation to cancer and insurance contracts (Law 193/2023), on which the very recent IVASS provision No. 196/2026 of 15 January established the right not to be discriminated against on the basis of one's medical history. On the impact of AI in the insurance sector, see also EIOPA, *Report on Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector*, 2021.

[27] On this topic, see P Manes, 'Insurance and the legal challenges of automated decisions: An EU perspective' in *Routledge Handbook of Financial Technology and Law* (2021) 213 ff.

processing of personal data through, for example, but not exclusively, artificial intelligence systems.

In fact, one of the key features that characterises the *Insurtech* phenomenon is the use of *big data* and predictive analytics for pricing. In the insurance sector, digitalisation has made it possible to leverage data collected from customers, combining it with *big data*[28] , to perform *clustering* operations capable of profiling customers and improving not only the alignment of products with their insurance needs, but also pricing[29] : the combination of a vast amount of data can be used to generate profiles of insured customers, which can in turn be used to decide whether to offer (or not offer) them tailor-made products based on insurance premiums that are cost-effective for insurance companies. In other words, this profiling is, therefore, made more effective by the use of algorithms and artificial intelligence systems, thanks to which companies make decisions based exclusively on automated processing carried out by algorithms regarding, for example, the insurability of the individual concerned and the premium quotation: as mentioned, this has eroded the significant information asymmetry that has always placed insurers at an 'informational disadvantage'[30] , by reducing the gap caused by the absence of data useful for companies' decision-making.

To put the picture just outlined into context, we can start with a practical example. Within the US healthcare insurance system, the *CMS* (*Centers for Medicare & Medicaid Services*) has taken an initial step aimed at increasing protection for policyholders[31] , ensuring that an artificial intelligence system, without human intervention, cannot decide whether an insured citizen is (or is not) entitled to insurance cover. This issue is particularly relevant in the United States, where insurance companies use artificial intelligence systems to assess the risk profile of potential policyholders and, consequently, may exclude those deemed too high-risk to receive health insurance cover[32] . The absence of human oversight in monitoring these algorithms and the inability to correct any

---

[28] For a definition, see OECD, *Big Data: Bringing Competition Policy to the Digital Era,* 2016, available at: https://web-archive.oecd.org/temp/2022-02-21/414870-big-data-bringing-competition-policy-to-the-digital-era.html), according to which *Big Data* is the set of information characterised by such volume, velocity and variety that it requires specific technologies and analytical methodologies to be transformed into value.

[29] S. Landini, 'Insurtech: innovation in production', (9) 434.

[30] See E. Giorgini, 'Profilazione automatizzata, (12) 751 ff. The Insurtech phenomenon has thus revolutionised the way in which policyholders' data is processed, including through the use of algorithms and artificial intelligence systems. On these issues, see S. Landini, 'Corporate governance e assicurazioni' (2023), Giur. Comm., 389 ff.

[31] In particular, reference is made to the guidelines (FAQ) published by the CMS (https://www.aamc.org/media/74896/download?attachment).

[32] And such decisions are not without consequences. Indeed, class actions have been brought against the insurance company UnitedHealth regarding the use of *NHPredict* (*Estate of Gene B. Lokken et al. v. UnitedHealth Group, Inc. et al.*, District Court of Minnesota, docket no. 0:23-cv-03514), in which so-called *post-acute care* was denied on the basis of automated assessments and without any human review of the decisions *ex post*. Along the same lines are the *class actions United States ex rel. Shea v. eHealth, Inc. et al.* (*Massachusetts District Court,* 1:21-cv-11777) and *Barrows et al v. Humana* (*Kentucky Western District Court*, 3:23-cv-00654), as well as *Kisting-Leung v Cigna Corp. Case* No. 2:23-at-00698 (2023). On these topics, see E. Faletti, 'La nuova 'gold rush' dell'intelligenza artificiale: l'AI Action Plan negli Stati Uniti della seconda presidenza Trump', in *CERIDAP*, 19 January 2026; M. Mello, S. Rose, 'Denial—Artificial Intelligence Tools and Health Insurance Coverage Decisions', in *JAMA Health Forum*, 2024; A. Amidei, 'Decisioni automatizzate in sanità: il caso UnitedHealth', available at https://dirittoesanita.unipv.it/aree-di-ricerca/decisioni-automatizzate-caso-unitedhealth.kl

biases inherent in the system lead to the exclusion of those belonging to often marginalised demographic groups, including, by way of example but not limited to, vulnerable people, immigrants and foreigners[33] .

The issues just mentioned are further complicated by the fact that decision-making algorithms can be trained using training *datasets* that do not comply with the fundamental principles of the GDPR set out in Article 5 of the Regulation[34] . Furthermore, the algorithms themselves can be difficult for data controllers and processors to understand, raising considerable doubts about the transparency and interpretability of the system[35] .

The spread of these technologies, which are in some respects opaque and difficult to interpret and comprehend, within modern society has been widely referred to as the *'black box* society'[36] , a term that highlights the challenges posed by the integration of algorithms and *AI* solutions into various aspects of society, including the insurance sector.

This complex landscape raises the question of whether policyholders are entitled to an explanation of automated decisions concerning, for example, whether or not to purchase an insurance policy and based on the use of algorithms or artificial intelligence systems that do not involve any human intervention, an operation that may be further complicated not only by machine learning (*ML*) but also by the inference of new personal data from so-called 'raw' personal data[37] .

