REGULATING INSURTECH IN THE EUROPEAN UNION

PIERPAOLO MARANO | Professor of Insurance Law, Catholic University of the Sacred Heart, Milan, Italy, and University of Latvia, Riga, Latvia
MICHELE SIRI | Jean Monnet Professor of European Union Financial and Insurance Markets Regulation, Department of Law, University of Genoa, Italy

ABSTRACT

The European Union (E.U.) is one of the leading financial and insurance markets in the world. Fintech and insurtech have also developed in the E.U. The European Commission has taken numerous steps to fully comprehend and evaluate the challenges of applying new technologies to the financial services sector. This study provides an overview of the E.U. approach to insurtech from a regulatory point of view. Thus, risk governance within the E.U. Solvency II regime, including the role of the actuarial and risk management functions when dealing with this risk, will be illustrated. This analysis outlines the need for fair treatment of clients, as protecting policyholders is the main objective of E.U. regulations and supervision in insurance.

1. THE EUROPEAN UNION APPROACH TO FINTECH

The European Commission has taken numerous steps to fully comprehend and evaluate the fintech phenomenon and its implications for the financial services sector over the last three years. To this end, one of the most relevant papers issued by the European Commission is the FinTech Action Plan [E.C. (2018)], in which the E.U. acknowledged that fintech presents both opportunities and challenges for regulatory compliance and supervision. There was also a recognition that Europe's regulatory and supervisory frameworks should allow firms operating in the E.U. Single Market to benefit from financial innovation to safely provide their customers with the most suitable and accessible products. Moreover, such frameworks should also ensure a high level of consumer and investor protection and ensure the resilience and integrity of the financial system.

The European Commission clearly stated that technological neutrality is one of the guiding principles of the Commission's policies. This principle aims to repeal legal provisions that are outdated, unnecessary, or excessive about changing business models and/or the "digital" environment. Thus, one can achieve the underlying public policy objectives without a barrier to the development of fintech.

The FinTech Action Plan outlined (i) how specific E.U. rules that predate the emergence of innovative technologies may, in practice, not always be technology-neutral, (ii) that the benefits of technological innovation were already at the heart of the revisions to the Payment Services Directive [E.U. (2015)] and of the Directive and Regulation on Markets in Financial Instruments [E.U. (2014a)], and (iii) that new financial services do not always fall entirely under the existing E.U. regulatory framework; this is the case of the crowd and peer-to-peer activities for startups and scale-up companies. On the other hand, the Insurance Distribution Directive (IDD) [E.U. (2016)], as well as the Solvency II Directive [E.U. (2009a)] have not been adopted with technological neutrality at heart.

The European Commission, therefore, proposed that the European Supervisory Authorities (ESAs) should systematically take fintech into due consideration in all their activities.[1] This

decision is undoubtedly relevant for the insurance sector, as European legislation – IDD and Solvency II – has not been formally developed based on technological developments. Accordingly, the European Insurance and Occupational Pensions Authority's (EIOPA) Board of Supervisors confirmed EIOPA's commitment to insurtech and agreed to establish a multidisciplinary insurtech taskforce whose mandate was delivered in January 2019 [EIOPA (2019a)]. At the initial stages, and considering the European Commission's FinTech Action Plan, the taskforce will perform the following tasks.

Firstly, a thematic review on the use of big data by (re-) insurance undertakings and intermediaries (both incumbents and startups), including the mapping on an ongoing basis of the innovation facilitators set up by the different jurisdictions in the area of insurtech, to establish efficient and effective supervisory practices in the form of best practices, and, where appropriate, issue guidelines; the mapping of the current authorizing and licensing requirements and assessing how the principle of proportionality is being applied in practice, specifically in the area of financial innovation (e.g., regarding insurtech startups such as peer-to-peer insurers); and the assessment of National Competent Authorities (hereinafter NCAs) supervisory practices and expectations on outsourcing to cloud service providers and exploring the need to issue guidelines.

At a later stage and subject to EIOPA's work program, the taskforce will also undertake the following tasks: (i) convergence on supervision of algorithms; (ii) scrutiny of the (re-)insurance value chain and new business models arising from insurtech to propose remedies to the supervisory challenges arising from the new business models and the possible fragmentation of the (re-)insurance value chain as a result of new technologies and actors entering the insurance market; (iii) development of a European Insurance Innovation Hub, where EIOPA would cooperate with NCAs and insurtech firms (regardless of their size) to promote financial innovation in the European insurance and pensions market; (iv) assessment of the impact of insurtech in the context of regulatory monitoring, reporting, and compliance by (re-) insurance undertakings and intermediaries; and (v) exploring the benefits and risks arising from the use of blockchain and smart contracts for (re-)insurance undertakings and consumers, including assessing possible regulatory barriers preventing the deployment of this innovation.

Concerning potential barriers to insurtech, the methodology for the assessment of each barrier should include the following steps: identifying the public policy objectives sought by the relevant applicable provisions, analyzing why such provisions might represent a barrier to insurtech, and suggesting balanced solutions where the original public policy objectives are achieved without giving place to potential barriers to innovation.

Insurance Europe, the European (re-)insurance federation, shared with EIOPA's insurtech taskforce a list of examples of obstacles created by existing legislation and recommendations on how to address them.[2] However, most of the recommendations ultimately seem to demand considering the principle of proportionality for obligations deemed unjustifiable rather than relate to technology neutrality. The examples listed by Insurance Europe, which are connected to technology neutrality, mainly consist of paper requirements by default. One of the main factors for technologically driven cost efficiency is processing data digitally throughout the entire process. The Insurance Distribution Directive that applies to all insurance distributors, including automated advisory tools, sets out a default paper requirement and should, therefore, be appropriately modified (see Article 23). Similarly, Article 14 of the Packaged Retail and Insurance-based Investment Products Regulation (PRIIPS)[3] should be adapted to be more reflective of digital innovation. The paper-driven nature of these information disclosures conditions will hinder digital innovation.

