Credit-Based Insurance Scores: some Observations in the Light of the European General Data Protection Regulation[1]

«Credit-based insurance scores»: reflexiones a la luz del reglamento general de protección de datos de la Unión Europea

M.ª Dolores Mas Badia
Senior Lecturer In Civil Law
University of Valencia (Spain)
Profesora Titular de Derecho civil
Universidad de Valencia
dolores.mas@uv.es

Summary. I. Delimitation of the scope of the study.—II. Preliminary concepts. 1. Credit Reporting Systems and credit scoring. 2. Insurance risk *vs*. credit risk.—III. Credit-based insurance scoring. 1. Concept and function. 2. Arguments in favour. 3. Arguments against.—IV. Some observations in the light of the regulation (EU) 2016/679. 1. Lawful basis for processing of credit history information by insurers. 2. Decisions based solely on automated processing, including profiling.—V. Conclusion

---

Abstract: Despite the differences between credit risk and insurance risk, in many countries large insurance companies include credit history amongst the information to be taken into account when assigning consumers to risk pools and deciding whether or not to offer them an auto or homeowner insurance policy, or to determine the premium that they should pay. In this study, I will try to establish some conclusions concerning the requirements and limits that the use of credit history data by insurers in the European Union should be subject to. In order to do this, I shall focus my attention primarily on Regulation (EU) 2016/679. This regulation, that came into force on 24 May 2018, not only forms the backbone of personal data protection in the EU, but is also set to become a model for regulation beyond the borders of the Union. This article will concentrate on two main aspects:

---

the lawful basis for the processing of credit history data by insurers, and the rules that should apply to decisions based solely on automated processing, including profiling.

Keywords: Insurance Law. Personal Data Protection. GDPR. Credit-based insurance scores. Discrimination.

Resumen: A pesar de las diferencias entre el riesgo de crédito y el riesgo de seguro, en muchos países las grandes compañías de seguros incluyen el historial de crédito entre la información a tener en cuenta para clasificar a los consumidores en los grupos de riesgo y decidir si les ofrecen o no una póliza de seguro de automóvil o de vivienda, o fijar la prima que pagan. En este estudio intentaré establecer algunas conclusiones sobre los requisitos y límites a los que debe someterse el uso de los datos del historial crediticio por parte de las aseguradoras en la Unión Europea. Para ello, atenderé, fundamentalmente, al Reglamento (UE) 2016/679. Esta norma, que entró en vigor el 24 de mayo de 2018, no sólo constituye la columna vertebral de la protección de datos personales en la Unión Europea, sino que también está llamada a ser un modelo más allá de sus fronteras. Me concentraré en dos aspectos: la base legal para el tratamiento de los datos relativos al historial de crédito del cliente por parte de las aseguradoras, y las normas que deben aplicarse a las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles.

Palabras clave: Derecho del Seguro. Protección de datos personales. RGPD. «Credit-based insurance scores». Discriminación.

I. Delimitation of the scope of the study

Today it is almost impossible to imagine a business that does not handle the personal data of customers, with perhaps one exception: those that provide basic everyday services or goods immediately and upon payment in cash. Furthermore, this information is managed in a way that is increasingly sophisticated and complex.

This holds true, in particular, in the field of insurance. The processing of the personal data of policyholders, the insured and, to a lesser extent, beneficiaries or injured third parties, is a core component of the business. The insurance industry depends on the management of this information for a number of different purposes that go far beyond the mere conclusion of the contract: pricing based on risk assessment, the acquisition and maintenance of clientele by offering more competitive and customized products, the identification of claims that are potentially fraudulent, and advertising and marketing are just some examples of how this data is used.

This study will concentrate on the issue of the processing of personal data in risk management, an activity that lies at the very heart of the insurance business. Customers take out insurance policies on the basis of their estimate of the risk of loss. Insurers, for their part, offer coverage based on their assessment of the cost of covering losses. To achieve this goal, they need to have accurate information, and the information they gather has become one of the richest assets of the industry.

There is, of course, nothing new in this. So what has forced legal scholars to pay closer attention to this issue?

The answer has to do with the Fourth Industrial Revolution, a phenomena that has altered the way we live, work, and relate to one another and, of course, the way in which businesses are managed[2]. The treatment of personal data has undergone a radical change due to breakthroughs in technologies such as artificial intelligence, robotics, the Internet of Things, autonomous vehicles, big data and quantum computing.

It has multiplied the sources from which data are extracted (social networks, websites, smartphones, telematic devices) and data is collected in huge quantities, whether it comes already structured or not. At the same time, increasingly sophisticated algorithms are being developed to analyse this information, creating the phenomenon that has been called «Big Data»[3]. A further factor in this process has been the perfecting of artificial intelligence

---

[2] «The Fourth Industrial Revolution has been steadily building on the Third, the digital revolution that began in the middle of the last century. The Fourth Industrial Revolution, however, is not only about smart and connected machines and systems. Its scope is much wider. There have been waves of simultaneous breakthroughs in areas ranging from gene sequencing to nanotechnology, and from renewable fuels to quantum computing. It is the fusion of these technologies and their interaction across the physical, digital and biological domains that make the fourth industrial revolution fundamentally different from previous revolutions» [Klaus Schwab, *The Fourth Industrial Revolution* (New York: Penguin Random House, 2017), 8]. This author emphasizes that there are three reasons why today's transformations represent not merely a prolongation of the Third Industrial Revolution but rather the arrival of a Fourth and distinct one: velocity, scope, and systems impact.

[3] This expression refers both to the collection and the storage of data as well as the methods of analysis applied to them. The mass compilation of information is possible thanks to the development of ICT: search engines on the internet, wireless sensors implanted in loyalty cards, in mobile devices, readers, cameras, microphones, etc. Moreover, the analytical methods applied to this information are designed to detect repetitive patterns that can serve various purposes. These include the development of predictive models, which are able to predict future events or behaviour based on the analysis of past behaviour or events. The areas in which these predictive statistical models are used are more diverse. Such models have been employed in a great number of fields, including, among others, advertising and marketing, the analysis of businesses, the fight against organized crime and security, espionage, and the offer of products and services custom tailored to the client's profile. The correct elaboration of methods of analysis and the resulting models is essential to achieving optimum results.

mechanisms that are capable of self-learning. Phenomena such as these have transformed decision making processes, introducing automated elements that reason in a new way[4]. Indeed, as O´NEILL says, «(t)he systems are built to run automatically as much as possible. That´s the efficient way; that´s where the profits are» [5]. This new framework for the treatment of personal data not only increases the ability to collect, store and process information, but also greatly reduces the associated costs. It opens up new business opportunities and competitive advantages through cost reduction and speed of decision-making.

The Fourth Industrial Revolution will undoubtedly bring about fundamental changes in the insurance sector. This is well illustrated by the auto insurance sector, in which the utility of processing mass data through predictive models is highlighted by their use to adjust premiums to customer profiles. The premiums must be high enough for the insurance company to make a profit in covering the risk, and at the same time, be attractive enough to ensure that the customer does not switch to a cheaper competitor. Auto insurance is subject to intense competition and customers invest considerable time and effort in comparing what is on the market. The younger generation, who are more at home with new technologies, are better equipped to research online through comparison sites.

Hence the importance of offering competitive products. Some insurers already offer personalized services based on telemetry. Sensors installed in the vehicle or apps hosted on the smartphone of the insured, collect and send information in real time on drivers' behaviour: including the speed at which they drive, the time they spend behind the wheel, the locations they frequent, and other key items of data. The data of each driver is compared with that of others, allowing the insurer to develop driver profiles and to assess the risk of losses such as accidents or theft. These predictive models assess future risks based on past behaviour. Thus the premium can be adjusted to suit specific risk profiles, something which has led to the coining of the phrase «pay as you drive». We might add another expression: «pay when you drive», because the same technologies permit insurers to offer products allowing the customer to choose the time frame in which they have insurance cover e.g., that can exclude time slots in which the car is parked in a garage. Telemetry enables insurers to corroborate the information provided by their clients.

However, the legitimate aspiration of insurers to take advantage of new business opportunities, is not the only aspect to consider.

---

[4] Robert D. Helfand, «Big Data and insurance: what lawyers need to know and understand», *Journal of Internet Law,* n.º 3 (2017): 1.
[5] Cathy O´Neil, *Weapons of math destruction. How Big Data Increases Inequality and Threatens Democracy* (United Kingdom: Penguin Books, 2016), 153.