However, in the context of the automated processing of personal data through the use of algorithmic systems, including those involving artificial intelligence, it is Articles 13(2)(f), 14(2)(g) and 15(1)(h), alongside Article 22(3), that provide *tailored* protection for the data subject.

---

[33] This topic is also addressed in I Carnat, 'When algorithmic regulation could save lives, quite literally' (2025) https://www.predictivejurisprudence.eu/author/wp_1400504/

[34] Key principles include lawfulness, fairness, transparency, so-called *data protection by design* and *by default*, data minimisation, purpose and storage limitation, accuracy, integrity and confidentiality

[35] G. Comande, 'Algorithms and Big Data: The Legal Response' (2023), Corporate Law, Digitalisation and Artificial Intelligence, 95 ff.

[36] F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard 2015).

[37] E. Pelino, *Art. 22 GDPR*, (15) 160. On these issues, see G. Malgieri and G. Comandé, 'Why a right to legibility of automated decision-making exists in the General Data Protection Regulation', (2017) *International Data Privacy Law*, 4, 243 ff.; more recently, B. Parenzo, *La profilazione algoritmica nel prisma dell'autonomia privata*, (Naples 2025), in particular 102–118, as well as A.G. Grasso, *GDPR Feasibility and Algorithmic Non-Statutory Discrimination* (Naples 2023), *passim*; G. Comandé, Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali, (2022) Danno e Responsabilità 141 ff. This includes, for example, *machine learning* systems, defined in the literature as *'a multidisciplinary sub-field of Artificial Intelligence (AI) focused on developing and implementing algorithms and statistical models that enable computer systems to perform data-driven tasks or make predictions through 'leveraging data' and iterative learning processes'*; see P. Dong, Z. Quan, 'Automated machine learning in insurance', (2025) Insurance: Mathematics and Economics, 120, 17 ff. Furthermore, as noted by L. Dani, 'The processing of genetic data in insurance contracts' (2025) Ann. Sisdic, 13, 58, *'it is precisely AI systems, intended for use in risk assessment and pricing in life and health insurance, that are classified as 'high-risk' systems within the meaning of Article 6 of EU Regulation 2024/1689 (AI Act). Consequently, the data controller is subject to specific and stringent measures regarding control, transparency, accuracy, traceability, documentation and supervision, necessary to prevent effects that infringe upon the fundamental rights of the individual'*. See also Annex III, point 5(c), which classifies AI systems intended for use in risk assessment and pricing in relation to natural persons in the case of life and health insurance as *high-risk AI systems* as referred to in Article 6(2), *'as they may 'have a significant impact on people's livelihoods and, if not properly designed, developed and used, (…) infringe their fundamental rights and lead to serious consequences for people's lives and health, including financial exclusion and discrimination' (again, recital 58)'*; thus, U. Malvagna, 'Intelligenza artificiale', (14), 54.

These articles, in fact, are of particular relevance in the context of automated processing involving automated profiling as referred to in Article 4(4) of the GDPR. Furthermore, in this regard, Recital 71 of the Regulation is noteworthy, which states that *'The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her, or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention'*.

In this context, the provisions of Article 22(1) of the GDPR constitute a first concrete instrument for safeguarding against and restricting the use of automated decision-making processes, essentially prohibiting their use[38]. This restriction applies when decisions are made solely by automated means, with a significant impact on individuals, and are not based on a contractual agreement, the law, or the explicit consent of the data subjects[39]. In other words, this provision grants data subjects (in the context of this discussion, insured persons) the right to intervene in the logical process followed by the algorithm, challenging it and requesting human intervention, when the processing is exclusively automated, i.e. does not involve 'substantial' human involvement at any stage.

The exceptions to this general prohibition[40] are set out in paragraph 2 of the same article, providing for the possible use of such processes in cases where a decision of this kind is necessary for the conclusion or performance of a contract between the data subject and the data controller, is authorised by European Union law or the law of a Member State, or is taken on the basis of the data subject's consent[41]. That said, it is essential to understand what information the data subject may request from the data controller, what they may learn about the mechanism adopted and, furthermore, how they may concretely intervene in the automated decision-making process. In other words, the question has arisen as to whether there is a right to receive an explanation of how an algorithm works.

In the European Union, a 'right to *explanation*' can be identified within *the framework* of the GDPR by analysing various provisions of the Regulation. In particular, those relating to the right to information (specifically, Articles 13 and 14), the right of access (Article 15) and the aforementioned right not to be subject to automated decision-making (Article 22)[42].

A first *ex ante* safeguard is therefore provided for in Articles 13 and 14 of the GDPR, concerning the information to be provided to the data subject, by means

---

[38] *'The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'*

[39] G. Malgieri-G. Comandé, 'Why a right to legibility' (37), 244.

[40] This view is widely held in legal scholarship. Among others, see B. Parenzo, 'Profilazione e discriminazione. Dal GDPR alla proposta di Regolamento sull'IA' (2023) Tecn. e dir., I, 2023, 122, as well as E. Giorgini, 'Profilazione automatizzata' (12), 761.