However, as was mentioned, most of the other examples refer to the principle of proportionality rather than technological neutrality. This is the case, for instance, with the unnecessary reporting requirements. All providers, such as incumbents and new insurtech startups, would benefit from the reduced complexity of supervisory provisions. Rules that have proven unnecessary or overly burdensome need to be identified and revoked. One example of excessively burdensome provisions is that of the excessive reporting requirements as stipulated under Solvency II. It is also the case with the overly strict requirements in the case of outsourcing of functions/insurance activities and with the access to data and information sharing.

EIOPA (2019a) reported that the E.U. insurtech market is at an early stage but evolving based on the evidence. Most NCAs have limited experience with insurtech companies or do not differentiate those with "digital" business models. However,

[1] https://bit.ly/2UVHT53
[2] https://bit.ly/3fdoAuD
[3] https://bit.ly/3fbzRMc

both NCAs and external stakeholders highlighted the need for a level playing field, proportionality, and technological neutrality. EIOPA also believes that regulation and supervision must be technology-neutral and ensure a level playing field.

Following these principles and technological neutrality, EIOPA stated that facilitating innovation is not about deregulation. If an insurtech company offers the same services and products as an established insurance provider and is exposed to the same risk portfolio, it should be subject to the same legislation and supervision regarding the services and products in question. The preference for technological neutrality leads EIOPA to hold that there seems to be no need for further regulatory steps regarding licensing requirements, apart from some peer-to-peer insurance business models. As a best practice, EIOPA suggests that a member state that applies provisions regulating insurance in addition to those set out in E.U. law should ensure that the administrative burden stemming from those provisions is proportionate about consumer protection and financial stability and remains limited and technology-neutral.

Concerning peer-to-peer insurance, a regulatory issue could be identified when the business model consists of purely technical service providers/platforms acting as administrators for the risk-sharing groups without an underlying insurance carrier. Since the platform acts purely as an administrator for the risk-sharing groups (e.g., it might leverage blockchain and smart contracts and facilitate users coming together and creating their own "pools"), these platforms will not be easy to qualify under current regulation. Thus, it is a matter of evaluating concrete business models, and the outcome can be that a given business model falls under insurance regulation, or outside of it, as well as, say, under the regulations applicable to payments services. In addition, many do not believe that peer-to-peer insurance carried out by brokers, which is the most common type available in the market, can circumvent the standards of Solvency II [Marano (2019)].

2. TRANSFORMATION OF THE E.U. INSURANCE REGULATION

The rationale behind the use of the principle of technological neutrality is to evaluate if existing legal provisions are still up to date and/or necessary and appropriate in the context of changing business models and/or the digital environment. This assessment has been performed by identifying the public policy objectives sought by the provisions concerned, analyzing why such provisions might represent a barrier to insurtech and suggesting balanced solutions where the original public policy objectives are attained without causing any obstacles to technological development and integration.

However, the technology-driven innovations applicable to the business cycle of insurance and insurance intermediation activities may lead to gaps other than those listed by authorities: technological neutrality does not mean that the technology is neutral. Technology can affect the phenomena that have been regulated since the dawn of insurance. Insurance has now begun to develop in the environment of digital technology, which poses different challenges compared to those incurred in the "traditional" environment in which insurance has evolved.

As many have already observed [Eling and Lehmann (2018)], digital transformation can affect all components of the insurer's value chain. At the production side of an insurer, the benefits of technology (artificial intelligence) are still in development. Artificial intelligence (AI) solutions are likely to improve insurance offerings, especially customer segmentation. However, the outcome is not irrelevant for social welfare and – consequently – for insurance regulation. If AI were to be used to better assess customer risk profiles and optimize pricing systems, social welfare would be enhanced. It seems reasonable to predict that insurance products are likely to become more personalized and usage-based because of the availability of the client's data on a real-time basis. More in-depth information dataset and real-time analytics allow insurance pricing based on usage and behavior of the customers.

The role of AI and big data within the (re-)insurance sector has been specifically reviewed by EIOPA to assess the current trends and plan accordingly [EIOPA (2019b)]. The study underlined how, so far, AI and big data have been introduced alongside traditional means of data gathering and processing and thus have not replaced them. Not only has this combination generated benefits in terms of efficiency, but it has also brought about changes to the actual structure of the (re-)insurance market. In particular, EIOPA noted how this greater and much more accurate availability of data had fostered the identification of more numerous and smaller risk pools, based on new ratings strictly tailored on the customers' risk exposure.[4]

[4] As well as, potentially, the development of use-based insurance products and due to the impact of technologies, such as the Internet of Things and the 5G network.

A similar task has also been undertaken by the E.U.-U.S. Insurance Dialogue Project's Big Data Working Group.[5] The Dialogue Project carried out a joint E.U.-U.S. analysis of the impact of said technologies on the (re-)insurance sector and subsequently identified a series of areas of future study and/or intervention, such as the further development of AI principles in the U.S. and E.U., including the ethical issues; a regulatory review of predictive models, including, but not limited to, assessing transparency and explainability issues arising from the use of machine learning algorithms; the industry use of big data for fraud detection and claims settlement; and the continued monitoring of developments on third-party vendors and consumer disclosure issues [EIOPA (2020a)].

