AIDA Europe Research Series on Insurance Law and Regulation 1

Pierpaolo Marano
Kyriaki Noussia *Editors*

InsurTech: A Legal and Regulatory View

Springer

AIDA Europe Research Series on Insurance Law and Regulation

Volume 1

Juan Bataller Grau, Polytechnic University of Valencia, Valencia, Spain
Laura Núñez, IE Business School, Madrid, Spain
Manfred Wandt, Goethe University Frankfurt, Frankfurt am Main, Germany
Simon Grima, Department of Insurance, University of Malta, Msida, Malta
Ecehan Yeşilova Aras, Yaşar University, Yaşar, Turkey

The AIDA Europe Research Series on Insurance Law and Regulation is the first book series of its kind and area of specialization. It comprises volumes on topics researched and written with an international, comparative or European perspective.

The regulatory response to the financial crisis in 2008 has pushed towards the adoption of transnational principles and rules also in the field of insurance by encouraging the convergence of national regulations to common regulatory framework. The need for a common legal language emerges to fully understand the process of transnational convergence in place and its impact on national legislation. On the other hand, persisting national peculiarities must be examined in the light of the transnational convergence of rules and concepts. Moreover, new risks, business practices and customers' issues are emerging worldwide, so requiring increasingly global responses.

The scope of the series is to bring together academics, practitioners and policy makers in order to exchange views and approaches to the topics concerned, which are based on the new transnational dimension of insurance law, business and regulation.

More information about this series at http://www.springer.com/series/16331

Pierpaolo Marano • Kyriaki Noussia
Editors

InsurTech: A Legal and Regulatory View

Springer

Editors
Pierpaolo Marano
Department of Legal Studies
Catholic University of the Sacred Heart
Milano, Italy

Kyriaki Noussia
Law School
University of Exeter
Exeter, UK

ISSN 2662-1770 ISSN 2662-1789 (electronic)
AIDA Europe Research Series on Insurance Law and Regulation
ISBN 978-3-030-27385-9 ISBN 978-3-030-27386-6 (eBook)
https://doi.org/10.1007/978-3-030-27386-6

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Part I
Technological Innovations and Insurance

FinTech, InsurTech, and the Regulators

Viktoria Chatzara

1 Introduction

The rapid developments in the FinTech and, particularly, the InsurTech industry, do not only affect the operations of the insurance industry, but are also highly disruptive to the operation of the competent regulatory authorities. New FinTech applications of a broad range and with very different nature, meanings and functions,[1] new methods and channels of product distribution, new forms of cooperation between industry players, and even the entry of non-financial institutions in the financial markets, all in a global, digitalized environment, create added complexities to the regulators when exercising their supervisory competences and powers.

The expansion of the FinTech industry breeds a number of questions concerning the scope of the regulation in the financial sector.[2] Which of the new FinTech applications and services should be subject to regulation? Will the insurer cooperating with a FinTech provider or the FinTech provider itself be regulated and supervised? What will be the case in more complex cooperation scenarios?

Apart from inquiring who and which activity will be subject to regulation, the question of which authority will be competent to regulate and supervise may still need to be answered: what would happen in the case of a FinTech provider, the

[1]Remarks by Svein Andresen (Secretary General, FSB), *Regulatory and Supervisory Issues from FinTech*, Cambridge Centre for Alternative Finance conference on Navigating the Contours of Alternative Finance, 29 June 2017, available at: http://www.fsb.org/wp-content/uploads/Cambridge-Centre-for-Alternative-Finance-Regulatory-and-Supervisory-Issues-from-FinTech.pdf.

[2]J.P. Morgan, *FinTech Redefining the Role of Regulators*, J.P. Morgan Chase & Co., 2017, available at https://www.jpmorgan.com/global/ts/tf2017/fintech.

V. Chatzara (✉)
Rokas Law Firm, Athens, Greece
e-mail: v.chatzara@rokas.com

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_1

services of which are used by insurers, credit institutions, and investment services providers? Which regulator should be competent over the insurance, the banking, or the investment activities, and to what extent? How could the issuance of contradictory decisions be prevented? Further, considering the globalization of the financial sector, particularly within the EU Single Market notion, and the cross-border provision of services that is the norm in the digitalized economy, it seems that the effective regulation of FinTech applications/services will require more, new, and enhanced forms of international cooperation between the competent national regulators.[3] Moreover, other regulatory authorities, apart from those competent in the financial services sector, such as the competition authorities, the data protection and telecommunications regulators, could be also involved for a number of issues.