[41]. It should be noted that stricter restrictions apply to decisions based on special categories of personal data pursuant to Article 9 of the GDPR, where explicit consent will be required for specific purposes or where processing is necessary for reasons of public interest. In this regard, see Aa.Vv. *GDPR and Privacy Legislation Commentary*, (Milano 2022), 277 ff.

[42] In this context, the right to erasure of data and to restriction of processing, pursuant to Articles 17 and 18 of the GDPR respectively, are also relevant.

of which – specifically – consistently inform them of the manner and terms under which their data will be processed, the purposes of the processing for which the personal data are intended and the legal basis for the processing, as well as informing them, where applicable, of the use of automated decision-making, including profiling, as referred to in Article 22(1) and (4). The principle of *accountability* requires that it is the data controller who must demonstrate, for the purposes of the validity of consent, that the contested access and processing are attributable to the purposes (with all the critical issues in the event of the reuse of the same data and their compatibility with the new purposes, where different from the purposes indicated at the time of their collection[43]) for which valid consent was requested – and validly obtained – specifically adequate consent, together with evidence regarding the significance of the information on the logic employed, as well as the importance and anticipated consequences of such processing for the data subject[44] .

However, it often happens that data subjects consent to the processing of their personal data without fully understanding the content of the *privacy* notices provided to them, which often appear, at the very least, cryptic to the data subject, particularly with regard to the use of artificial intelligence systems or algorithms employed to make decisions in a fully automated manner. Therefore, in addition to a complete, intelligible and comprehensive policy provided in advance, it is also necessary to identify safeguards and guarantees at a later stage, *ex post*[45] .

The primary safeguard[46] is enshrined in the aforementioned Article 22(3) of the GDPR and ensures that natural persons are not subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This article, as noted, constitutes the first line of defence against the distorted or harmful use of the aforementioned systems, thereby mitigating the risks of exclusion from insurance cover and from the range of policies offered on the market. Furthermore, the provision grants the data subject-policyholder the power to intervene in the assessment process conducted by the insurance company. It should be noted, however, that the protection mechanism of Article 22 of the GDPR can only be invoked if the individual is in fact aware and has knowledge of both the existence of automated processing and the specific data that have been processed, as well as the manner in which the processing took place[47] .

In this way, the insured person must first refer to the protection afforded by Article 15 of the GDPR, which grants the data subject the right of access and the right to obtain meaningful information on the logic used by the algorithm in order to challenge the automated processing of personal data carried out. Indeed, Article 15 stipulates that, upon request, the data controller must

[43] In these terms, see U. Malvagna, 'Intelligenza artificiale', (14), 69.
[44] See also G. Comandé, Leggibilità algoritmica e consenso al trattamento dei dati personali (37) 148.
[45] A. Roig discusses the concept of *'safeguards'* in 'Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)' (2017) European Journal of Law and Technology, 2017.
[46] In the insurance sector, the topic has been addressed by G. D'Ippolito and E. Incutti, 'I processi decisionali interamente automatizzati nel settore assicurativo' (2019) Riv. dir. Impr., 3.
[47] B. Parenzo, 'La profilazione algoritmica' (37), 113 ff.

provide the data subject with sufficiently detailed information on the logic used to enable them to verify the accuracy and consistency of the decision made as part of the automated decision-making process. Such information must be specific to the data subject and the processing carried out must be clearly explained: therefore, this provision aims at *the disclosure* of targeted information and clarifications regarding the specific processing carried out in relation to the data subject's data[48] .

The right to receive an explanation thus extends to the logic underpinning the algorithmic decision-making process, ensuring transparency and accountability in the use of automated systems, and is enshrined in Articles 13, 14 and 15, which establish the data controller's obligation to provide meaningful information on the logic used in the automated decision-making process (both *ex ante* and *ex post*).

It should, of course, be noted that this right of access (with a view to achieving an understanding and, in so doing, effective 'algorithmic explainability') is essential for reaching a remedial solution in relation to automated processing, becoming a fundamental prerequisite for the enforceability of any safeguard regarding the subsequent right to challenge the automated decision, as expressly provided for in Article 22(3)[49] .

In practical terms, this principle also applies where profiling with a significant legal impact, carried out by means of fully automated operations, is performed by 'third parties' (such as *business information* and data analysis firms to which insurance companies might entrust profiling and *scoring*) but the decisions based on such profiling are subsequently taken by those who commission the profiling (banks, insurance companies, etc.). Ultimately, in these latter cases, there is a disconnect between 'third parties' (the company carrying out the *scoring*) and those we might call 'decision-makers', such as banks or insurance companies. Despite this separation, it must not be forgotten that what essentially matters for the activation of protection is the existence of a decision that affects the rights attributable to the individual; consequently, for the purposes of classifying *credit scoring* as an automated 'decision', the existence of a 'decisive link' between the preparatory *scoring* act carried out by the third party and the subsequent decision, which ensures that the safeguards referred to in Article 15 – first – and Article 22 – subsequently – of the GDPR can be triggered, even though the *scoring* is initially carried out outside the decision-maker's sphere of decision-making and the actual decision is subsequently taken by the commissioning entity[50] .

Consequently, the articles cited provide a safeguard ensuring that the insured person receives timely human intervention in the process carried out by a predictive algorithm – even where an artificial intelligence system is involved – which determines 'insurability' by processing personal data and identifying a specific risk profile.