While technological developments, as underlined by the EIOPA (2019b), do not present any systemic issues at this point (e.g., concerning consumer protection), one can note that they have been causing concerns from an ethical standpoint, particularly regarding the fairness and transparency of data and AI analysis (as well as machine learning). To that end, EIOPA has given the mandate to an ad hoc working group to analyze the ethical aspects of these phenomena.

This research [EIOPA (2021a)] underlined that, as is often the case with new technologies, AI may bring some inclusion concerns to vulnerable customers and it may cause issues considering the impact mentioned above on ratings. AI should not be bent to the realization of prices and claims structured to bring customers to underwrite a contract that is unfavorable and/or unnecessary compared to the current standard.

Consistent with the technological neutrality principle, these issues should be faced through a cautious systematic application of the existing applicable framework, with particular care for proportionality. While (re-)insurance firms shall be required to have in place sound and prudent governance structures – also considering the introduction of AI in their value chain – regulation should tailor these requirements to not excessively hinder technological development.

Technology can transform the client relationship in the distribution chain, especially in increasing customer autonomy. Mobile and online customized channels can substitute traditional marketing tools. Conventional distribution channels can be replaced or supplemented by online distribution as well as by insurtech startups. First and foremost, the ambition of many insurtech startups is to automate the underwriting and intermediation of customers and the detection of claims and fraud.

Insurtech will transform insurance regulation because it will be necessary to update the framework to regulate the insurance business as a part of an integrated environment with the technology/data companies at the center of the ecosystem. Secondly, the scope of the supervision should include the "technology company" given that these "quasi-insurers" will be the source of almost all the data that the insurance industry will use. The traditional insurer will remain on the market as a risk carrier. However, technology-driven companies will be the providers of data and algorithms without being regulated in how they affect the insurance business model.

EIOPA remarked that one of the significant risks related to the mainstreaming of AI and big data within the (re-)insurance sector is that of excessive fragmentation and the possible ensuing regulatory gaps. To that end, EIOPA has opened a public consultation aimed at assessing the impact of such technologies on the value chain of (re-)insurance services to identify the appropriate regulatory measures (if any) [EIOPA (2020b)]. Technology has not only impacted how "traditional" services are provided (i.e., data gathering and processing), it has also given birth to platforms and services that are not easily qualified under existing categories (as mentioned above regarding peer-to-peer insurance models). These services may represent autonomous problems when included in the traditional (re-)insurance value chain (i.e., outsourcing). From the perspective of the regulatory authorities, they can cause a dangerous regulatory fragmentation, bringing phases of the provision of such services – which would typically fall within the scope of the applicable regulations – outside of its purview because of the new format in which they are provided.

Such risks are closely monitored by EIOPA, not only for the sake of legal certainty but also, and most importantly, because of the material risk that it may loosen the "supervisory grip" of the authority over service providers. Consequently, EIOPA has set out to identify the regulatory needs and appropriate measures that will need to be put in place in accordance with a technologically neutral approach (as per above).

[5] A project shared by the U.S. Treasury and the E.U. institutions aimed at supervisory and regulatory convergence.

Furthermore, EIOPA, under its mandate within the more general scope of the FinTech Action Plan, has been tackling other urgent areas of intervention and has carried out a careful assessment of the possible appropriate actions to take. Although EIOPA has only addressed some of the following summarized topics, one can expect that these developments in insurance regulation will be driven by the findings and studies undertaken by EIOPA.

Such is the case, for instance, with distributed ledger technologies (DLT), the so-called blockchain. This issue has been on the E.U. political agenda for a number of years now, resulting in the publication of a proposal for a Markets in Crypto-Assets Regulation (MiCAR) [E.C. (2020a)]. However, it is only in recent years that the topic has been raised regarding the insurance sector – in which, so far, this type of technology has yet to be widely implemented and experimented with (as opposed to securities trading).

EIOPA has set out a preliminary review of the state of play through an open consultation [EIOPA (2021b)] to gauge the potential of blockchain to be applied to (re-)insurance services. The EIOPA has discussed how such a tool could be implemented in all steps of the insurance value chain. The insurance value chain would benefit from the use of blockchain through the reduction of the duplication of processes, increased process automation, reduction of costs, increased efficiency, enhanced customer experiences, and improved data quality, collection, and analytics. The potential impact, however, would not be limited to improvements in existing processes, as it is deemed that blockchain could also encourage the introduction of new types of services, such as decentralized peer-to-peer insurance models, as well as parametric insurance products.

Having said that, all of these potential benefits of blockchain could potentially be problematic for EIOPA. The fact is that blockchain-based products (such as cryptocurrencies) entail new and, so far, unclear risk profiles, which would need to be considered should these products be streamlined in the insurance sector, particularly regarding consumers. Moreover, although the existing regulatory framework is generally effective when it comes to addressing emerging technologies and risks, blockchain is still shrouded in a layer of legal uncertainty for some particular aspects of these technologies: from the legal qualification of certain types of crypto assets[6] to the legal status of smart contracts, including all of the privacy and data protection concerns related to the latter. Thus, EIOPA calls for a harmonized approach to blockchain across the E.U. and cooperation among NCAs to that end. In addition, EIOPA is encouraging growth in this field.

Among the potential benefits of blockchain, according to the EIOPA, is its possible use for supervisory purposes (so-called suptech). For example, the implementation of smart-contracts could help automate regulatory reporting, thus increasing efficiency and transparency of supervision, improve data consistency across firms, as well as enabling real-time regulatory monitoring.