The means and methodology used, as well as the time of regulation, are also critical. It is a fact—becoming more obvious in the case of FinTech developments—that regulators seem to always be one step behind the market.[4] The exponential development of FinTech applications also poses the questions whether the established regulatory competences and powers suffice for the regulators to effectively exercise their institutional roles, to what direction they should be further developed, and whether new ones should be elaborated.

Furthermore, for the market supervision to be effective, the regulator must have access to all the necessary and appropriate information concerning its operation and its participants. In the insurance sector and under the applicable Solvency II regime, insurance regulators mainly draw such information from the reports disclosed by the insurance undertakings, which, however, were not designed with a view to cover the FinTech (r)evolution. As such, regulators need to find alternative means and methods, to obtain appropriate and sufficient information concerning the interplay between FinTech applications and its operation in the insurance market, thereby enhancing their so-called "RegTech" capabilities. Within the recent years numerous national regulators, in an attempt to fully understand and keep up with the FinTech phenomenon, have launched FinTech regulatory "sandboxes", cooperating as such, not only with each other, but with other market players as well.

Another issue the regulators face refers to the necessary resources for the effective exercise of their role. Financial sector regulatory authorities are usually manned with personnel familiar with financial and legal notions. The FinTech penetration in the financial services sector, however, makes it clear that these skills and experiences will not be sufficient for the regulators to cope with the constant evolution. Thus, it seems that regulators will need to choose between either reorganizing and

[3]Monica Machler, *Calibrating the Regulatory Approach on New Technologies*, 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", Warsaw, 12 April 2018, available at: http://www.aida.org.uk/AIDAEurop/AIDA-Europe-Warsaw-presentations.asp.

[4]See an illustrative example concerning third-party payment operations: platforms such as Alipay began providing such services in 2003, but the competent authorities issued third-party payment licenses only in 2011—Ben Shenglin, *Fintech – Challenges to financial regulation and stability*, Part of the IFF China Report 2018, available at: https://www.centralbanking.com/central-banks/economics/3456571/fintech-challenges-to-financial-regulation-and-stability.

establishing technology departments with tech experts, or outsourcing competences and powers.[5]

In general, the development of FinTech and the increasing "InsurTech" participation in the insurance industry do not only affect insurers, but insurance regulators as well, causing them the need to quickly adapt into the new reality and posing an additional challenge to them to keep-up with the technological developments. Regulators are faced with a difficult balancing exercise between their traditional role to ensure the financial stability and consumer protection, on one hand, and, on the other hand, the need to not stifle innovation to follow the constantly changing needs of the consumers and the market, and to enhance the free competition within the relevant market. It is being argued, in this relevance, that regulators may now undertake a new role, as being proxies between innovation and law,[6] adopting such a regulatory stance to adapt long established laws and provisions into the new, digitalized reality, and legitimizing new products and services.

The disruption caused by FinTech in the operations of the regulators is evident on: international, EU, and national level. International schemes, such as the Financial Stability Board (FSB), the Organisation for Economic Co-operation and Development (OECD), and the International Association of Insurance Supervisors (IAIS) have produced papers to address the FinTech issue, whereas EIOPA and the other European Supervisory Authorities (ESAs) have established working parties and have undertaken initiatives, with the aim to examine and determine the regulatory approach to the phenomenon. At national level, numerous regulatory authorities launching further initiatives such as regulatory sandboxes, have proposed and adopted specific regulation to keep up with the developments.

Evidently, the entire financial sector is alerted regarding FinTech, and there is less focus on insurance when compared to banking and investment entities, which have experienced the FinTech effect somewhat earlier. However, the problematics and the cumulative effect of the solutions and actions taken can be employed by the insurance sector. A relevant short presentation follows in the next sections.