---

[48] G. Malgieri and G. Comandé, 'Why a right to legibility' (37), 5.

[49] B. Parenzo, Profilazione e discriminazione (40) 105 ff., as well as in Ibid., 'Il diritto alla spiegazione tra GDPR e AI Act', in T. Della Massara and E. Al Mureden (eds) *La volontà macchinica. Realità o soggettività* (Pisa 2025).

[50] On this point, see *below* the recent judgment of the CJEU in Case C-634/21 of 7 December 2023 (*'reference for a preliminary ruling from the Verwaltungsgericht Wiesbaden — Germany) — OQ v Land Hessen, SCHUFA Holding'*).

Similarly, in *the AI Act*[51] , Article 86 stipulates that any data subject who is the subject of a decision adopted by *the deployer* – in the research being conducted here, the insurance undertaking – based on the output of a high-risk AI system listed in Annex III[52] , and which produces legal effects or similarly significantly affects that person in a way that they consider to have a negative impact on their health, safety or fundamental rights, has the right to obtain from *the deployer* clear and meaningful explanations regarding the role of the AI system in the decision-making process and the main elements of the decision taken. Furthermore, Recital 171 states that the explanation should be clear and meaningful and should provide a basis on which data subjects can exercise their rights.

4. The insurance sector

The rules just mentioned clearly establish the existence of a right to an explanation (or algorithmic transparency[53]) in European law and offer further protection to the insured[54] .

Consequently, there is a clear need to reconcile the use of profiling techniques with the *compliance* regulations designed to safeguard the rights of data subjects, in order to continue using such systems without the risk of infringing the rights guaranteed to the insured, whilst also anticipating appeals to the relevant authorities – including regulatory bodies – as well as litigation (in other words, unnecessary financial outlays for companies, the outcome and timing of which are often uncertain). For this reason, an insurance company, in light of the safeguards granted and provided for by European legislation, is obliged to ensure *compliance* by putting in place specific measures to protect the insured. Firstly, the insurance company must grant the insured the possibility to 'intervene' in the automated process. It is necessary to guarantee the insured person the right to human intervention and, progressively, to organise well-defined access procedures and all the mechanisms necessary for a person to intervene effectively in the process conducted by an algorithm, to request meaningful information on the logic used (see Articles 13, 14, 15 of the GDPR), express their opinion and challenge the assessment made by the algorithm after having accessed the logic behind the automated decision (with the *ex post* protection referred to in Article 22 of the GDPR)[55] . In addition to the articles cited, it is essential to emphasise that, in order to ensure the effectiveness of this process, the individual must be able to intervene not only

[51] Reg. (EU) 1689/2024.
[52] E.g. *'AI systems intended for use in risk assessment and pricing in relation to natural persons in the case of life insurance and health insurance'.*
[53] G. Malgieri-G. Comandé, 'Why a right to legibility' (37), *passim.*
[54] See also P. Gaggero, P., & C.A. Valenza, 'Le nuove prassi valutative del merito creditizio tra GDPR, CCD II e AI Act | New Creditworthiness assessment practices between GDPR, CCD II and the AI Act (2024), European Journal of Privacy Law & Technologies.
[55] As well as the right to obtain human intervention from the data controller; the right to express one's point of view; the right to challenge the decision.

during automated processing, but also to give their consent *ab initio* in a deliberate manner[56] .

In the context of Insurtech, this right to transparency implies the need for individuals to understand what data is processed by insurers, defining the scope of the purposes for which it is collected, and which is then subject to automated decision-making processes, together with the inferential processes underpinning such decisions. An optimal solution would be to provide individuals with the ability to understand, in a transparent and intelligible manner, the functionality, impact, consequences and rationale of these decision-making processes.

In this context, the right in question has recently been recognised, not only through a coordinated interpretation of the legislation mentioned above, but also by the Court of Justice of the European Union in the judgments widely known as the *'Schufa Holding'* (C-634/21) [57] and *'Dun and Bradstreet'* (C-203/22)[58] cases.

The first is a recent ruling by the Court of Justice of the European Union in which a German citizen was denied a loan by a bank, whose data had been processed automatically by a credit *rating* agency. The judges in Luxembourg ruled that the process of assessing creditworthiness [59] carried out by credit *rating* agencies and preparatory to the decision of the bank (or insurance company) falls within the scope of Article 22 of the GDPR. The safeguards set out in Article 22 of the GDPR therefore, apply whether the bank uses dedicated *credit scoring software or* whether the assessment (*or rather*, the decision) is carried out by an *outsourced* third-party provider other than the bank (through a so-called preparatory act, which nevertheless maintains a decisive link between the *score* itself and the final decision to grant credit or to issue a policy). This conclusion is reached because the *score* determined by the third-party provider leads the bank or insurance company, which commissioned that *rating*, to adhere in an entirely 'passive' manner to the upstream decision, relying – therefore – on the results of processing carried out by third parties[60] .

For this reason, if one were to exclude these latter cases of 'disconnection' (namely, a 'passive' decision taken by the entity commissioning the *rating*, following processing carried out by a third-party company appointed by that entity) from the scope of Article 22, this would result in a genuine short-circuit:

---

[56] As already argued in the literature, the European system recognises a right to the legibility and explainability of algorithms. G. Malgieri-G. Comandé, 'Why a right to legibility' (37), *passim*.