Fintech could be a useful tool for supervisory purposes. To that end, EIOPA has adopted a strategy to include these tools in its processes and develop the regulatory background to ensure consistency in the use of said technologies across the E.U. Moreover, suptech has been introduced in EIOPA's Annual Supervisory Convergence Plan [EIOPA (2021c)], hence, it will be pursued and developed, together with the other objectives of EIOPA, through its specific regulatory tools, such as guidelines, handbooks, statements [EIOPA (2020c)].

As has been mentioned, one of the most disruptive impacts of fintech in the field of (re-)insurance services is that of data collection, sharing, and analytics. To fully benefit from the added value that relates to that, EIOPA has identified four main objectives to be achieved using suptech as a means of harmonization and cooperation: knowledge and experience exchanges among NCAs and with EIOPA, improvement of the existing cooperation agreements and exchange of market data, and strengthening of data collection and data analytics. Furthermore, these tools could thrive, according to EIOPA, in the context of the Solvency II mandatory reporting: this reporting framework has built – and continues to develop – an unprecedented database of market data, which, if analyzed and exploited in its full potential thanks to technologies such as AI, could be conducive to a significant improvement of supervisory standards, and, ultimately, investor protection.

Among the challenges to this strategy, other than the aforementioned legal uncertainties, is the currently diverse approach of NCAs to suptech, which will represent a burden to harmonization and cooperation and may require time and effort to overcome.

[6] For instance, it has been discussed whether and under what conditions cryptocurrencies can be considered commodities and thus represent the underlying asset to a derivative, see AMF (2018), SEC (2017).

Guidelines on information and communication technology security and governance are a concrete example of EIOPA's course of action pursuant to all the strategies outlined [EIOPA (2020d)]. The Guidelines[7] find their purpose in the currently dominant fragmentation of information and communications technology (ICT) in the insurance sector, as well as the ever-growing reliance on technology in this sector across the E.U. To that end, EIOPA aims to provide a much-needed clarification to market participants on the minimum degree of information they can expect; avoiding regulatory arbitrage (and forum shopping), increasing supervisory convergence.

The authority adopted a dual approach with the guidelines. On the one hand, it acknowledged the peculiarities of insurtech, and technological risk in general, and thus provides for specific tech-related guidelines. On the other hand, it emphasized how such elements should be considered as part of the "business as usual" of all insurance sector participants, and thus requires said entities to include these elements in their everyday actions.

Examples of the first category of guidelines include, for example, specific requirements related to the security of access to the company's data, both in terms of logical access (i.e., identification tools) and in terms of physical access (access to data centers, as well as their safety from external threats).

A broader approach is adopted as to the second category of guidelines. EIOPA has provided that at least one of the governance bodies of (re-)insurance service providers must ensure that the company's governance undertake due measures to manage ICT and security risks (see Guideline 2). This requirement is then further developed, as the authority requires companies to adopt an ICT strategy and ensure that the business plan is aligned with such strategy (see Guideline 3). Lastly, while it is acknowledged that ordinary risk management tools and business continuity (see Guideline 21) plans may already have issues deriving from the use of technologies, EIOPA chose to specify the role that this component must be attributed in risk management systems and business continuity. These measures are then required to be constantly updated, monitored, and approved by the corporate body in charge of ICT-related matters (Guideline 4).

3. RISK GOVERNANCE WITHIN THE E.U. SOLVENCY II REGIME

The actual insurance regulatory framework cannot comprehensively assure proper risk governance for those technologies once they get out and are used on a broad scale. The Solvency II Directive (2009/138/EC) sets out the framework for a regulatory regime for the insurance sector, innovating the standards for capital requirements and risk management for insurers and reinsurers within the E.U. Articles 41 to 49 focus on ensuring insurers and reinsurers establish systems that lead to good governance. Article 49 deals with outsourcing, making it clear that insurance and reinsurance undertakings remain fully responsible for discharging all their obligations under the Solvency II Directive when they outsource functions or any insurance or reinsurance activities and require that outsourcing of critical or important operational functions or activities shall not be undertaken in such a way as to lead to any of the following:

- Materially impairing the quality of the system of governance of the undertaking concerned
- Unduly increasing the operational risk
- Impairing the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations
- Undermining continuous and satisfactory service to policyholders.

The regulatory framework sets forth specific requirements for outsourcing, including detailed provisions which must be included in a written outsourcing agreement required with any service provider providing services that are "for any critical or important operational functions or activities." Explanatory Notes to the 2013 Level 3 Guidelines by EIOPA give examples of critical or essential functions or activities, and these include the investment of assets or portfolio investment, claims handling, provision of data storage, and the provision of ongoing day-to-day systems maintenance or support (the latter two of which are likely to be of significance in many technology-related services).

[7] In the banking sector, a recent Grand Chamber court decision stated that the guidelines issued by the European Banking Authority (EBA) can be the subject of a referral for a preliminary hearing pursuant to Art. 267 TFUE, thus potentially laying the basis for the official recognition of the binding nature of this kind of instrument, see case C-911/19, https://bit.ly/2V82L8Z.

EIOPA identified the need to develop specific guidelines on outsourcing to cloud service providers. These services combine business and delivery models that enable on-demand access to a shared pool of resources such as applications, servers, storage, and network security [EIOPA (2020e)]. The Guidelines aim to (1) provide clarification and transparency to market participants avoiding potential regulatory arbitrages, and (2) foster supervisory convergence regarding the expectations and processes applicable to cloud outsourcing. In addition, as mentioned, EIOPA issued Guidelines on ICT security and governance, including a guideline on the outsourcing of ICT services and ICT systems (see Guideline 25). Without prejudice to the Guidelines on cloud services, insurers should ensure that where ICT services and ICT systems are outsourced, the relevant requirements for the ICT service or ICT system are met. Moreover, insurers must monitor and seek assurance on the level of compliance of these service providers with their security objectives, measures, and performance targets.