The revolution in the processing of personal data increases the risk of a breach of the fundamental rights of consumers to have their privacy, autonomy and control of this information properly protected and could lead to unfair discrimination. According to BYGRAVE[6], corollaries of the trends I have described above include increases in: 1) the use of data for purposes other than the purpose for which it was originally collected («re-purposing»); 2) the potential for the misinterpretation and the misapplication of data and for the dissemination of invalid or misleading data; 3) the automation of organizational decision-making processes; 4) the blurring and dissolution of transactional contours, as business decisions concerning contracts with consumers and their contents are often adapted from profiles based on the automated treatment of data.

It is not surprising that these new technologies are raising increasing concerns as to how data is used and whether they will result in negative discrimination.

Returning to our previous example (usage-based or connected car insurance), the information used to create a client profile and to determine the insurance premium payable is directly related to the type of risk that the insurer is trying to assess: the likelihood of losses and the consequent size of the claim against the insurance company. However, insurance companies do not use this type of data solely to draw profiles of their customers and then to offer them customized products. Insurers also process information —generated by the possibilities of Big Data— that seemingly has little to do with the risk of claims, or with determining the propensity for loss. In the same way that they decide whether or not to offer an insurance policy or recalculate the amount of the premium that has to be paid, they make use of the credit history of applicants when underwriting and rating both auto and homeowner insurance policies[7].

---

[6] Lee A. Bygrave, *Data privacy Law. An international perspective* (Oxford: Oxford University Press, 2014), 9.

[7] As reported by Linda L. Golden, Patrick L. Brockett, Jing Ai & Bruce Kellison, «(i)ndications of financial behavior (such as credit-scoring variables) have been used for decades as an aid in classification and underwriting in commercial lines and life insurance. Although not used until recently in personal lines, there have been indications for more than 65 years that financial history may be related to driving accidents. Tillman, W.A. and G.E. Hobbs, W.A. (1949). The Accident-Prone Automobile Driver: A Study of the Psychiatric and Social Background. *American Journal of Psychiatry*, (106: 321-331) found that drivers with bad credit histories have repeated crashes at a rate six times higher than those with good credit history» (Linda L. Golden, Patrick L. Brockett, Jing Ai & Bruce Kellison, «Empirical Evidence on the Use of Credit Scoring for Predicting Insurance Losses with Psycho-social and Biochemical Explanations», *North American Actuarial Journal* 20:3 (2016): 233-251, doi: http://dx.doi.org/10.1080/10920277.2016.1209118).

This paper focuses on this practice, known as «credit-based insurance scoring», and examines it not only in terms of its efficiency, but also from the perspective of how consumer rights can be fairly protected. This issue is a good example to use to illustrate a number of risks that arise from the processing of personal data by insurers in the era of the fourth technological revolution. It shows that a re-examination of the value of the information that insurers manage is required and highlights the risks of its processing in the context of the digital era, where personal data has become the new oil, the new «most valuable resource in the world»[8].

Section II deals with what credit scores are and what their genuine purpose is. Section III then analyses the use of credit scores by insurers. This section has several parts which compare credit risk with insurance risk and then present the arguments in favour of and against the use of credit scores by insurers. Section IV goes on to explore credit-based insurance scores in the light of Regulation EU 2016/679. I will focus mainly on two aspects: the lawful basis for the processing of credit history data by insurers, and the rules that should apply to decisions based solely on automated processing, including profiling. Section V contains an overall conclusión.

II. **Preliminary concepts**

1. *Credit Reporting Systems and credit scoring*

Prior to examining the use of credit scores by insurers we should remind ourselves what these are and what their original purpose was.

How do banks or credit card companies decide whether a customer is to be granted credit or not? How is the price of this credit determined? Fundamental to these decisions is the evaluation of the applicant's solvency and their ability to meet repayment schedules (credit risk).

A Credit Reporting System (CRS) is an essential tool in the assessment of credit risk. It aims to monitor the collection, processing and communication of information concerning the solvency of an applicant, understood as the probability of debt repayment. Its main purpose is the exchange of information between credit market operators to assist in quickly and accurately assessing the applicant's solvency and thereby reaching informed decisions on whether

---

[8] «The world's most valuable resource is no longer oil, but data», *The Economist*, 6 May 2017, accessed December 18, 2019: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

or not to grant credit and to determine levels of interest[9]. The goal is to control credit risk, as profit and/or losses depend on it.

Credit bureaus (or credit report agencies) like Equifax, Experian, and TransUnion play a leading role. They are specialized intermediaries in gathering, selecting and storing credit data in a structured form, and verifying, statistically analysing and communicating credit reports, whilst also offering other value added services. Among these services are credit ratings known as «credit scores», portfolio tracking, the detection of fraud, functions of collection, or other relevant services for the marketing of products. Companies outsource in whole or in part the collection and processing of information on creditworthiness to such credit bureaus because it both reduces costs and speeds up their decision-making processes.

Among the complementary services that credit bureaus offer is the development of credit scores. Credit scoring is a statistical method, initiated in the 1960s in connection with the issuance of credit cards, which then spread to other sectors involved in financial services, and also to small and medium-sized companies. It has become increasingly more common as a means of measuring credit risk. It consists of assigning a number («credit score») to the borrower that quantifies the probability of a borrower repaying credit. The credit score shows lenders such as banks or credit card companies the level of risk involved in lending to the customer[10]. The number assigned to the applicant falls within a certain range, and the higher the credit score, the better the subject's chances of being accepted for credit, at the best rates. The credit rating is calculated by examining the credit history of an applicant using a statistical model or a mathematical algorithm. «Credit scores can be used in the loan approval process for simple accept/reject rules or for more sophisticated risk- based pricing rules and credit limits»[11].

----

[9] On the problems arising from the lack of homogeneity between Credit Reporting Systems among the different EU Member States, see M.ª Dolores Mas Badia, «Credit information registries in the Draft Personal Data Protection Law. A breakthrough or a lost opportunity?», *Actualidad Civil,* n.º 11 (2017): 95-96.

[10] Therefore, it has a more or less reliable predictive value depending on different parameters. The World Bank highlights that this predictive value is greater when applied to a population of borrowers that are homogeneous with respect to the type of product or credit for which their creditworthiness is being assessed. This is why different score tables are used for personal or mortgage loans, respectively [The World Bank, *General Principles for Credit Reporting* (Washington: International Bank for Reconstruction and Development/ The World Bank, 2011), 14. Accessed December 18, 2019: http://documents.worldbank.org/curated/en/662161468147557554/pdf/70193-2014-CR-General-Principles-Web-Ready.pdf].

[11] International Financial Corporation, *Credit Bureau Knowledge Guide* (Washington: IFC, 2012), 78. Accessed November 20, 2019: https://www.ifc.org/wps/wcm/connect/industry_ext_content/ifc_external_corporate_site/financial+institutions/resources/toolkits/credit+reporting+knowledge+guide

2. *Insurance risk* vs. *credit risk*

Credit risk is different from insurance risk. The former is associated with the probability that the borrower will repay the credit. In contrast, insurance risk evaluates whether the insurance applicants and policyholders are more or less likely to have insurance claims that will result in a loss for the insurer. In other words, this risk relates to the likelihood that an insured event will occur requiring the insurer to pay a claim. Insurance companies try to adjust premiums according to the risk.

III. **Credit-based insurance scoring**

1. *Concept and function*

Despite the differences between credit risk and insurance risk as described above, in some countries like the United States, Canada or Mexico large insurance companies include credit history amongst the information to be taken into account when assigning consumers to risk pools and deciding whether or not to offer them an auto or homeowner insurance policy, or to determine the premium that they will pay. This constitutes a clear example of credit reports being used for purposes well beyond their original scope. «Credit-based insurance scoring» is a practice which began in the mid-1990s[12] and the fairness of which is questioned, notably by academics and consumer organizations, as well as by regulators and legislative bodies. Critics claim that a consumer with the worst credit score —everything else being equal— can pay two, three or even four times as much as a consumer with the best credit score. The credit score is likely to have more impact on the premium than any other factor, including the driving record of applicants or the condition of their homes. It is possible that a driver with a completely clean record can pay

---

[12] A summary of the historic development of this practice can be found in Federal Trade Commission, *Credit-Based Insurance Scores: Impacts on Consumers of Automobile Insurance. A Report to Congress by Federal Trade Commission* (Federal Trade Commission, 2007), 3. Online Access on October 20, 2019 at: https://www.ftc.gov/sites/default/files/documents/reports/credit-based-insurance-scores-impacts-consumers-automobile-insurance-report-congress-federal-trade/p044804facta_report_credit-based_insurance_scores.pdf. Credit-based insurance scores were introduced by FICO in 1993. In 2011 it was estimated that 95% of automobile insurance underwriting and/or pricing and 85% of homeowner insurance were based in part on insurance scoring.

more than a driver with a history of accidents or traffic violations purely due to their credit rating[13].