[57] On the so-called *Schufa Holding* case, see F. D'Orazio, 'Il credit scoring e l'art. 22 del GDPR al vaglio della Corte di giustizia', (2024) La nuova giurisprudenza civile commentata, 2 410 ff.; A. Aza, 'Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context' (2024) Industrial Law Journal, 840 ff.

[58] Judgment of the Court (First Chamber) of 27 February 2025. *CK v Magistrat der Stadt Wien.* On the *D&B* case, B. Parenzo, 'Informazioni significative' nei processi decisionali automatizzati: parla la Corte di Giustizia, (2025) Nuova Giur. Civ. Comm. 4 972 ff.

[59] On this subject, see B. Paal, 'Case Note: Article 22 GDPR: Credit Scoring Before the CJEU', (2023) Global Privacy Law Review 4, 127 ff.; G. Cerrina Feroni, 'Intelligenza artificiale e sistemi di scoring sociale. tra distopia e realtà' (2023) Il diritto dell'informazione e dell'informatica 1 ff.; A. Davola, *La valutazione del merito di credito del consumatore*, in L. Modica, E. Pellecchia (eds.) La riforma del sovraindebitamento nel codice della crisi d'impresa e dell'insolvenza, (Pisa 2019), 129 ff..

[60] We agree with the observation made by U. Malvagna, 'Intelligenza artificiale', (14), regarding *the vulnerability* that arises in terms of reporting to the supervisory authority, in the event that it is *the outsourcer* who carries out customer profiling using AI, subsequently providing the insurance company with the 'decision' that has already been reached.

the decision-maker, i.e. the bank or insurance company, does not hold the data in the event of a data subject's request for access under Article 15, whilst the party holding the information and data, the third-party entity (bank or insurance company), does not 'decide', as it cannot, paradoxically, be contacted for the purposes of exercising rights under the GDPR[61] . Therefore, the Court ruled that the data subject has the right to access their data pursuant to Article 15 of the GDPR and to obtain human intervention from the data controller (in this case the third party) to express their point of view and challenge the decision pursuant to Article 22 of the GDPR, regardless of which entity carries out profiling and automated data processing and who ultimately makes the decision. In this context, the Court interpreted the term 'decision' broadly, including automated *credit scoring* even where carried out by a third party other than the bank or insurance company that commissioned the *rating*.

The so-called right to transparency and to an explanation was further clarified in the *'Dun & Bradstreet'* judgment (C-203/22) of the same Court. The judges clarified that the obligation to provide 'meaningful information' as defined in Article 15(1)(h) does not imply the full disclosure of the algorithm used in automated decisions, in order to avoid information overload and the disclosure of trade secrets. On the contrary, the data controller is required to provide adequate and accessible explanations, such as to enable the data subject to understand the relevant factors and decision-making criteria adopted, as well as the general logic that led to the automated result. In other words, they must indicate the personal data processed and provide the algorithm's implementation scheme, i.e. the internal logic of its operation[62] .

The transparency requirement demands that such information be communicated in a clear, concise and easily understandable manner[63] . It is also necessary to ensure a balance between the data subject's right to obtain information and the protection of the data controller's trade secrets[64] . Whilst recognising the importance of safeguarding trade secrets and the rights of third parties, the Court emphasised that such commercial interests cannot be used as a basis for an absolute refusal to provide the requested information.

Ultimately, insurance companies are obliged to adopt an internal *governance* structure that is in line with the technological challenges posed by the

---

[61] See B. Parenzo, in 'Resoconto di un webinar su «credit scoring e decisione automatizzata', V. Gargani, available at https://deiustitia.it/wp-content/uploads/2024/05/GARGANI_RESOCONTO-DI-UN-WEBINAR-SU.pdf

[62] The Court has ruled that: *'Article 15(1)(h) of Regulation (EU) 2016/679 (…) must be interpreted as meaning that, in the case of automated decision-making, including profiling, within the meaning of Article 22(1) of that regulation, the data subject may require the controller, as 'meaningful information about the logic involved', to explain, by means of relevant information and in a concise, transparent, intelligible and easily accessible form, the procedure and principles actually applied in order to use, by automated means, the personal data concerning that person with a view to obtaining a specific result, such as a credit profile.'*

[63] See also Recitals 58 and 60 of the GDPR.

[64] In Italy, the first ruling to define the scope of 'access' under Article 15 of the GDPR was delivered by the Civil Court of Cassation, Section I, Order 25 May 2021, No. 14381 in *One Legale* with a note by G. Comandé, Leggibilità algoritmica e consenso al trattamento dei dati personali (37) 665 ff., which requires that *'the algorithm's execution scheme* (internal operating logic) *and the elements considered* (data processed)*'* be made known, and then Civil Cassation, Section I, Order, 10 October 2023, No. 28358, which explains that the execution scheme consists of elementary, unambiguous steps, of finite number, executable within a finite time and yielding a single result.

development of decision-making algorithms[65] . This *governance* structure must ensure the company's efficiency, whilst constantly seeking a balance with the principles set out in Article 5 of the GDPR regarding the processing of personal data. On the other hand, policyholders must be able to rely on an insurance company that is capable of serving its customers even better in the future, offering increasingly integrated products whilst respecting the rights of policyholders.