However, the aforementioned regulatory framework seems ineffective in dealing with insurtech's new environment. The existing regulatory framework is still strongly influenced by the model of traditional bilateral outsourcing relationships, where financial institutions purchase a solution from a service provider and negotiate the related contract documentation with them. A revision of outsourcing rules must determine whether it enables insurers to make full use of new technologies such as cloud solutions and distributed ledger technologies and integrate them into their business models while ensuring the necessary risk management, security, and regulatory compliance. Furthermore, assessing the fit and proper requirements of all persons who effectively run the undertaking or have other key functions should include knowledge of these systems and services.

4. THE NEW E.U. SUPERVISORY APPROACH TOWARD NEW TECHNOLOGIES

The E.U. 2018 Action Plan laid down a series of steps and objectives aimed at allowing innovative business models to scale up at the E.U. level, particularly by supporting the uptake of the new technologies in the financial services sector, while also further developing cybersecurity to maintain the integrity of the financial system despite the introduction of such unique factors. Furthermore, with an approach like that of the NIS Directive (the first piece of E.U.-wide legislation on cybersecurity),[8] the Commission's plan proposed to enhance supervisory convergence toward new technologies so as to better prepare the European financial services sector to embrace the opportunities provided by fintech and benefit from the scale economies of the single market while preserving financial stability and consumer protection.

To that end, the Commission gave a mandate to the European Supervisory Authorities (ESAs)[9] to deliver an opinion on ICT-related risks, outlining the areas of financial legislation that required intervention in terms of ICT-risk management requirements. First, the joint advice[10] of the ESAs proposed an overview of the current state of play in the E.U. financial regulation as to the said requirements, underlining, despite a widespread presence of operational risk requirements throughout the different sectors, the absence of specific ICT and cybersecurity risk requirements. The authorities, therefore, suggested introducing such bespoke requirements and a dedicated supervisory framework to ensure compliance and effectiveness. In particular, the ESAs considered that the two main areas of the intervention consisted of ICT incident reporting and the provision of an appropriate oversight framework for monitoring critical service providers to the extent that their activities may impact relevant entities, both of which found their expression in the proposal for digital operational resilience regulation.

As a result of the joint advice, of the convergence mentioned above among the national authorities, of several public consultations, as well as of several other initiatives[11] aimed at fostering debate on matters related to fintech among the leading players of the market, the E.U. Commission adopted a digital finance package, comprising a new digital finance strategy [E.C. (2020b)], as well as a retail payments strategy [E.C. (2020c)]. Regarding the digital finance strategy, its scope goes beyond just addressing the challenges raised by fintech, tackling its development and implementation in the E.U. With the declared objective of boosting responsible innovation in the E.U.'s financial services sector, the strategy sets out to adopt a set of legislative proposals of a broad reach as to the technology applied, covering four primary objectives: the achievement of a single digital market for financial services, a European financial

[8] https://bit.ly/3iehrwd
[9] European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority, established by Regulations EC/2010/1093, EC/2010/1094, and EC/2010/1095.
[10] EBA, EIOPA, ESMA, 2019, "Joint advice on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector," April 10, JC 2019 26, p.4.
[11] The so-called "digital finance outreach" adopted by the European Commission on February 4, 2020, https://bit.ly/3x8HWaw

data space to promote data-driven innovation, a regulatory framework facilitating innovation, and addressing the risks of digital transformation [Zetzsche et al. (2020)].

Out of the four pillars of the strategy, only the last two have already been acted upon so far, tackling crypto assets and cyber resilience topics. On the one hand, the proposal of a Markets in Crypto-Assets Regulation (MICAR) [E.C. (2020d)] introduces a framework aimed at facilitating innovation in developing a market of digital representations of value that can be stored and traded electronically. On the other hand, the proposal for a Regulation on Digital Operational Resilience (DORA) [E.C. (2020e)] aims to ensure that all participants in the financial ecosystem have the necessary safeguards in place to prevent cyberattacks and mitigate other cyber-related risks, therefore, addressing the last of the objectives of the digital finance strategy [Zetzsche et al. (2020)], as well as the two areas of intervention identified by the ESAs joint advice of 2019. The preeminent role of DORA within the strategy appears clear, since the need for security and resilience is naturally more pressing as technologies are further developed, implemented, and streamlined within financial services, as is the case with the MICAR.

Other than pursuing the general strategy and political agenda according to which DORA was proposed, the regulation aims to tackle certain specific shortcomings of the E.U. financial services sector identified by the Commission's impact assessment [E.C. (2020f)], as well as by the public consultation processes which lead to DORA. Notably, a necessary action includes solving the currently existing differences of ICT security requirements in the different fields of the E.U. financial legislation. Thus, for example, the Commission noted how certain players in the financial services sector are subject to specific requirements regarding ICT risk,[12] while only general conditions, if any, are provided for other financial market participants.[13]

Moreover, a second action requires ensuring a level playing field throughout the E.U. about incident reporting obligations. One can achieve this outcome not only by introducing requirements where the financial regulatory framework is silent, but also by avoiding inconsistent and multiple reporting obligations where, for example, a financial institution is required to notify the incident to their NCA, and a different national authority under the NIS.