To produce a credit-based insurance score, not all the variables listed in the credit score are taken into account, but only those which are considered to have a predictive value on the insurance risk. The goal is not to predict defaults on loans but rather insurance losses. On the other hand, while the decision of the insurers is not based solely on credit history, it does form part of the data that defines the risk profile, along with a great deal of information directly related with the risk of accidents and claims (e.g., in auto insurance, driving record, vehicle type, age, gender, geo-location). Not all insurance companies handle the same behavioural and financial variables but develop their own statistical credit-based insurance score[14]. The scoring models are often kept secret in full or in part, when the law allows it, because they play a significant role in competition.

The use of credit scoring in insurance underwriting and rating is certainly controversial. Before reaching any judgment on the legitimacy of this practice and the limits that should be imposed upon it, it is appropriate that we look carefully at its advantages and disadvantages.

2. *Arguments in favour*

First of all, insurance companies argue that credit scores are accurate predictors of insurance risk and as a result assist them in evaluating insurance risk more accurately and at lower cost. Furthermore, they add new information about losses not contained in traditional underwriting and rating variables. The danger of information asymmetry and adverse selection decreases, thus producing an insurance market which is more efficient. Insurers can charge each individual consumer the premium that most closely corresponds to the risk of loss he or she actually represents. It is its key strength.

It is alleged that even if there is not a causal relationship between credit score and insurance claims frequency, there is in fact a statistical correlation.

---

[13] This line of argument is pursued, among others by, O´Neil, *Weapons*, 164, who provides some figures, and Birny Birnbaum, «Credit Scoring in Insurance: An Unfair Practice», *United Policyholders* (2011), 5. Online Access on October 20, 2019 at: https://www.uphelp.org/sites/default/files/publications/credit_scoring_and_insurance_an_unfair_practice_5-11.pdf

[14] Further information in Linda L. Golden et al., *Empirical* …, 233 ss. They explain: «this score can be created either by the credit history vendor or by the insurance company itself. Many insurance companies use their own algorithms to customize credit scores based on their particular market segments».

It has been empirically proven that the frequency of claims decreases as credit scores increase[15]. The simple fact is that people with better credit ratings have fewer accidents and make fewer claims. Insurers explain this correlation by drawing a comparison between credit history and financial responsibility: an individual who pays less attention to the proper management of credit is also likely to focus less on the management of insurance risk.

Additionally, a credit score is a predictor of the likelihood a policyholder will continue to pay monthly premiums on time. However, it must be taken into account that «companies do not use credit-based insurance scores to predict payment behaviour. Rather, they use scores as a factor when estimating the number or total cost of insurance claims that prospective customers (or customers renewing their policies) are likely to file»[16].

In addition to statistical correlation and efficiency, supporters of credit-based insurance scoring say that this is completely non-discriminatory and uses no data on gender, nationality, ethnicity, address or income. In the case of the USA, the federal Fair Credit Reporting Act governs its use[17]. Only credit-related information is included. As the variables considered in the rating process are directly linked to probable losses, it

---

[15] It has been recognized by the Federal Trade Commission which, after a close study done upon requirement of Section 215 of the FACT Act (FACTA), submitted the corresponding report to Congress titled «Credit-based insurance scores: impacts on consumers of automobile insurance»: «Credit-based insurance scores (…) are predictive of the number of claims consumers file and the total cost of those claims. The use of scores is therefore likely to make the price of insurance better match the risk of loss posed by the consumer. Thus, on average, higher-risk consumers will pay higher premiums and lower-risk consumers will pay lower premiums» (Federal Trade Commission, *Credit-Based* …, 3). In the same sense see, among others, the studies of Michael J. Miller and Richard A. Smith, «The Relationship of Credit-Based Insurance Scores to Private Passenger Automobile Insurance Loss Propensity. An Actuarial Study» *(EPIC Actuaries, LLC, 2003)* -online access on November 12, 2019 at: http://www.progressive.com/content/PDF/shop/EPIC-CreditScores.pdf-; Lawrence S. Powell, «Credit-Based Scoring in Insurance Markets. Independent Policy Report» (*The Independent Institute,* 2009), online access on April 25, 2019 at: http://www.independent.org/pdf/policy_reports/2009-10-01-scoring.pdf; or Linda L. Golden et al., *Empirical*.

[16] Federal Trade Commission, *Credit-Based Insurance Scores*, 2.

[17] The federal *Fair Credit Reporting Act (FCRA)* promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies.

The Casualty Actuarial Society's Statement of Principles Regarding Property and Casualty Insurance Ratemaking (Adopted by the Board of Directors of the CAS May 1988) require insurance rates to meet three criteria. They must not be inadequate, excessive, or unfairly discriminatory. And adds: «A rate is reasonable and not excessive, inadequate, or unfairly discriminatory if it is an actuarially sound estimate of the expected value of all future costs associated with an individual risk transfer» (Principle 4). A summary of the historical background on Michael J. Miller, «Disparate Impact and Unfairly Discriminatory Insurance Rates», *Casualty Actuarial Society E-Forum,* (Winter 2009), 276-288. Online Access on November 12, 2019 at: https://www.casact.org/pubs/forum/09wforum/miller.pdf

prevents discrimination based on factors unrelated to loss. Furthermore, this standardized method is applied consistently for each and every consumer. This it is argued guarantees objectivity and fairness. However, as we will see in the next section most critics of credit-based insurance scores allege that this practice is unfairly discriminatory.

Finally, in support of the use of credit history information by insurers it is often claimed that it also brings benefits for consumers because it allows insurers to evaluate risk with greater accuracy and at lower cost. Consumers who represent a lower risk receive a reduction in premium and insurers are «more willing to offer insurance to higher-risk consumers for whom they would otherwise not be able to determine an appropriate premium» [18]. It also prevents lower-risk individuals from subsidizing the premiums of higher-risk individuals. Moreover «(s)cores also may make the process of granting and pricing insurance quicker and cheaper, cost savings that may be passed on to consumers in the form of lower premiums» [19]. It is said that credit-based insurance scoring is not a redistribution of insurance premiums but a reduction of the risk premium[20].

3. *Arguments against*

Critics deny the fact that there is a causal link between credit score and claims frequency. However, this argument does not stand up to closer scrutiny as the predictive power of the credit score is not based on a causal relationship, but on an empirically proven correlation as mentioned above[21].

There are however other negative aspects to consider, not the least of which is lack of transparency. Insurers do not advertise their use of credit information to customers. This leads the customer in the dark, generates helplessness and the complexity of the algorithms lead to a total absence of

---

[18] Federal Trade Commission, *Credit-Based Insurance Scores*, 3. However, as FTC recognize, «little hard data was submitted or available to quantify the magnitude of these benefits to consumers».

[19] *Idem*.

[20] Vance Gudmundsen, *«The history and philosophy of CBIS»* (Fair Isaac Corporation: 2010), 3. Confidential. Online Access on December 12, 2019 at: https://vdocuments.mx/the-history-and-philosophy-of-cbis.html.

[21] But still, those who point to the lack of a causal link add that simply relying on a statistical correlation with data that is easy to appreciate, such as sex, and thus incurring fewer costs than investigating the real causes, encourages insurers to avoid costlier but more accurate calculations that address the causal factors (Wouter P. J. Wills, «Insurance Risk Classifications in the EC: Regulatory Outlook», *Oxford Journal of Legal Studies*, 14 (1994): 457).

transparency[22]. Customers have no insight into when or why there should be a connection between a person's credit profile and their likelihood of making insurance claims in the future.

In some countries there is a legal obligation for notification to be given if information in your file is used against you. This is the case in the USA where the Adverse Action Notification is part of the federal Fair Credit Reporting Act (FCRA). According to this law, anyone who uses a credit report or any other form of consumer report to reject an application for credit, insurance, or employment —or to take any adverse action against you— is obliged to inform you and must provide you with the name, address, and phone number of the agency that provided the information. In the case of insurance this adverse action would be refusing coverage or demanding a higher premium. However, some would argue, that this notification requirement is not in itself sufficient to properly protect the insured. This can only be achieved by insurers providing prior information (even in advertising) about their use of credit history information and the impact that it can have on their decisions.

In the European Union, and specifically in the context of the General Data Protection Regulation (from now on, GDPR)[23], the requirement for transparency is of particular importance. As the EDPB /WP29[24] states, «it is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union»[25]. The GDPR regulates the principle of transparency in Article 5 (a) —in accordance with Recital 39— and develops it in Article 12, which applies transversally to information, communications and modalities of exercise relating to all the rights recognized in favour of the data subject. In addition to Article 12, Articles 13 and 14 GDPR detail

---

[22] More information can be found on Birnbaum, «Credit Scoring …».

[23] 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, and repealing Directive 95/46/EC (General Data Protection Regulation). DOUE L 119/1, 04.05.2016.