2 International Regulatory Cooperation

As explained, owing to the value of FinTech as an international phenomenon, regulators are trying to comprehend and address it on an international level. The FSB is one of the international bodies, active in the financial services sector, that has

[5]Gary Stern, *Can Regulators Keep Up with Fintech?*, Published by Yale School of Management, Yale Insights, 13 December 2017, available at https://insights.som.yale.edu/insights/can-regulators-keep-up-with-fintech.

[6]Kevin Petrasic, *The Role of Regulation in Financial Innovation: Does FinTech Need Regulation to Flourish?*, 20 December 2017, first appeared in Chambers Professional Advisers: Fintech, and available at: https://www.whitecase.com/publications/article/role-regulation-financial-innovation-does-fintech-need-regulation-flourish.

begun monitoring FinTech. OECD has also been monitoring the technological developments, both in the financial sector in general and in the insurance industry in particular. With respect to the insurance industry, the International Association of Insurance Supervisors (IAIS) has also issued a report concerning the FinTech developments in the insurance industry.

2.1 The Financial Stability Board's Approach

The Financial Stability Board (FSB), successor to the Financial Stability Forum (FSF), coordinates national financial authorities and international standard-setting bodies, with the mandate and the aim to promote and safeguard financial stability.[7] In this scope of work, the FSB understands FinTech as technologically enabled innovation in financial services that affects many different areas of financial services and may have implications on the financial stability, affecting the resilience of the financial system.[8] In this relevance, the FSB has issued two general reports, one identifying the main issues to the financial stability arising from FinTech developments that merit the regulators' attention, and one concerning the financial stability implications of the growing use of artificial intelligence (AI) and machine learning in financial services.[9] The FSB has also issued a more sector-specific report, along with the Committee on the Global Financial System (CGFS), concerning FinTech platforms engaging in credit provision, which concluded, among others, that such platforms could increase competition and put more pressure to the banks, but that FinTech could also lower lending standards, thus having negative consequences for financial stability.[10]

[7]Remarks by Svein Andresen, op.cit.

[8]See speech given by Mark Carney (Governor of the Bank of England and Chair of the FSB), *The Promise of FinTech – Something New Under the Sun?*, Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy", Wiesbaden, 25 January 2017, available at: https://www.bankofengland.co.uk/speech/2017/the-promise-of-fintech-something-new-under-the-sun.

[9]Financial Stability Board, *Artificial Intelligence and machine learning in financial services: Market developments and financial stability implications*, 1 November 2017a, available at: http://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/. This second report addresses the more specific issue of Artificial Intelligence (AI) and machine learning applications that are being rapidly adopted in the financial services industry, and the potential benefits and risks arising from them.

[10]See *FinTech credit: Market structure, business models and financial stability implications*, Report prepared by a Working Group established by the Committee on the Global Financial System (CGFS) and the Financial Stability Board (FSB), 22 May 2017, available at: http://www.fsb.org/2017/05/fintech-credit-market-structure-business-models-and-financial-stability-implications/.

The first report of the FSB, issued in June 2017,[11] addressed the issues arising from FinTech developments in the financial sector in general, identifying the potential benefits[12] and risks[13] to the financial stability,[14] and reviewing the steps already taken by regulators.[15] It is noted, however, in the report, that the assessments undertaken in it are challenging, mainly because of the lack of the necessary data and information on the FinTech activities; as official data is limited and any information derives from voluntary private disclosures, any conclusions drawn in the report could be subject to revision. Furthermore, considering that most FinTech activities are currently small compared to the overall financial system, the analysis in the report focuses on potential benefits and risks.

The FSB also identified 10 key issues of focus for the authorities, three of which are considered priorities for international cooperation.[16] The priority areas for international cooperation include:

- the management of operational risks from third-party service providers and the determination of whether the existing oversight frameworks for important third-party service providers to financial institutions are appropriate;
- the mitigation of cyber risks; and
- the monitoring of macrofinancial risks, although at this stage no compelling signs of any such risks materializing have been noted.

The other issues that merit the authorities' attention include any relevant cross-border legal issues and regulatory arrangements, the governance and disclosure frameworks for big data analytics, the assessment of the regulatory perimeter and its timely updates, shared learning and communication channels with the private sector, further development of open lines of communication across relevant

[11]Financial Stability Board, *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention*, 27 June 2017b, available at: http://www.fsb.org/2017/06/financial-stability-implications-from-fintech/.