Lastly, a further essential action aims to grant a coherent oversight over ICT third-party providers (TPP) to European financial market participants. The introduction of an efficient oversight framework including TPP is an important part of the DORA proposal, since TPP may result in either operational issues or contractual limitations, which can temporarily prevent financial institutions from benefiting from their services. In addition, they are currently subject to variable monitoring, inconsistent at the E.U. level, with a material risk of failing to identify failures in a timely fashion. Moreover, financial institutions have been experiencing difficulties in gathering insight on the TPP they outsource ICT services to, which, about certain ICT services, are limited in their number, entailing possibly more severe risks related to the market concentration and subsequent contagion risks and capable of undermining the E.U. financial system.

The proposed E.U. regulation requires financial entities to equip themselves with internal governance and control frameworks capable of ensuring effective and prudent management of ICT risks. While the requirement is broad, DORA explicitly acknowledges its intention of assigning the responsibility of the company's management of ICT risks. Although the task is to be delegated to specifically identified ICT-related roles and functions, the company will be held liable for any failures, considering its obligations to approve and oversee the said governance arrangements.[14] This choice was driven by the intention to attribute particular importance to cybersecurity and resilience, granting relevance also in terms of business strategies, rather than introducing them as a mere compliance obligation, and ensuring that they receive the necessary budgetary consideration.[15]

Following the ESA joint technical advice, DORA then lays down a set of specific ICT risk management requirements, which revolve around several ICT risk management functions, including (1) identification of all ICT-related business functions and their risks (art. 7); (2) protection of the company's ICT systems and operations, aimed at preventing business

[12] This is is the case under the Payments Service Directive 2 [PSD2, E.U. 2015)], Central Securities Depositories Regulation [CSDR, E.U. (2014b)], and European Market Infrastructure Regulation [EMIR, E.U. (2012)].

[13] These include the Capital Requirements Directives [CRD, E.U. (2013a)], Capital Requirements Regulation [CRR, E.U. (2013b)], Solvency II [E.U. (2009b)], Undertakings for Collective Investment in Transferable Securities Directive [UCITS, E.U. (2009c)], and Alternative Investment Fund Managers Directive [AIFMD, E.U. (2011)].

[14] The choice to hold the management body liable for ICT risks is not uncommon and the exact requirement has been provided concerning credit institutions, payment services providers and investment firms pursuant to the CRR [EBA (2019)]

[15] Recitals 36 and 37 of the DORA.

disruptions through continuous monitoring and the provision of detailed security strategies, policies, procedures, tools and protocols (art. 8); and (3) prompt detection of any anomalies and incidents in the business's ICT functions (art. 9), so as to allow the timely activation of the company's ICT business continuity policy, or, if need be, the ICT disaster recovery plan (subject to independent audit review), and that these policies shall undergo regular testing, and be aided by the provision of a crisis management function.

5. EMBEDDING THE INSURTECH RISK GOVERNANCE INTO THE ACTUARIAL AND RISK MANAGEMENT FUNCTIONS

Sound risk management and governance systems should evaluate and control pricing, including the risk factors used and the claim reserving methods based on aggregated data. While under the Solvency II prudential regime this activity is under complete control of the insurance undertaking, in an insurtech environment the data process is less transparent, and data availability is in the technology provider's hands. Consequently, an important question to ask is whether such activities should be under the governance of the insurance company and, ultimately, under the control of humans.

From a prudential and the supervision of conduct perspective, it seems unsafe to leave the functioning of a pricing mechanism or a loss reservation process to an algorithm. As a counterbalance – which is again not technologically neutral – a second layer of checks should be performed on the activities conducted through the algorithms by an ex-ante control of the risk management and the actuarial functions.

E.U.'s Solvency II Directive requires four key functions (actuarial, risk management, compliance, and internal audit) to comply with the framework's second pillar requirements. However, new technologies, new organizational strategies, and new strategic moves might demand further discussions about these functions. For example, let us take one of the requirements for the actuarial function: "assess the sufficiency and quality of the data used in the calculation of technical provisions" (Art 48, (c), Solvency II Directive). A very challenging role for this function is when data is generated, transformed, and processed within an insurance organization and outside the company by the technology provider.

We conclude that the E.U. insurance regulation should demand that the actuarial function assesses an algorithm's performance, as well as any insurtech tool, and potentially intervene when assessing the design and the results of the algorithmic decision-making process. In this sense, a sound prudential framework for the insurance company should consider the role of the actuarial function in the new insurtech environment to adopt the internal process and ensure the effectiveness of the performance of the algorithms. Furthermore, from a practical point of view, other critical functions of the insurance company should be involved to address the reputational risk, including the technology's ethical issues. Thus, the governance rules for underwriting and loss reserving need an update for insurtech.

Furthermore, the E.U. Solvency II Directive requires insurance and reinsurance undertakings to have in place an effective risk-management system comprising strategies, processes, and reporting procedures necessary to continuously identify, measure, monitor, manage, and report the risks at an individual, as well as at an aggregate level to which they are or could be exposed, and their interdependencies.

This risk-management system shall be effective and well-integrated into the organizational structure and in the decision-making processes of the insurance or reinsurance undertaking with proper consideration of the persons who effectively run the undertaking or have other vital functions. The risk-management system shall cover at least the following areas:

- Underwriting and reserving
- Asset-liability management
- Investment, in particular derivatives and similar commitments
- Liquidity and concentration risk management
- Operational risk management
- Reinsurance and other risk-mitigation techniques.

Does the EU Solvency II Directive properly assess the implications of insurtech on the risk-management system?