In this regard, one of the main issues that still needs to be resolved is how privacy notices are drafted. The privacy notices contained in insurance policies are often dense and written in 'legalese' as well as insurance jargon: a difficult maze in which the policyholder very often cannot find their way. This undermines the proper flow of information and the requirements of clarity – including regarding the purposes of processing – and transparency that should characterise the processing.

Nor should the interpretative uncertainties regarding the legal bases for data processing used by insurance companies be overlooked. From a data protection perspective, processing carried out for the assessment, underwriting and management of insurance risk (the so-called insurance profile), as well as the analysis of requests and needs pursuant to Article 58 of IVASS Regulation No. 40/2018 (which transposes the obligations of the EU Insurance Distribution Directive, IDD, Dir. (EU) 2016/97[66]), only when carried out by automated means, constitute profiling within the meaning of Article 4(4) of the GDPR. As 'profiling' to determine the risk profile of the insured person is a legal obligation, the legal basis for the processing must be sought in Article 6(1)(c) of the GDPR (the so-called legal obligation) or in Article 6(1)(f), where it can be classified as a legitimate interest of the controller (i.e., the insurance company), or, alternatively, in Article 6(1)(b), concerning the performance of the contract. Building on these premises, it is necessary to ask what changes if the profiling is automated profiling, within the meaning of Article 4(4) of the GDPR, for which an appropriate legal basis for processing must be selected, anticipating from the outset the critical issues regarding the basis under Article 6(1)(a) of the GDPR.

A review of some of the privacy notices accompanying insurance policies currently available on the market it is clear that the legal basis most frequently chosen by insurance companies for the processing of data associated with insurance activities is that set out in Article 6(1)(b) of the GDPR, namely the performance of pre-contractual or contractual measures, with consent being used in the case of data processing under Article 9 of the GDPR[67] .

---

[65] S. Landini, Corporate Governance (30), 389 ff. On these topics, see also N. Abriani, G. Schneider, *Diritto delle imprese e intelligenza artificiale*, (Bologna 2021), *passim*.

[66] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution.

[67] On the critical issues surrounding consent as a legal basis for the processing of health data in the insurance sector, see J. Amankwah, N. Stroobants, 'GDPR and the Processing of Health Data in Insurance Contracts: Opening a Can of Worms?', in M. Rego and B. Kuschke (eds), Insurance and Human Rights, (Springer Cham 2022). Article 9 of the GDPR imposes a prohibition in the first paragraph and then specifies, in paragraph 2, a series of 'exceptions', including the case where *'the data subject has given explicit consent to the processing of such personal data for one or more specific purposes* (…)*'*.

In the case of the use of automated decision-making processes[68] , in relation to which policies often state*: 'The provision of data for these purposes is necessary: therefore, in the absence thereof, it will be impossible to conclude and perform the insurance contract'*[69] , these are justified by Article 22(2)(a), explaining how the automated decision-making process is necessary for thethe performance of the contract in order to ensure compliance with the requirements of insurability/risk acceptance/pricing, arguing, in conclusion, that such activity is necessary for the conclusion or performance of a contract, as well as in view of regulatory requirements (for example, in order to offer the product best suited to the insurance needs, or for the purpose of complying with anti-money laundering and anti-terrorism regulations).

Furthermore, where data under Article 9 of the GDPR is concerned, consent reverts as the legal basis, since the Personal Data Protection Code (Legislative Decree 196/2003 and subsequent amendments) does not include insurance activities among those of significant public interest, and therefore Article 9(2)(g) of the GDPR cannot be applied[70] . However, consent is ineffective from a protection perspective (also in light of the WP29 guidelines on this point), due to the presence of a situation of 'conditionality' (given that failure to provide consent makes it impossible to provide the service), as well as a 'power imbalance' between the customer and the insurer[71] .

A privacy notice drafted in this way selects one of the legal bases also provided for by the WP29 and complies with the requirements set out in Articles 6 and 9 of the GDPR, requiring the insured person to give their consent for activities involving automated decision-making relating to special categories of data. We must, however, ask ourselves whether sufficient attention is paid to the insured person's actual need to understand and interpret the processing methods at the time of entering into the insurance contract. Indeed, the insured person often lacks both the technical insurance knowledge and the legal expertise to understand how their data is actually processed, for what purposes, and what implications this has for the conclusion of an insurance contract. At present, in certain cases, the data subject is effectively obliged to provide their data for the performance of these processes[72] .

---

[68] It should be noted that such profiling could also be carried out without the use of technology. Consequently, it does not appear necessary for this methodology to be employed and, therefore, it would not seem to constitute the applicable legal basis in the present case.

[69] It should also be borne in mind, as U. Malvagna, 'Intelligenza artificiale', (14), 68, that *'For the purposes of the lawfulness of the processing of personal data[37], it is essential that the initial collection of data be compatible with the purposes stated by the data controller, in accordance with the criteria set out in Article 6.'*

[70] On this subject, note the detailed research, including quantitative analysis, carried out by A. Soldato, 'Processi decisionali automatizzati e assicurazioni: indagine sul right to explanation nel settore assicurativo', in ETD-UNIPI.