[24] Since 25 May 2018, Article 29 Working Party (WP29) has ceased to exist and has been replaced by the European Data Protection Board (EDPB), established by the GDPR. On 25 May 2018, the EDPB endorsed the guidance provided by WP29. The EDPB is also developing additional guidance. All of them are available here: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

[25] As pointed out in Article 29 Working Party, *Guidelines on Transparency under Regulation 2016/679* (wp260rev.01), 4-5. Adopted on 29 November 2017. As last Revised and Adopted on 11 April 2018.

the content of the right of information according to whether personal data has been collected from the data subject (Article 13 GDPR) [26] or has not been obtained from him or her (Article 14 GDPR)[27] [28]. In the first case, the information must be made available «at the time the data is requested, prior to collection or registration». When the processed data have not been collected from the data subject, the controller shall provide the information «within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed» (Article 14 GDPR)[29].

According to the European regulation, the data subject must be informed, among other issues, of the purposes and legal bases of the processing and where the processing is based on point (f) of Article 6(1) the legitimate interests pursued by the controller or by a third party for which data processing serves must be made known to the data subject. Therefore, if insurance companies use customer credit information in order to determine the premium to be paid or to make other decisions affecting the customer, they should warn the customer as indicated above. If the data handled comes from sources other than the data subject (as is the case when a credit report system is consulted), he or she must also be informed about the sources from which this personal data was obtained.

In addition, the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR requires an increment

---

[26] The EDPB/WP29 considers, in its Guidelines on Transparency under Regulation 2016/679, as data collected from data subject, those that a data subject consciously provides to a controller (e.g. when completing an online form); or those that the controller collects from a data subject by observation (e.g. using automated data capturing devices or data capturing software such as cameras, network equipment, Wi-Fi tracking, RFID or other types of sensors).

[27] In summary, as is pointed out in the EDPB/WP29, «Transparency is an overarching obligation under the GDPR applying to three central areas: (1) the provision of information to data subjects related to fair processing; (2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and (3) how data controllers facilitate the exercise by data subjects of their rights» (*Guidelines* …).

[28] Articles 13 and 14 GDPR refer to some exceptions -not entirely identical in both precepts- to the obligation to provide information. They address the following circumstances: the data subject already has the information; the provision of such information is impossible or would involve a disproportionate effort; the data controller is subject to a national law or EU law requirement to obtain or disclose the personal data and that the law provides appropriate protections for the data subject's legitimate interests; or an obligation of professional secrecy exists.

[29] If the personal data are to be used for communication with the data subject, the controller shall provide the information at the latest at the time of the first communication to that data subject; and if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed (article 14.3 (b) and (c) GDPR).

of the information that is offered to the data subject. In such cases, the controller (here the insurer) must provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Articles 13(2) (f) and 14(2) (g) GDPR). I will return to this issue in more detail in a later heading.

It is important to note that if the data were initially collected for a particular purpose such as assessing the creditworthiness of the data subject in order to decide whether and under what conditions credit was to be granted, and afterwards it were going to be used for a purpose other than that for which the personal data was collected, such as assessing insurance risk and taking appropriate decisions on that basis, the controller must provide the data subject, prior to that further processing, with information on that other purpose, and also with any relevant further information. In addition, that other purpose must be covered by the corresponding legitimate grounds from among those set out in Article 6(1) GDPR.

The problems associated with the use of credit information by insurers do not end here. It is not uncommon that credit history records contain inaccurate information[30]. In other instances, although the information may be accurate no consideration is given to the level of culpability of the individual. This occurs when the non-payment of a debt is due to misfortune, i.e. to circumstances beyond the control of the subject, such as illness or the loss of employment due to an economic crisis[31].

The use of credit history by insurers reduces the incentive for individuals to behave in a more responsible and thus less risky way. This is understandable if the credit score is considered to have more impact on the premium than any other factors, including the driving record or the condition of the subject´s home.

---

[30] A good example of this is offered by the successive annual reports of the AEPD, which reflect a worrying trend by giving an undesirable prominence to «credit blacklists». They constitute the area with the highest overall amount of sanctions imposed by the Spanish supervisory authority and the one that has given rise to the greatest number of legal actions initiated by the supervisory authority in recent years (M.ª Dolores Mas Badia, «Credit information registries in the Draft Personal Data Protection Law. A breakthrough or a lost opportunity?», *Actualidad Civil*, n.º 11 (2017): 94).

[31] Among many other authors, this is highlighted by Marco Celentani, «El intercambio de información y el funcionamiento del mercado de crédito», in *Préstamo responsable y ficheros de solvencia*, coord. by Lorenzo Prats Alventosa and Matilde Cuena Casas (Cizur Menor: Thomson Reuters-Aranzadi, 2014), 93. Insofar as credit information does not make it possible to assess the debtor's solvency accurately, it is more than questionable whether his rights and interests, and in particular his fundamental rights, can be sacrificed on that basis. I have already drawn attention to this in M.ª Dolores Mas Badía, «Los ficheros de solvencia patrimonial y crédito en España: Algunas cuestiones pendientes», in *Nuevos retos jurídicos de la sociedad digital* (Cizur Menor: Thomson Reuters-Aranzadi, 2017), 217.

Furthermore, instances of unfair discrimination may arise. As the Federal Trade Commission has recognized, the use of these scores results in low-income consumers and members of minority groups paying higher premiums than other consumers[32]. This issue is one of the most hotly debated between supporters and detractors of credit based scoring.

At this point it is appropriate to consider the current controversy regarding anti-discrimination legislation in the field of insurance. The experts are divided when it comes to concluding whether or not absolute prohibitions of discrimination (such as gender discrimination) are compatible with proper risk selection, insurance pricing and even the solvency management of insurance companies.

As is often pointed out in the legal literature, the price of insurance (the premium) has a special feature compared to that of other services that are calculated on the basis of actual costs. In the case of insurance, by contrast, the «pure premium» is, in principle, assessed by estimating the statistical insurance risk. The price must be sufficient to cover the liabilities arising from the expected claims, which makes it a matter of actuarial technique. The great advances in the application of mathematics and statistics in the field of insurance (the law of large numbers —LLN—, the calculation of probabilities) have made it possible to overcome the concept of insurance as merely a gamble or subject to chance alone, by establishing it on a firmer scientific basis, «which is no longer a mere instrument but part of the essence of private insurance»[33].

The question then, is whether it is legitimate or convenient for the legislator to impose interference in matters referring to legal policy considerations —such as those derived from the protection of certain vulnerable groups— on these actuarial calculations, even if they imply an

---

[32] Federal Trade Commission, *Credit-Based*…, 3-4. In particular, it points out that «Credit-based insurance scores are distributed differently among racial and ethnic groups, and this difference is likely to have an effect on the insurance premiums that these groups pay, on average».

[33] M.ª José Morillas Jarillo, «Fundamentos de la ordenación de seguros privados y derechos fundamentales», in *Supervisión en seguros privados: Hacia solvencia II. Actas del Congreso de Ordenación y Supervisión en Seguros Privados. Valencia, 15 y 16 de septiembre de 2011*, dir. Vicente Cuñat Edo and Juan Bataller Grau (Valencia: Tirant Lo Blanch, 2013), 48-49 and cited authors. The translation is mine. Veiga Copo introduces nuances to this perspective. The insurance contract, he says, is an aleatory contract, but this does not prevent «the insurance technique from being less and less random or, if you prefer, anti-random» «(…) the insurance contract is random per se, another thing is that the actuarial-statistical insurance technique as well as the business activity are increasingly studied, more anti-random. One question is risk, and another is how an insurance company assumes it in figures» -Abel B. Veiga Copo, *El seguro. Hacia una configuración del contrato* (Cizur Menor: Thomson-Reuters-Civitas, 2018), 57, 71- (the translation is mine).

inconsistency with the principles of sufficiency and equity or, what is the same, with the results that are considered correct from the point of view of pure economic-actuarial calculation. These regulatory interferences are not unknown, on the contrary, in the international sphere and, specifically, in European Union law. They respond to the consideration of factors linked to fundamental rights of the person, widely recognized in the Declarations of Human Rights and in the Constitutions of other social democracies, such as the right not to suffer any discrimination based on the grounds of sex, race, colour, ethnic or social origin, genetic characteristics, language, religion or belief, political or other opinions, membership of a national minority, property, birth, disability, age or sexual orientation (Article 21 Charter of fundamental rights of the European Union). This principle of equal treatment is so widely proclaimed that it would be pointless to cite all the rules of international law that reflect it here. In order to strengthen the guarantee of these rights, the European Union has created what is known as anti-discrimination law (which originated in the field of employment law and later spread to other contractual spheres, particularly finance), with a clear and controversial impact on insurance law[34].