Highly dynamic, usage-based insurance (UBI) products proliferate and are tailored to the behavior of individual consumers. As a result, insurance transitions from a "purchase and annual renewal" model to a continuous cycle, as product offerings constantly adapt to an individual's behavioral patterns. Furthermore, products are disaggregated substantially into micro coverage elements (for example, phone battery insurance, flight delay insurance, different coverage for a washer and dryer within the home) that consumers can customize to their needs, with the ability to instantly compare prices from various carriers for their individualized baskets of insurance products [McKinsey (2021)].

Price remains central in consumer decision making, but carriers innovate to diminish competition purely on price. Sophisticated proprietary platforms connect customers and insurers and offer customers differentiated experiences, features, and value. As a result, in some segments, price competition intensifies, and razor-thin margins are the norm, while in other parts, unique insurance offerings enable margin expansion and differentiation. In addition, pricing is available in real time based on usage and a dynamic, data-rich assessment of risk, empowering consumers to decide how their actions influence coverage, insurability, and pricing [McKinsey (2021)].

Let us mention the scenario in which there will be fierce competition with the associated risk of insolvency of insurance providers – lower margins and increased customer mobility that triggers more market instability. The development of multi-channel offers is likely to induce lower retention and more risk of default. New systemic risks may arise in case of a technology failure. Reputational risk and competition are expected to rise.

Supervisors need to review risk management requirements due to the insurtech players. However, again, technology is "not" neutral from the perspective of Pillar II of the E.U. Solvency II regulation.

In conclusion, technology-driven companies will be the providers of both data and algorithms, but the traditional insurer remains on the market as a risk carrier. Thus, both the actuarial function and risk management function are challenged in their ability to check if the insurance business is under the insurer's control. Nonetheless, their assessment of the implications of insurtech on the insurance business is unavoidable due to the repercussions on price mechanisms and risks. Insurers' management and internal control functions and supervisors should be fully aware of this.

6. FAIR TREATMENT OF CLIENTS IN THE NEW TECHNOLOGIES LANDSCAPE

Directive (EU) 2016/97 of January 20, 2016 on insurance distribution (IDD) provides an updated harmonized legal framework governing the rules applicable to the distribution of insurance and reinsurance products, including insurance-based investment products.

The insurance distribution directive aims to enhance the protection of consumers and retail investors buying insurance products or insurance-based investment products by ensuring greater transparency of insurance distributors about the price and costs of their products, better and more comprehensible product information, and improved conduct of business rules, particularly about advice. The new rules will apply to all distribution channels, including direct sales by insurance companies, to creating a level playing field for all distributors, and guaranteeing uniform high standards of protection for consumers.

The insurance distribution directive introduced generalized product oversight and governance (POG) into E.U. insurance

distribution law to ensure that all insurance products for sale to customers meet their specific target market needs to avoid and reduce an early-stage risk of failure to comply with customer protection rules. The product oversight and governance rules will be mainly addressed at manufacturers of insurance products and oblige them to maintain, operate, and review a POG policy to ensure that all insurance products marketed are appropriate for their specific target market. Insurance distributors must support this by operating product distribution arrangements to ensure that they have all the information needed to sell the product in line with the POG policy set by the manufacturer.

Product oversight requirements for manufacturers set out the core obligation for manufacturers to maintain, operate and review appropriate product oversight and governance arrangements for all newly developed insurance products and significant adaptations of existing insurance products. These arrangements include the definition of a target market for each insurance product. In addition, they shall ensure that insurance products are continuously aligned with the interests, objectives, and characteristics of the customers belonging to the target market. Thus, manufacturers must undertake appropriate testing of insurance products and monitor and regularly review their products continuously.

This task is likely to challenge manufacturers operating in the insurtech environment. The accessibility of more information will influence significant components of the company model of insurance, such as pricing and risk classification. Furthermore, additional data and new forms of digital monitoring (for instance, via apps, wearables, or GPS technology) offer additional information regarding the loss distribution. However, a more intrusive regulatory intervention on insurance pricing would limit the freedom of risk classification and probably increase the adverse selection and moral hazard as a side effect. So, as the first choice, it would be beneficial to adapt the existing regulatory framework in product oversight and governance to perform appropriate testing of insurance products and continuously monitor and regularly review their products coherently with the new insurtech environment.

7. CONCLUSION

The European Commission is committed to understanding, evaluating, and regulating the fintech phenomenon and its implications for the financial services sector, including insurance. Accordingly, European Supervisory Authorities systematically take fintech into due consideration in all their activities. In addition, market participants are testing the impacts of new technologies by creating new products or services or innovating how they provide “traditional” ones.

Regarding the insurance sector, EIOPA's work program refers to technological neutrality as one of the guiding principles of the European Commission's policies. This principle aims to repeal legal provisions that are outdated, unnecessary, or excessive about changing business models and the digital environment.

However, the technology-driven innovations applicable to the business cycle of insurance and insurance intermediation activities may lead to gaps other than those listed by authorities: technological neutrality does not mean that the technology is neutral. Along with opportunities and benefits to customers and the market participants, technology challenges the insurance business and its regulation.

Insurance business and regulation were both developed in an environment other than insurtech. The insurance business is becoming a part of an integrated environment with technology/data companies at the center of the ecosystem. Thus, the regulatory framework on the insurance business needs to be updated to level the playing field and ensuring all risks are duly identified, measured, and managed.

The European Commission adopted the digital finance package, which provides the general framework for digital transformation in the financial sector. This package includes several regulatory proposals. However, market participants must comply with the current framework, pending their adoption, which calls for sound risk management and governance system for financial operators, including insurers.