[12]Such noted benefits include, among others, the greater decentralization and diversification caused by FinTech, the possibility of technological innovations to lead to greater efficiencies, better use of data, more transparent services, improved access to financial services, etc. See in this relevance p. 15 et seq of the *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention* Report.

[13]Although no evidence of any adverse systemic impact exists yet, the FSB identified both micro- and macro-financial potential risks, such as the risk of maturity mismatch (particularly in the field of FinTech lending operations), liquidity mismatch, operational risk arising from information systems, management failure, contagion, procyclicality, etc.

[14]The FSB also evaluated the interplay between the potential benefits and risks to the financial stability to better evaluate the potential implications of FinTech applications.

[15]According to FSB findings, 20 out of 26 reviewed jurisdictions have enacted or intend to enact policy measures on FinTech (such as publications, proposals, regulatory sand boxes, innovation hubs, etc.), while the others are considering changes and only one has assessed its existing framework as adequate.

[16]Page 29 et seq of the *Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention* Report.

authorities, ensuring adequate resources for the efficient regulation and supervision of the FinTech phenomenon, and studying alternative configurations of digital currencies. It is also highlighted that, at the current stage, it is crucial for regulators to gain a deeper understanding of the business models of both emerging FinTech companies and incumbents in the financial sector as they evolve.

2.2 OECD's Involvement with FinTech and InsurTech

The Organisation for Economic Co-operation and Development (OECD) has also addressed the issue of both the FinTech in general, and the InsurTech phenomenon in particular. According to OECD, the appearance and evolution of FinTech ranks among the structural changes to the trade finance market that occurred during the last decade, as companies active in this sector have become successful in sectors that had been traditionally occupied by credit institutions, while at the same time alternative trade finance solutions, such as supply-chain financing, have appeared.[17] According to the OECD, disruptions at supply level in the finance value chain, such as these caused by the evolution of FinTech, can affect the entire value chain and, consequently, affect the investment and growth in the whole economy. The OECD, as other international institutions, points out the significance to gather and examine more and better data and information on the phenomenon, to monitor and evaluate its evolution, and the evolving dynamics in the global finance market as well. With respect to FinTech companies, offering new and evolved services in the financial sector either on their own or in cooperation with traditional market players, OECD particularly notes that most of them, because of the new and innovative form of the services they provide, have not yet been subjected to the same regulatory constraints unlike traditional providers in the financial sector.

Apart from its work on the FinTech phenomenon in general, OECD has also addressed the issue of the technology penetration in the insurance sector, with its Insurance and Private Pensions Committee issuing in 2017 a report[18] in the context

[17]OECD, Directorate for Financial and Enterprise Affairs, Statistics Directorate, Working Party on Financial Statistics, *FinTechs and the Financial Side of Global Value Chains – Statistical Implications*, 18 October 2017b, available at: https://www.google.com/url?q=http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/%3Fcote%3DCOM/STD/DAF(2017)1%26docLanguage%3DEn&sa=U&ved=0ahUKEwi415veqfndAhVSzKQKHdH4BwgQFggFMAA&client=internal-uds-cse&cx=012432601748511391518:xzeadub0b0a&usg=AOvVaw2lHVjrXz5XPSN4oYW5EtK4.

[18]OECD (2017a), *Technology and innovation in the insurance sector*, available at: https://www.google.com/url?q=https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf&sa=U&ved=0ahUKEwiWj9f039PdAhUCgVwKHaXHAykQFggEMAA&client=internal-uds-cse&cx=012432601748511391518:xzeadub0b0a&usg=AOvVaw35pEXGS_a-RTBghdnkCRvf.

of its Going Digital project,[19] recording the InsurTech technologies having the potential to bring innovation to the insurance sector and affect the regulatory practices of insurance marks, examining how InsurTech is being funded and how insurers are engaging with start-ups entering the market. Further to reviewing the current situation in the InsurTech sector, OECD attempted to highlight the role of regulators in the further evolution of InsurTech. It started by stating that the entry of InsurTech, from a competition law point of view, could be viewed as having the potential to increase the competition in the relevant market, improve the efficiency in production and supply, and ultimately result in lower prices and wider choice.