---

[34] The debate is built on a certain normative framework and the jurisprudence that has interpreted it. Among the rules that define the legal framework, the following stand out: Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin (OJ L 180/22, 19.7.2000); Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services (OJ L 373, 21.12.2004); and the Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation COM/2008/0426 final. The fact is that these dispositions include general prohibitive rules aimed at avoiding discrimination but, at the same time, contain exceptions, which function, in the field of insurance contracts, precisely in the area of the peculiarities of the pricing of such contracts, to which I referred earlier.

Council Directive 2004/113/EC, restricts the use of the gender factor which, among other things, affects the private insurance sector. It states that Member States may decide «to permit proportionate differences in individuals premiums and benefits where the use of sex is a determining factor in the assessment of risk based on relevant and accurate actuarial and statistical data» —Article 5(2)—. This rule was echoed in Article 1:207 in the Principles of European Insurance Contract Law (PEICL), in its 2009 version, and in the national laws implementing the Directive.

However, the impact of a very important judgment could end up curtailing the exception by turning the prohibitive rule into an absolute one and causing the modification of the previous rules (as an example, the version of the PEICL of 2015, already adapted to the ruling, which goes on to make a clear statement: «Gender, pregnancy, maternity, nationality and racial or ethnic origin shall not be factors resulting in differences in individuals' premiums and benefits»). I refer to the Judgment of the Court (Grand Chamber) of 1 March 2011. Association Belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministres, Case C-236/09 (ECLI:EU:C:2011:100), known as the Test-Achats case. It radically prohib-

I cannot go into detail on this issue, given the limitations of the scope of this work. However legal literature is divided between those who agree with the radical prohibition of considering certain factors, such as sex, when setting insurance premiums and those who believe that it is better to permit proportionate differences in individual premiums and benefits where the use of sex is a determining factor in the assessment of risk based on relevant and accurate actuarial and statistical data. In favour of the first position it is argued that the opposite would hinder the desirable objective of equal treatment between men and women and the same could be said of equality in terms of other factors, perpetuating the marginalisation of certain groups[35]. Underlying these ideas is the radical respect for human dignity that must characterise the social rule of law. On the other hand, those in favour of admitting exceptions to the prohibition of considering factors such as gender in the area of private insurance contracts argue that there is no discrimination when people are treated unequally because they are not in fact in a comparable or analogous situation, since they have a statistically proven different propensity to making claims according to their sex or other factors, which does not mean that the sex, or the factor considered, is the cause of the claim[36].

IV. Some observations in the light of the regulation (EU) 2016/679

In the event that the use of «credit-based insurance scores» is deemed acceptable, the challenge for legislators is to formulate a legal and regulatory framework which imposes adequate quality parameters to ensure

---

its, without exception, insurers from calculating premiums based on the sex of the customer, as of 21 December 2012. And this is the case, even if a correlation is statistically proven between sex and, for example, life expectancy, or the number of car accidents suffered, or the frequency of use of medical benefits.

[35] In this context, some significant recent legislative developments have taken place in Spain. I am referring to Law 4/2018, of 11 June, which modifies the consolidated text of the General Law for the Defence of Consumers and Users and other complementary laws, approved by Royal Legislative Decree 1/2007, of 16 November. It seeks to avoid discrimination against people living with HIV/AIDS, «or other health conditions» (an expression, moreover, that is ambiguous and open, which will undoubtedly cause problems in the field of insurance).

[36] In this sense argue, among others, Abel Veiga Copo and Sánchez Graells, «Discriminación por razón de sexo y prima del contrato de seguro», *Revista de responsabilidad civil, circulación y seguro*, n.º 4 (2011): 17-18; or Morillas, «Fundamentos», 72 ss. The latter author writes, with reference to the Test-Achat case: «The question that needs to be asked is not whether the practice of adjusting premiums to take into account the sex of the insured party when this affects the risk covered is contrary to the principle of equality, but whether a single judgement might, by hurling a depth charge into its path, affect the true essence of the insurance premium, that is the principles of equity, mutuality and sufficiency».

not only the efficiency of this practice but also to avoid transgressions of the rights and interests of consumers. These rights include the right to the protection of personal data, which is fundamental to EU law[37]. The use of the credit history information by insurers in Europe is not as deeply rooted as in the USA, as is witnessed by the lack of academic studies on this issue. However, it is to be expected that this will change[38]. It will then be essential to comply with the derivative requirements of 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, and repealing Directive 95/46/EC (General Data Protection Regulation —GDPR—).

In this section, I will try to establish some conclusions about the requirements and limits to which the use of credit history data by insurers should be subject in the European Union. Those will be determined in the light of the Regulation (EU) 2016/679. This regulation, that came into force on 24 May 2018, not only forms the backbone of personal data protection in the EU, but is also considered a model beyond its borders as was already the case with the Directive 95/46/EC. Due to space limitation, I will concentrate on two aspects: the lawful basis for the processing of credit history data by insurers, and rules that should apply to decisions based solely on automated processing, including profiling.

1. *Lawful basis for processing of credit history information by insurers*

The first question that arises is whether the use of credit history by insurers in underwriting and risk assessment should be a factor in deciding whether or not to offer insurance coverage or the level of premium and whether or not the consent of the customer should be required.

Article 6(1) GDPR sets out an exhaustive list of the lawful bases for personal data processing[39]. In doing so, it gives consent [referred to in

---

[37] Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16.1 of the Treaty on the Functioning of the European Union.

[38] In Italy, a research study carried out by CeTIF and Crif in 2017, presented at the Catholic University of Milan, analyzed the use of Credit history information by the insurers, and conclued in favor of its utility.

[39] The processing of personal data is only lawful if one of the six legal grounds listed in Article 6 GDPR apply. They are the following: consent given by the data subject (Article 6.1 (a) GDPR); necessary for the performance of a contract or the application of pre-contractual measures (Article 6.1 (b) GDPR); necessary for compliance with a legal obligation (Article 6.1 (c) GDPR); necessary to protect vital interests (Article 6.1 (d) GDPR); necessary for the performance of a task carried out in the public interest or exercise of official au-

Article 6.1 (a)] and the other bases that support the lawfulness of such processing [spelled out in Article 6(1) (b) a (f)] the same importance. It should be noted that in cases which do not require consent because other considerations outweigh this do not remove the need to respect the other requirements and limits laid out in the GDPR (lawfulness, fairness and transparency[40], purpose limitation, data minimization, accuracy, storage limitation, identity and confidentiality, accountability and all the rights and security measures that the GDPR prescribe). In particular it will be necessary that any of the other lawful bases for data processing other than consent outlined in Article 6(1) GDPR is fulfilled. These include, notably, for the purposes that now interest us, the base collected in paragraph (f) of the Article 6(1) GDPR[41], referring to the case in which such processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual which require protection of personal data, what must be determined by applying the principle of proportionality[42].

----

thority (Article 6.1 (e) GDPR); necessary for the legitimate interest pursued by the controller or by a third party (Article 6.1 (f) GDPR). Article 6 GDPR formally places these grounds on the same level. That is to say, any of them is a general rule with the rest being exceptions. In compliance with the principle of accountability, every controller must ensure that one of these grounds is in place before processing is carried out and throughout the entire duration of the processing.

[40] The lack of transparency is one of the negative aspects of the practice that we are analysing, as I have emphasized in previous pages.

[41] It could be considered that the use of credit information by insurers is also in line with the grounds collected in paragraph (b) of the Article 6(1) GDPR: «processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract». However, the EDPB/WP29 performs a restrictive interpretation of the lawfulness of this basis for the processing of data, that would exclude the case analysed from its application (EDPB/WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/ EC. Adopted on 9 April 2014. WP217*, 16-18. Online Access on November 15, 2019 at: http:// www.dataprotection.ro/servlet/ViewDocument?id=1086). Article 6(1)(b) GDPR may include, for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to effect payment. In the employment context this ground may allow, for example, processing salary information and bank account details so that salaries could be paid. But the provision must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some data processing is covered by a contract does not automatically mean that the processing is necessary for its performance. Article 6(b) only applies to what is necessary for the performance of a contract. It does not apply to all further actions triggered by non-compliance or to all other incidents in the execution of a contract.

[42] Recital 47 provides further explanations.

This lawful basis for data processing has a particular importance for us. There are various interests to consider: the insurer's interest in controlling insurance risk, the general interest in the stability and successful operation of the financial markets, the free movement of data and healthy competition, and the interests of consumers themselves in accessing insurance on advantageous terms and in controlling his or her personal data. The key lies in clarifying when interference in the right to data protection is justified by the presence of other such interests and when not[43]. For this purpose, the principle of proportionality, explicitly mentioned in Article 52 of the Charter of Fundamental Rights of the European Union[44], is essential. The proportionality principle in a broad sense (not written until Maastricht Treaty —Article 3B TEU—) is composed of three sub-principles: usefulness or suitability of the average employee in relation to the purpose pursued; need —there cannot be any less onerous way of achieving the aim—[45]; and proportionality *strictu sensu*, which ensures a balance in the cost-benefit ratio.