[71] Ibid., 'Processi decisionali automatizzati e assicurazioni' (70) p. 109.

[72] In this regard, reference is made to Recital 43 of the GDPR, which *states that 'Consent shall be presumed not to have been freely given* (...) *if the performance of a contract, including the provision of a service, is made conditional upon consent, even though consent is not necessary for such performance.'* This constitutes the so-called *'conditionality'* of the data subject, as argued in WP29, 'Guidelines on Consent under Regulation 2016/679 (WP259)', 2017, pp. 8–9, available at: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. From this perspective, one might hypothesise a breach of the obligations of good faith, transparency, fairness, protection and information pursuant to Articles 1175, 1337 and 1375 of the Italian Civil Code. On this subject, see Civil Court of Cassation, 24 April 2015, No. 8412, in *Onelegale*. Or, furthermore, Articles 119 et seq. and 120 of the Private

It is therefore desirable that the approach to drafting privacy notices relating to policies on the market should change, without hindering technological development and the evolution of insurance companies' business management systems.

In this regard, in order to make the processing of the insured person's personal data more comprehensible, one might consider establishing a right to an explanation, a right to explainability and algorithmic readability, which is not merely exercised *retrospectively* following the exercise of rights, but which also exists for the insured person *prospectively*, deriving directly from the reading of the insurance contract documentation. In this regard, a legibility test could be employed (*legibility test*[73] , explaining the architecture and implementation to ensure transparency and comprehensibility), whereby the insured party can be aware, from the moment the insurance contract is concluded, of the data being processed and the logic of the system used, informing them of the logic behind the automated decision-making process not only 'on request', through the right of access, but by providing, in the privacy notice and at the time of signing the contract, a set of intelligible information for the policyholder[74] .

In the wake of the *Kirchberg* court rulings, one could begin to provide adequate and accessible explanations, such as to enable the data subject to understand the relevant factors and decision-making criteria adopted, as well as the general logic that led to the automated result, by indicating the personal data processed and providing the algorithm's implementation scheme, i.e. its internal operating logic[75] .

Furthermore, another element could be the rigorous conduct and partial or full publication of the results of a DPIA pursuant to Article 35 of the GDPR,

Insurance Code, concerning pre-contractual information, as well as Article 166 of the Private Insurance Code on the criteria for drafting policies; or, additionally, Title XIII of the same Code, dedicated to the transparency of transactions and the protection of the insured. Regarding the liabilities of the insurance intermediary, Articles 119 et seq. are provided for the protection of the insured, as well as, in particular, Article 120 of the so-called Code, entitled *'Pre-contractual* information', and Article 183 of the so-called Code, entitled *'Rules of* conduct', as well as Article 58 of IVASS Regulation 40/2018 on the suitability of the insurance product in relation to the policyholder's insurance requirements and needs); alongside the 'sector-specific' rules, the provisions of the Civil Code shall also apply (in particular, Articles 1176(2), 1337, as well as 1175 and 1375 of the Civil Code and Article 2 of the Constitution, which set out the obligations of good faith, protection and information). Among other things, the law establishes specific obligations on the part of the insurance undertaking regarding the preparation of contractual documents in a clear and comprehensive manner and, with regard to the acquisition of potential customers, regarding the need to provide all information deemed useful for the individual contractual relationship (Articles 119-ter and 166 of the Private Insurance Code; and it should also be noted that the pre-contractual disclosure obligation is provided for in Article 56 of IVASS Regulation 40/2018, as well as Article 20 of the IDD, Directive (EU) 97/2016). In the academic literature on this subject, see P. Marano, *L'intermediazione assicurativa*, (Milan 2013), and G. Volpe Putzolu, 'La valutazione di adeguatezza del contratto di assicurazione offerto', in M. Franzoni (ed) La responsabilità civile nell'intermediazione assicurativa, (Milan 2012). Furthermore, it should not be forgotten that the obligation to provide pre-contractual information is laid down in Article 56 of IVASS Regulation 40/2018.

[73] G. Malgieri, G. Comandé, 'Why a right to legibility' (37), op. cit., p. 259 ff.

[74] See also A. Colmenarejo, L. State, G. Comandé, 'How should an explanation be? A mapping of technical and legal desiderata of explanations for machine learning models', (2025) International Review of Law, Computers & Technology, 2025, 1 ff.

[75] Ensuring compliance with the principles set out in Article 5 of the GDPR, as well as the so-called 'seven ethical principles' referred to in Recital 27 of the AI ACT.

taking into account the technology employed[76] . Moreover, on these issues, no particular problems arise with regard to trade secrets, just as the Court of Justice in Luxembourg found[77].

5. Conclusions

Although certain issues still require further investigation – such as the purpose of processing or the selection of an appropriate legal basis for health data – the unresolved problems highlighted in the current landscape, which form the subject of this research, could play a crucial role in securing the data subject's 'informed' consent (or, in any event, where data must be provided regardless due to the existence of other legal bases for processing)[78] the use of *legal design* models[79] , envisaging the drafting of more layered *notices* (so-called *'layered notices*'), featuring a first graphic-visual level (with icons, diagrams, etc.) to illustrate the fundamental rights of the insured data subject, as well as a second, more technical level (but always in compliance with the guidelines set out in the judgments of the Court of Justice) for the details of the algorithmic functioning. IVASS has recently intervened[80] , providing for the use of the so-called Single Pre-contractual Form (MUP), differentiated by product type, whenever companies decide to enter the market by offering a new policy. It could initially be assumed that more *'insured-friendly'* forms will also be used for documentation relating to privacy notices, where insurers should already guarantee the policyholder 'transparency' regarding the data processing carried out, in particular with regard to automated decision-making processes[81] .