The Solvency II prudential regime requires insurers to evaluate and control pricing, including the risk factors and the claim reserving methods based on aggregated data. Outsourcing to technology/data companies challenges the actuarial function and risk management function to check if the insurance business is under the insurer’s control. Moreover, the set of rules on product oversight and governance requires manufacturers to embed customer protection in the design and distribution of insurance products in the new insurtech environment. Finally, supervisors must be aware of the challenges posed by the new environment. Digital transformation involves everyone, and no one can be unprepared to face it.

REFERENCES

AMF, 2018, "Analysis of the legal qualification of cryptocurrency derivatives," Autorité des marchés financiers, https://bit.ly/3xjRRu8

EBA, 2019, "EBA guidelines on ICT and security risk management," European Banking Authority, November 29, https://bit.ly/3xiPUOm

E.C., 2018, "The FinTech action plan: for a more competitive and innovative European financial sector," European Commission, March 8, https://bit.ly/3zQSQDD

E.C., 2020a, "COM (2020) 593: Proposal for a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Directive (EU) 2019/1937," European Commission, https://bit.ly/3rLT4Jw

E.C., 2020b, "Digital finance package," European Commission, https://bit.ly/3j8z7bG

E.C., 2020c, "Retail Payments Strategy for the EU," Communication, European Commission, https://bit.ly/3xdMYTf

E.C., 2020d, "Proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets," European Commission, https://bit.ly/2TlKfDw

E.C., 2020e, "Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector," European Commission, https://bit.ly/3j3UUkQ

E.C., 2020f, "Inception impact assessment on the Regulation on Digital Operational Resilience for the Financial Sectors," European Commission, https://bit.ly/3fc5EfQ

EIOPA, 2019a, "Report on best practices on licensing requirements, peer-to-peer insurance and the principle of proportionality in an InsurTech context," European Insurance and Occupational Pensions Authority, https://bit.ly/376mf0c

EIOPA, 2019b, "Big Data analytics in motor and health insurance: a thematic review," European Insurance and Occupational Pensions Authority, https://bit.ly/3j0CrWp

EIOPA, 2020a, "Summary report of the EU-US insurance dialogue project big data working group," European Insurance and Occupational Pensions Authority, https://bit.ly/2V7ZDdc

EIOPA, 2020b, "Discussion paper on (re)insurance value chain and new business models arising from digitalisation," European Insurance and Occupational Pensions Authority, https://bit.ly/3fbEaak

EIOPA, 2020c, "Supervisory technology strategy," European Insurance and Occupational Pensions Authority, https://bit.ly/3yfVBOf

EIOPA, 2020d, "EIOPA finalises Guidelines on Information and Communication Technology Security and Governance," European Insurance and Occupational Pensions Authority, https://bit.ly/2UVPZKX

EIOPA, 2020e, "Guidelines on outsourcing to cloud services providers," European Insurance and Occupational Pensions Authority, https://bit.ly/2WscEPa

EIOPA, 2021a, "Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector," European Insurance and Occupational Pensions Authority, https://bit.ly/3rJsoZV

EIOPA, 2021b, "Discussion paper on blockchain and smart contracts in insurance," European Insurance and Occupational Pensions Authority, https://bit.ly/3zTkMa6

EIOPA, 2021c, "Supervisory convergence plan for 2021," European Insurance and Occupational Pensions Authority, https://bit.ly/3ldJQ7h

Eling, M., and M. Lehmann, 2018, "The impact of digitalization on the insurance value chain and the insurability of risks," Geneva Papers on Risk and Insurance – Issues and Practice 43, 359-396

E.U., 2009a, "Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)," European Union, December 17, https://bit.ly/3iakANx

E.U., 2009b, "Directive EC/2009/128 on the taking-up and pursuit of the business of insurance and reinsurance," European Union, November 25, https://bit.ly/3fc9c1E

E.U., 2009c, "Directive EU/2009/65 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities," European Union, July 13, https://bit.ly/3xcOsgr

E.U., 2011, "Directive EU/2011/61 on alternative investment fund managers," European Union, July 1, https://bit.ly/3xkHuWY

E.U., 2012, "Regulation EU/2012/648 on OTC derivatives, central counterparties and trade repositories," European Union, July 27, https://bit.ly/3fd6QQj

E.U., 2013a, "Directive EU/2013/36 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms," European Union, June 27, https://bit.ly/3ldy4tD

E.U., 2013b, "Regulation EU/2013/575 on prudential requirements for credit institutions and investment firms," European Union, June 27, https://bit.ly/3fdqdlY

E.U., 2014a, "Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance," European Union, June 12, https://bit.ly/375yNFc

E.U., 2014b, "Regulation EU/2014/909 on improving securities settlement in the European Union and on central securities depositories," European Union, August 28, https://bit.ly/2V4SxGw

E.U., 2015, "Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market," European Union, December 23, https://bit.ly/2VkTRVm

E.U., 2016, "Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast)Text with EEA relevance," European Union, February 2, https://bit.ly/3fecZf3
InsuranceEurope, 2019, "Making EU insurance regulation that works and benefits consumers,"

Marano, P., 2019, "Navigating InsurTech: The digital intermediaries of insurance products and customer protection in the EU," Maastricht Journal of European and Comparative Law 26:2, 307-308

McKinsey, 2021, "Insurance 2030–the impact of AI on the future of insurance," McKinsey & Co., March 12, https://mck.co/3zSlrbz

SEC, 2017, "Statement on cryptocurrencies and initial coin offerings," U.S. Securities and Exchange Commission, https://bit.ly/3fcotiV

Zetzsche, D. A., F. Annunziata, D. W. Arner, and R. P.Buckley, 2020, "The markets in crypto-assets regulation (MICA) and the EU digital finance strategy," https://bit.ly/3fe0VKR