From an insurance regulatory aspect, OECD notes that the currently applicable provisions on prudential capital and/or fit and proper requirements may be the cause that most InsurTech providers do not obtain insurance and/or insurance mediation licenses. Thus, the prudential requirements provisions, although important for financial stability purposes, may at the same time act as obstacles for the entry into the relevant market of new and innovative players and, as such, as a hindrance to free and greater competition. In this context, OECD documented the different approaches that national regulatory authorities begin to take to address InsurTech, ranging from regulatory sandboxes to the enactment of new regulation, with a particular focus on privacy and data protection issues that emerge from the new InsurTech applications.

The paper also pinpointed some wider policy considerations arising from the appearance of InsurTech and its entry in the relevant market. It is, for example, noted that ampler digital policies can assist in the development of technological solutions in the insurance markets.[20] In the same relevance, the efforts undertaken to improve cyber security could also assist in raising awareness to the public for the risks associated with internet-based transactions, as well as ensuring sufficient development of cyber security measures. With respect, particularly, to insurance regulation and supervision, as insurers are subject to direct audits, among others, on their IT systems, the competent authorities should examine ways in which such supervision could be carried out, to appropriately monitor the risks to insurers caused by the use of technological advances.

[19]Considering the ongoing digital transformation of economies and societies, OECD launched the "Going Digital" project, with the aim to construe a coherent and comprehensive policy approach, so that the digital evolution may result in stronger and more inclusive financial growth. Detailed information on the project and its preliminary findings are available at: http://www.oecd.org/going-digital/project/.

[20]The Estonia's ID card and digital signature services that resulted in the seamless incorporation of digital insurance solutions, as ID authentication can be easily facilitated, were mentioned as an example.

2.3 The View of the International Association of Insurance Supervisors

The International Association of Insurance Supervisors (IAIS) in the context of its mission as an international standard setting body to promote effective and globally consistent supervision of the insurance industry, aiming at fair, safe, and stable insurance markets, has addressed the FinTech evolution issue, with a focus particularly on its implications for the insurance industry.[21] In its report, IAIS proceeds with a description of the innovative technologies and business models that have the potential to transform the insurance business, their drivers, and their potential impacts. The analysis considered the main types of innovations that are currently affecting the insurance business, including, among other, digital platforms (internet, smartphones), Internet of Things (IoT), telematics/telemetry, Big Data and Data Analytics, Machine Learning and Artificial Intelligence, etc. The report noted as well that at this stage there are many uncertainties that prevent IAIS from reaching the most likely outcome and, hence, the impact on insurance regulation and supervision, which is anticipated to result from the combination of technology and the disruption it may cause to the insurance industry in the long term (supply side disruption), and societal changes, in the sense of consumer reactions from or influence to the insurance value chain (demand side disruption).

To reach some conclusions concerning the supervisory implications from InsurTech, the IAIS examined three different scenarios: one where insurers effectively maintain the overall customer relationship and use technology firms for their advantage, one where the insurance value chain is increasingly disaggregated and insurers rely on their business cooperation with technology firms or service providers for premium income, and one where big technology firms use their technology and analytical advantage to squeeze out of the market the traditional insurers. Following the above analysis and with respect to all three scenarios, the IAIS resulted in some core themes and supervisory considerations that (will) need to be addressed, including the following:

- **Competitiveness:** According to IAIS, it is expected to reduce longer-term. As such, IAIS enquires whether supervisors should take actions to encourage competition and new entrants in the relevant market.
- **Consumer choice:** It is also expected to reduce, because:
  - technology is expected to lead to more customized products, thus possibly to less comparability between product providers, and
  - existing insurers will benefit from increasing policyholder data. In this relevance, according to IAIS, supervisors will have to consider how to safeguard

[21] IAIS, *FinTech Developments in the Insurance Industry*, 21 February 2017, available at: https://www.iaisweb.org/page/news/other-papers-and-reports//file/65625/report-on-fintech-developments-in-the-insurance-industry.

the ability to compare products from different providers, and whether to legislate on data portability between providers.[22]