Such simplification would certainly benefit the policyholder, but not only them. Indeed, insurance companies, in addition to increasing levels of transparency and *accountability*, are required to adopt *Product Oversight and Governance* (POG) measures based on a holistic and integrated management of

[76] Furthermore, taking into account the AI systems used by the Company, the impact assessment referred to in Article 27 of the AI Act, known as FRIA. This suggestion is also raised in A. Soldato, Processi decisionali automatizzati e assicurazione, (70), 110.

[77] On this point, see paragraph 71 of the Judgment in Case C-203/22 of the Court of Justice of the European Union, which states*: 'In light of the related right to obtain a copy, enshrined in Article 15(4) of the GDPR, the Court has already had occasion to note that its application should not infringe the rights and freedoms of others, including trade and business secrets and intellectual property, in particular copyright protecting software'*. On *the disclosure* of DPIA results from the perspective of *multi-layered explanation*, see M.E. Kaminski and G. Malgieri, 'Multi-layered explanations from algorithmic impact assessments in the GDPR' (New York 2020) Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 78.

[78] *'However, the identification of the explicit consent of the individual data subject as the basis for all automated processing is met with general scepticism, risking becoming a 'blank cheque' for the legitimacy of decisions and resulting in insufficient and inadequate protection'*, as stated by N. M. Faraone, 'Spunti ricostruttivi' (n 21) 275

[79] This solution has been effectively provided by the White Paper resulting from the working group established under the agreement between the GPDP and *Creative Commons Italia to collaborate on the issue of transparency as a fundamental pillar of the GDPR https://www.garanteprivacy.it/temi/creative-commons*

[80] IVASS Regulation 40/2018 (and subsequent amendments). Articles 185–187 of the Italian Civil Code and IVASS Regulation 41/2018 (and subsequent amendments) are also relevant to the issue of pre-contractual information.

[81] In addition to compliance with the Guidelines on automated decision-making relating to natural persons and profiling for the purposes of Regulation 2016/679, 3 October 2017 of *the WP29.*

the entire life cycle of the insurance product[82] . This approach, moreover, would foster greater awareness among policyholders regarding the diligent use of technological tools (such as *black boxes*, on whose data insurers base – in part – their automated pricing processes), thereby creating an incentive effect. In essence, greater awareness of how data is processed can encourage policyholders to adopt innovative technologies, such as *black boxes* in the motor insurance sector, where it is effectively understood that, for example, driving data plays a significant role in premium pricing. This approach, combined with the promotion of safe driving habits to reduce risk, would help lower insurance premiums, bringing benefits to individual policyholders even in those geographical areas usually penalised by insurers' statistics, as well as, from a mutualistic perspective to all relevant risk classes.

The challenge that insurance companies will face in the coming years therefore concerns not only the integration of technologies within *governance*, *underwriting* and product distribution processes, but also the concrete and effective protection of the rights of the policyholder/data subject.

Thus, a crucial test case on these issues is the choice of the information provided to the policyholder, in particular the section concerning the policyholder's rights regarding automated decision-making processes at the time of concluding the insurance contract.

One possible solution could be to provide, including in the sections relating to profiling and automated decision-making, *ex ante* readability [83] , an explanation of the logic of the algorithm used, anticipating the right of access through algorithmic readability as well as simplifying, as mentioned, the privacy notices through effective *legal design* solutions[84] .

In conclusion, the coordination between supranational and national legislation, primary and secondary, as well as the use of *soft law* instruments, must therefore serve as useful solutions for managing the complexity that the use of new technologies brings to regulated markets[85].

[82] Similar to the provisions already set out in MiFID II (EU Directive No 65/2014), the provisions of the rules on product oversight and governance (POG) apply to insurance products. On this point, see the Letter to the Market of 27 March 2024 on expectations regarding the governance and control of insurance products (POG); in particular, it was Article 25 of the IDD (EU Directive No. 97/2016) that introduced all those safeguards for consumer protection from the moment of product design and launch, to ensure that the interests of *the target market* are adequately taken into account.

[83] On the concept of 'readability', see also R Mortier and others, 'Human Data Interaction: The Human Face of the Data-Driven Society' (2014) MIT Technology Review, as well as G Malgieri and G Comandé, 'Sensitive-by-distance: quasi health data in the algorithmic era' (2017) VI Information and Communications Technology Law 14 and ft. 33.

[84] See *the white paper 'Making privacy notices more understandable – legal design as a user-centred approach*' (available here https://www.garanteprivacy.it/temi/creative-commons), published by the Italian Data Protection Authority and Creative Commons, which provides a perspective on *legal design* solutions in the context of the protection of data subjects' personal data.

[85] A Falzea, 'Complessità giuridica' in *Enc. dir.* (Milano 2007) 207.