The sacrifice of the fundamental rights or interests of the insured or policyholder[46] can only be justified by the proportionate satisfaction of

---

[43] On this question see EDPB/WP29, *Opinion 06/2014*, 1-68. Although the opinion is issued on Directive 95/46/EC, with references to the draft Regulation, its conclusions are perfectly transferable to the GDPR. In particular, Article 7 of the Directive is equivalent, «mutatis mutandi», to Article 6 GDPR.

[44] DOCE, C 364/1, 18.02.2000. Article 52 states: «1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others».

[45] On another level, in order for this legal ground to operate, the processing of personal data must be «necessary» for the satisfaction of the legitimate interest of the controller (or third parties) that prevails, in the sense that no other less invasive means are available to reach the envisaged purpose (see Article 6(1)(f) and 5(1)(c) GDPR). One of the most important factors to consider when applying the balancing test of Article 6(1)(f) GDPR is the impact of the processing on the interests or fundamental rights and freedoms of the data subject. Both positive and negative consequences should be taken into account. In assessing the impact of the processing different aspects will be taken into account: the nature of the data; the way data are being processed; reasonable expectations of the data subject; status of the data controller and data subject; or potential sources of risk that may lead to impact on the individuals concerned, the severity of any impacts on the individuals concerned and the likelihood of such impacts materialising (*Opinion 06/2014*, 36-41).

[46] According to the interpretation of the EDPB/WP29 in the *Opinion 06/2014*, the reference to the interests or fundamental rights and freedoms of the data subject should have to be interpreted broadly: all relevant interests of the data subject should be taken into account. «This interpretation of the text makes sense not only grammatically, but

other legitimate interests of the insurer and the general interest in properly assessing the insurance risk and the level of premium appropriate to the level of risk[47]. However, it is unclear which of the interests involved should carry more weight for the purposes of Article 6.1.f GDPR. It seems that one cannot establish a general rule in this regard. The heated doctrinal controversy aroused by this practice in countries in which it has increased in the last decade, such as the USA, as well as the fact that, after

----

also when taking into account the broad interpretation of the notion of the 'legitimate in-terests' of the controller. If the controller - or the third party in the case of disclosure - can pursue any interests, provided they are not illegitimate, then the data subject should also be entitled to have all categories of interests to be taken into account and weighed against those of the controller, as long as they are relevant within the scope of the Direc-tive». (*Opinion 06/2014*, 30).

Concerning the negative impact of the data processing, *Opinion 06/2014* explains that negative consequences «may include potential future decisions or actions by third parties, and situations where the processing may lead to the exclusion of, or discrimina-tion against, individuals, defamation, or more broadly, situations where there is a risk of damaging the reputation, negotiating power, or autonomy of the data subject. (…) The Working Party emphasises that it is crucial to understand that relevant 'impact' is a much broader concept than harm or damage to one or more specific data subjects. 'Impact' as used in this Opinion covers any possible (potential or actual) consequences of the data processing (…) concept is unrelated to the notion of data breach and is much broader than impacts that may result from a data breach» (*Opinion 06/2014*, 37). In any case, it is important to note, as does the EDPB/WP29, *Opinion 06/2014*, 41, that not all negative impact on the data subjects weighs equally on the balance. The purpose of the balancing exercise «is not to prevent any negative impact on the data subject. Rather, its purpose is to prevent disproportionate impact. This is a crucial difference». Moreover, «it should be kept in mind that processing of personal data having an impact on a minority of data subjects - or even a single individual only - still requires a very careful analysis espe-cially if such impact on each individual concerned is potentially significant» (*Opinion 06/2014*, 38).

WP29 also draws attention to the importance of preventive measures: «Considering that establishment of a case for compensation of a suffered harm or damage is often dif-ficult for the data subjects in this context, even where the effect itself is very real, it is all the more important to focus on prevention and ensuring that data processing activities may only be carried out, provided they carry no risk or a very low risk of undue nega-tive impact on the data subjects' interests or fundamental rights and freedoms» (*Opinion 06/2014*, 37).

[47] Under the accountability principle, the controller himself is the one who, before proceeding with the processing on the basis of Article 6.1 (f) GDPR, is obliged to assess whether he has a legitimate interest, whether the processing is necessary to satisfy that le-gitimate interest and whether it prevails over the interests and rights of the data subjects in that specific case. The ECDC/WG29 recommends that the controller should document this balancing test in a sufficiently detailed and transparent way so that the complete and cor-rect application of the balancing test could be verified - when necessary - by relevant stake-holders including the data subjects and data protection authorities, and ultimately, by the courts (*Opinion 06/2014*, 43).

exhaustive analyses, different States of the USA have followed different paths is testament to this [48]. Ultimately, if there is a legal dispute it will be the Courts that will determine the outcome[49]. Circumstances will be the deciding factor: what if there could be an equally effective model at a reasonable cost which shows greater respect for Insurance consumer rights? This would provide a valid alternative to credit-based insurance scoring.

There is one factor which could tip the balance in favour of the requirement of the consent of the customer for the insurance company to be able to access your credit data and that is the fact that this data was collected at the time, in order to assess the solvency of the individual (the probability of prompt debt repayment). Insurance companies use the data for an entirely different purpose, namely to assess insurance risk i.e. the probability of losses as a result of customer claims. That said, the need for consent would be excluded if it were proven that there is a prevailing legitimate interest of the insurers or general interest in the use of the credit data —Article 6(1)(f) GDPR)—. However, to this effect, it would not be enough to prove the existence of a legitimate interest based on the statistical correlation between a good or bad credit history and a lower or higher accident rate and, consequently, the service that this type of data can provide to correct asymmetries of information and to avoid adverse selection problems and set the premium to be paid by each customer more accurately[50]. It would also be

---

[48] In USA, there are important differences between States. «Typically states will not allow credit-based insurance scores to be used as the sole basis for increasing rates or denying, cancelling or not renewing policies. Some states prohibit credit-based insurance scores being used as the sole basis in underwriting or rating decisions. Some states require insurers to notify applicants or insureds that adverse credit-related decisions have been taken regarding pending applications or existing coverage based on the consumer's credit score. A few states, (Georgia, Hawaii, Maryland, Oregon, and Utah), have established prohibitions on the use of credit history information in certain circumstances» (National Association of Insurance Commissioners —NAIC—, «Credit-Based Insurance Scores», Last Updated 12/7/18. Online Access on December 20, 2019: https://www.naic.org/cipr_topics/topic_credit_based_insurance_score.htm).

[49] The balancing test cannot be made in absolute terms by the legislator, but must be made by the controllers and may be judicially reviewed. The legislator can only establish presumptions in this respect. In this sense, the Spanish Council of State pronounced itself in the Mandatory Opinion issued on the preliminary draft of the Organic Law on the Protection of Personal Data, issued on 26 October 2017 - File number: 757/2017-, https://www.boe.es/buscar/doc.php?id=CE-D-2017-757. Further details are provided in M.ª Dolores Mas Badia, «Credit reporting systems and protection of personal data: a European regulation and an organic law conceived but still unborn», *Actualidad Civil*, n.º 5 (2018).

[50] In accordance with the EDPB/WP29, *Opinion 06/2014*, 25, in order to be relevant «a 'legitimate interest' must therefore: be lawful (i.e. in accordance with applicable EU and national law); be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific); represent a real and present interest (i.e. not be speculative)».

necessary to conclude that this interest is superior to the interests, rights and freedoms of the customer, including his fundamental rights. I believe that, insofar as it is possible to carry out the actuarial calculations necessary to set the premium, disregarding the credit data, in a less invasive way or with less interference in the rights and interests of the consumer, it would be difficult to defend this prevalence and the consent of the data subject would have to be sought.

In any case, it must be said that the exigency of consent if not supported by other measures does not provide sufficient protection for the consumer as it is often the case that insurance coverage and advantageous premiums are conditional on such consent being given. The consumer is therefore more or less compelled to grant consent[51]. Measures should be established to correct this practice.

The notion of freely given consent is closely related to an idea taken into account in the GDPR and emphasised by the EDPB/WP29 in the *Guidelines on consent under Regulation 2016/679[52]*: The possible existence of an imbalance of power in the relationship between the controller and the data subject. This imbalance of power may (but does not necessarily) imply that the data subject has been unduly influenced or pressured so that the consent given cannot be considered truly free, in which case it will not be valid.[53]

---

[51] «In most states *(USA)* insurers can do pretty much what they want with your credit information because most insurers today will only quote you a very high premium if you refuse to allow the insurer to obtain your credit story. And once you have a policy with an insurer, the insurer can check your credit story whenever it wants to» (Birnbaum, «Credit Scoring»).

[52] EDPB/WP29, *Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2018.* WP259 rev.01. Online Access on December 10, 2019: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[53] The EDPB/WP29, *Guidelines on consent*, 6-7, illustrates these situations of imbalance with some examples. There is often i.e. a clear imbalance of power in the relationship between a public authority and a citizen, or in the employment context. However this does not mean that public authorities or employers can never rely on consent as a lawful basis for processing. There may be situations when it is possible for them to demonstrate that consent actually is freely given. In any case, that of public authorities or employers are just that, examples, which does not exclude that such an imbalance may occur in other types of relationships. As the EDPB/WP29 emphasizes, if the data subject has no real choice, feels compelled to consent or will endure negative consequences if they do not consent (e.g. substantial additional costs), then consent will not be valid. Some clues to assess whether or not consent has been freely given are offered by Recital 43 GDPR: «Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance». As it points out the EDPB/WP29, «in doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract» (*Guidelines on consent*, 8).

The burden of proof that consent was freely given shall lie with the processing data controller, in accordance with the accountability principle that permeates the entire GDPR (I refer to Recital 42 GDPR, in this sense). It is the controller who must be able to provide evidence that there will not be negative consequences for the data subject if he or she does not consent[54].

It is important to point out that in those situations in which the imbalance of power to which I have referred exists, this may lead to considering that consent, due to its vulnerability, is not the most appropriate ground for legitimate personal data processing, it being preferable to resort to another of the legal grounds listed by Article 6 GDPR, notably the existence of a prevailing legitimate interest (Article 6.1(f) GDPR).

At this point, we should ask ourselves whether, in the context of the conclusion of an insurance contract, and as far as the use of credit information is concerned, there may exist a situation of imbalance of power between the data controller (insurer) and the data subject (customer). This does not seem to be the case when market competition enables the consumer to conclude a similar insurance contract with another insurer that does not require him to process his credit information.

In any case, it is interesting to note how data protection rules can be combined with competition law and consumer and user protection rules to ensure that the rights and interests of data subjects are not unduly harmed in situations of unequal power[55].

2. *Decisions based solely on automated processing, including profiling*

Technological advances favour automated decision-making, often based on subject profiling. This undoubtedly makes for the faster adoption of decisions and the reduction of costs. It also makes it possible to offer personalized products or services or to better control certain risks (insolvency, fraud, etc.). However, it increases the risks to privacy and the fundamental right to the protection of personal data of the individual

---

[54] Recital 42 GDPR and the *Guidelines on consent*, 11. This admits that the above idea does not exclude the possible offer of incentives if consent is given. It is worth asking whether it would be admissible, as an incentive, an improvement in the insurance premium. In my opinion, it could be if the difference in the premium to be paid depending on whether or not the customer consents to the processing of his or her credit data by insurer was actually justified by the greater efficiency in calculating the insurance risk and was proportionate in this respect, in addition to complying with all the guarantees established by the GDPR and the complementary regulations.

[55] In this sense, the EDPB/WP29, *Opinion 06/2014*, 40.

concerned. Moreover, automated decisions, especially when they are based on profiling, are likely to mask biases that are not always obvious and may lead to unfair discrimination. The seriousness of the consequences for individuals (think, for example, of the refusal of an insurance contract, based on profiling) is accentuated in the case of particularly vulnerable groups. These risks run parallel to the opacity of the processes. Often people are not aware that a profile is being created on them or do not understand what it involves.

As the EDPB/WP29 has highlighted, «(p)rofiling and automated decision-making are used in an increasing number of sectors, both private and public. Banking and finance, healthcare, taxation, insurance, marketing and advertising are just a few examples of the fields where profiling is being carried out more regularly to aid decision-making. Advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms. The widespread availability of personal data on the internet and from Internet of Things (IoT) devices, and the ability to find correlations and create links, can allow aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted»[56].

The same document summarizes the risks of automated decision-making based on subject profiling: «Profiling can perpetuate existing stereotypes and social segregation. It can also lock a person into a specific category and restrict them to their suggested preferences. This can undermine their freedom to choose, for example, certain products or services such as books, music or newsfeeds. In some cases, profiling can lead to inaccurate predictions. In other cases it can lead to denial of services and goods and unjustified discrimination»[57].

The GDPR introduces new provisions to address the risks arising from profiling and automated decision-making, notably, but not limited to, privacy. It does so by means of a set of rules distributed in its articles that address the following aspects: transparency and fairness requirements; proactive liability obligations; specific legal grounds for processing; specific rights to object to decisions based solely on automated data processing, including profiling; and impact assessments. Among all these rules, especially outstanding is Article 22 GDPR, that takes over from

---

[56] EDPB/WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)*, 5. Online Access on December 10, 2019: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

[57] EDPB/WP29, *Guidelines on Automated individual decision-making*, 5-6.

Article 15 of Directive 95/46/CE[58]. Recital 71 explains the rule. As a general rule, every «data subject shall have 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» (for example, an individual is denied a loan, or citizenship, or a public subsidy, or a job opportunity). Or, if preferred, there is a general prohibition on taking individual decisions based solely on automated processing, including profiling, which produce legal effects or similarly, significantly affects the person (the EDPB/WP29 advocates the «prohibition» perspective as being more protective). The general rule of prohibition admits a series of exceptions, always accompanied by appropriate guarantees.

If automated decisions are made that significantly affect the subject, without relevant human intervention, the provisions of Article 22 GDPR will apply.

To begin with, it will be necessary to make a distinction between cases where the decision whether or not to grant coverage and at what level of premium is based «solely» on automated processing including profiling —set of facts of the article 22 GDPR— (as can happen with an automated online decision to grant insurance), and where it is not. An automated process produces what is, in effect, a recommendation regarding the person concerned. If a human being reviews and takes into account other factors in making the final decision, that decision will not be «based solely» on the automated

---

[58] The article 22 GDPR establishes: «Automated individual decision-making, including profiling

1. The data subject shall have 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.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place».

processing, provided that the human intervention is significant and not merely symbolic. We will not therefore be in the case considered in Article 22 GDPR if the insurance company does not automatically take the decision on the basis of the credit-based insurance score, but crosses the outcome of the profiling with other information and with significant human intervention.

On the other hand, one should not think that automated decisions and profiling always go together. To understand this, it is necessary to specify these concepts.

Article 4(4) GDPR defines «profiling» as «any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements».

As the EDPB/WP29 explains[59], profiling is a procedure which may involve a series of statistical deductions. It is often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar. Profiling may involve three distinct stages: data collection; automated analysis to identify correlations; applying the correlation to an individual to identify characteristics of present or future behaviour.

Decisions based solely on automated processing represent the ability to make decisions by technological means without human involvement. Automated decisions can be made with or without profiling (EDPB/WP29, Guidelines)[60]. On the other hand, there may be decisions that are not based solely on automated data processing but also include profiling. This would be the case, e.g., if the insurer took into account the profiling of the client before granting the insurance or determining the premium to be paid, but other significant human interventions took place before any decision was made about the individual.

Thus, e.g., when applying for online insurance, if a person decides whether to approve the insurance on the basis of a profile drawn up

---

[59] EDPB/WP29, *Guidelines*, 7.

[60] The EDPB/WP29 illustrates this variety of possibilities with the following examples: «Imposing speeding fines purely on the basis of evidence from speed cameras is an automated decision-making process that does not necessarily involve profiling. It would, however, become a decision based on profiling if the driving habits of the individual were monitored over time, and, for example, the amount of fine imposed is the outcome of an assessment involving other factors, such as whether the speeding is a repeat offence or whether the driver has had other recent traffic violations».

solely by means of automated processing, this is a «profiling decision» which does not fit in the scope of Article 22(1) GDPR, as there is human intervention. On the other hand, in the case where an algorithm decides whether the insurance should be approved and the decision is automatically transferred to the person concerned, without any prior and meaningful assessment by a human being, we are dealing with a decision based «solely» on automated processing, including profiling, which produces legal effects on the data subject or significantly affects him/her in a similar way (case that falls within the scope of Article 22(1) GDPR). The cases covered by Article 22(1) GDPR are subject to specific safeguards and restrictions.

In accordance with the accountability principle, I understand that it is the burden of the data controller to prove that the decision was not based solely on the automated processing, or that one of the exceptions to the prohibitive rule to which I will refer later, applies.

Once it is established that it will be necessary to make a distinction between cases where the decision whether or not to grant coverage and at what level of premium is based «solely» on automated processing including profiling —by reference to the set of facts contained in article 22 GDPR— and where it is not, the following conclusions can be drawn from that precept:

1.º It establishes a prohibitive general rule. In other words, in principle, the decision on whether or not to grant insurance or in order to modify the conditions of the insurance should not be taken automatically, including by profiling.

2.º The prohibitive general rule supports exceptions. Such decisions can be based solely on the profile drawn by automated data processing in the following cases, subject to appropriate guarantees, which relate to the right to information, to obtain human intervention, to express a point of view or to challenge the decision on the part of the data subject[61]:

— If it is necessary for the entering into, or performance of, a contract between the data subject and a data controller —the insurer in the hypothesis analysed— (Article 22(2)(a) GDPR). In this

---

[61] Even if we are in one of the three cases referred to, decisions shall not be based on special categories of personal data referred to in Article 9.1 GDPR (those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), unless point (a) or (g) of Article 9.2 GDPR applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

case, «the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision» (Article 22(3) GDPR). In any case, I find it difficult to defend the need to operate, in relation to the subject matter, through purely automated decisions. It should be remembered that the exception refers to the automated decision being «necessary» for entering into, or performance of, the contract. «Necessity» shall not be considered to exist when effective, less invasive means exist to achieve the same objectives.

— If the data holder has explicitly consented to it (on the consent requirements, see Article 7 GDPR)[62]. It should be understood that the consent to which the Article 22(2)(c) GDPR refers, is not simply the consent to a solvency check by the insurer but is the customers consent to the decision on whether or not to grant cover and at what level of premium being based solely on automated processing, including profiling. Just like in the previous case, «the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision» (Article 22(3) GDPR).

— If the decision based solely on automated processing is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. That is to say, even in the absence of the consent of the person concerned, the European or national legislator could exclude the automated adoption of the decision by the insurers from the general rule of Article 22(1) GDPR being subsumed in

---

[62] What additional requirements are necessary to consider that there is explicit consent beyond those required for «normal» consent in Article 4(11), 6(1), 7 and concordant with the GDPR? In the EDPB/WP29 *Guidelines*, explicit consent is understood to consist of the following behaviours: the consent is confirmed explicitly by a written statement signed by the data subject; in the context of electronic communications, the consent is given by filling in an electronic form, sending an e-mail, uploading a scanned document with an individual signature or using an electronic signature; consent may be given via an automated telephone conversation, provided that the information on the options is fair, intelligible and clear and asks for specific confirmation from the data subject (e.g. by pressing a button or providing verbal confirmation). It should not be forgotten that the controller must be able to prove that he has obtained explicit consent in cases where such consent is required.

Article 22(2)(b) GDPR. But then, for the exclusion to be legitimate it would be necessary to «implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests». These measures must include «the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision». In my opinion, it should be obligatory for insurers to communicate to the consumer the information on which the decision is based and the source from which it is drawn thereby giving the consumer the possibility to defend their rights.

However, even if the case was assumed to be subsumed in one of the exceptions of Article 22(2) GDPR, I consider that the measures to guarantee the rights and interests of the debtor concerned should necessarily include «the right to obtain human intervention on the part of the controller», and allow the data subject «to express his or her point of view and to contest the decision» (Article 22(3) GDPR)[63].

Whether we find ourselves in the general rule of prohibition or in one of its exceptions, the principle of transparency that permeates the GDPR requires, in the case of profiling and automated decision-making, that consumers are given access to their profiles, as well as to the logic of the decision-making process (algorithm) that led to the development of those profiles. In other words, organisations should disclose their decision-making criteria. And they should do so in terms that are understandable to the subject[64].

V. Conclusion

The above considerations highlight the need to evaluate the practice known as «credit-based insurance scoring» not only in terms of its

---

[63] This statement may be based on the following reasons: If we enter the case exclusively in paragraph (b) of Article 22(2) GDPR, the affirmative answer derives from the general regulation of the right of opposition (Article 21 GDPR) and the rights of rectification (Articles 16 and 19 GDPR) and cancellation (Articles 17 and 19 GDPR). The right of the person concerned to express his opinion may be based on the former; the right to contest the decision may be based on the rights of rectification and cancellation when the information which gave rise to the decision to refuse him/her insurance or to impose an excessive premium on him/her does not truthfully reflect the insurance risk which may be linked to this particular individual. Furthermore, this can be interpreted as being the only way to sufficiently guarantee the interests of the data subject (Article 22(2)(b) GDPR). If, on the other hand, the hypothesis is considered to fall under Article 22(2)(a) or (c), the conclusion is drawn directly from the wording of Article 22(3).

[64] EDPB/WP29, *Guidelines on Automated individual decision-making*, 25.

efficiency in the insurance market but also from the perspective of the protection of the fundamental rights of the consumers. This protection must be interpreted with reference to both the «horizontal application» of fundamental rights, and the requirement of transparency. Particular attention must be paid to the impact of the prohibition of discrimination in the field of private contracts, and it is important to ensure that the use of credit scoring does not result in low-income consumers and members of minority groups paying higher insurance premiums than other consumers (a clear form of indirect discrimination). It is also essential to insist upon transparency, for as long as consumers are unaware of how insurance companies use their credit data when deciding whether or not to grant insurance cover and in setting insurance premiums, the possibility of effectively defending their rights is diminished. European Law has mechanisms to address this dual problem. The interpretation and practical application of these mechanisms will be decisive.

About the author

Senior Lecturer in Civil Law at the University of Valencia. Author of four monographs and more than seventy articles and collaborations in collective books in prestigious journals and publications on subjects related to civil law (contract law, housing, insurance contracts, data protection, matrimonial property regimes, Valencian civil law, leases, agrarian law, property, inheritance, mediation, etc.). Throughout her career as a researcher, she has taken part in numerous research projects; she is currently co-principal investigator in one of them: «Insurance Law in the welfare society of the twentieth century: The person as a central element», subsidized by the Ministry of Science, Innovation and Universities (RTI2018-097087-B-100). As a specialist of recognised prestige, she is a member of the Valencian Government's Advisory Committee on Valencian Civil Law and was awarded the «Savis en Dret» Prize (2012), by the University of Valencia and the Generalitat of Valencia.

From the very beginning of her academic career she has been actively involved in projects for educational innovation, and is Director of an educational innovation group at the University of Valencia. In 2016 she was awarded the Prize for Teaching Excellence by the Social Council of the University of Valencia and the Ministry of Education, Research, Culture and Sport of the Generalitat Valenciana (2016).

In the field of administration, she is at present Vice-Dean of Quality, Training, Culture and Social Projection of the Faculty of Law. Previously

she was Secretary of the Master's Degree in Law UVEG-ICAV, a member of the CCA of the Master's Degree in Mediation, Arbitration and Conflict Management in Private Law and Secretary of the Department of Civil Law, among other positions.

Sobre la autora

Profesora Titular de Derecho Civil de la Universidad de Valencia. Autora de cuatro monografías y más de setenta artículos y colaboraciones en libros colectivos en revistas y editoriales de prestigio sobre temas relacionados con el Derecho civil (Derecho contractual, vivienda, Derecho de seguros, protección de datos, regímenes económico matrimoniales, Derecho civil valenciano, arrendamientos, Derecho agrario, propiedad, sucesiones, mediación, etc.). A lo largo de su carrera como investigadora ha participado en numerosos proyectos de investigación, siendo en la actualidad co-IP en uno de ellos: «El Derecho del Seguro en la sociedad del bienestar del S.XXI: La persona como elemento central», Ministerio de Ciencia, Investigación y Universidades (RTI2018-097087-B-100). Como especialista de reconocido prestigio, es miembro del Comité Asesor de la Generalitat Valenciana en materia de Derecho Civil Valenciano. Ha sido galardonada con el premio "Savis en Dret" (2012), por la Universidad de Valencia y la Generalitat de Valencia.

Desde el inicio de su actividad ha participado activamente en tareas de innovación educativa y es, desde hace años, responsable de un Grupo de Innovación Docente estable de la Universidad de Valencia. En 2016 recibió el Premio a la Excelencia Docente del Consejo Social de la Universidad de Valencia y de la Conselleria de Educación, Investigación, Cultura y Deporte de la Generalitat Valenciana.

En el ámbito de la gestión, es Vicedecana de Calidad, Formación, Cultura y Proyección Social de la Facultad de Derecho. Anteriormente fue Secretaria del Máster en Derecho UVEG-ICAV, miembro del CCA del Máster en Mediación, Arbitraje y Gestión de Conflictos en Derecho Privado y Secretaria del Departamento de Derecho Civil, entre otros cargos.