- **Interconnectedness:** The development of InsurTech, in combination with a limited number of technology platforms that support big data and increased data analytics, may pose an increased risk of interconnectedness.[23] In this relevance, supervisors will have to examine whether current reporting standards may need to be amended to capture additional information.
- **Regulatory oversight:** New players are expected to be added in the insurance value chain because of new technologies and business models, thus limiting the potential for effective regulatory oversight. Supervisors and policymakers may need to reassess the scope of the regulation to ensure adequate consumer protection and the ability of regulators to monitor the market trends.
- **Business model viability and prudential capital requirements:** In the end, there is a possibility that business models will become less resilient. As the risk-profile changes, regulators and policymakers will have to ensure the efficiency and adequacy of the applicable prudential capital frameworks.
- **Conduct of business:** Insurers and/or technology providers are anticipated to provide more on-demand products, which, however may result in the provided insurance products to reflect more the insurers' objectives and less the customers'.[24] IAIS enquired in this relevance, whether a minimum level of transparency for consumers should be required for any potential conflicts of interest to be highlighted.
- **Data ownership:** Personal data collected from customers and processed is expected to increase, particularly considering the use of internet-connected devices (IoT applications). On this aspect, the IAIS examined whether regulation concerning data protection and, particularly, Big Data technologies will have to be re-evaluated and amended, to address any new risks to the customers.

The IAIS concluded that the evolution in the FinTech sector is expected to pose new challenges to the competent insurance supervisors, who will, first, need to understand the functioning of the technological innovations, so that they can adequately assess the new product and business models. Any risks deriving from said

[22]On data portability issues, it should be noted that, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of their personal data (General Data Protection Regulation—GDPR) that entered into force since 25 May 2018, already provides the tools for "data portability" right in favor of the data subjects in its Article 20.

[23]The issue of interconnectedness is already evident, for example in the operation of online insurance aggregators selling motor vehicle insurance products. In such websites, upon entry of the motor vehicle's plate number, all the corresponding data of the vehicle (i.e. type, age, etc.) and of the registered owner (i.e. full name, age, driving license, etc.), seem to appear automatically in the relevant spaces.

[24]On the issue of insurance product design, at least insofar as the EU insurance market is concerned, the provisions of the Directive (EU) 2016/97 on the distribution of insurance products (IDD) and of the Commission Delegated Regulation (EU) 2017/2358, must also be considered.

innovations will have to be duly balanced against the benefits to the customers and the insurance sector as a whole; thus, technological innovation will have to be supported by the insurance supervisors. IAIS also pointed out that supervisors and policymakers will have to evaluate and, where needed, adapt the applicable regulatory framework, for any new risk and business models to be adequately addressed. As also highlighted by the FSB, supervisors will have to ensure adequate resources, knowledge and skills, to have the capacity to effectively deal with the new InsurTech evolutions.

3 Activities on the EU Level

Apart from the initiatives on the international level, the European Union has also endorsed the importance of the FinTech (r)evolution both in general and in particular for the financial services sector. In this relevance, the competent EU institutions[25] and the ESAs (and other organs) are addressing the different issues arising from the penetration of FinTech in the relevant markets in various ways, including by setting-up expert working groups and fora, by issuing communications, announcements and guidelines, and in general, by proposing new policies for the EU Single Market to reap the benefit from the technological boost, and at the same time to be appropriately prepared against the ensuing potential risks.

In the same context, the European Economic and Social Committee (EESC) addressed the issue of the IoT emergence from a more general standpoint, particularly considering the issues arising from its use with respect to consumer and business safety and privacy. In its Opinion *"Trust, privacy and security for consumers and businesses in the Internet of Things"*,[26] the EESC referred to the notion of the IoT and its economic and social benefits as part of a globalized world, as well as to the problems deriving from its use, such as the difficulties that may arise in identifying liability in case of law violation or third-party damage, and the security issues that are inherent to the IoT use. In this context, the EESC proposed a series of actions to be taken by the competent authorities, with the aim of minimizing any potential adverse affects of the IoT, such as the creation and promotion of regulatory sandboxes, the appointment of independent institutes and agencies as caretakers of IoT projects, encouraging European and international standardization, ensuring affordable, high-quality access to all IoT users, guaranteeing the effective operation of alternative and online dispute resolution mechanisms, and establishing an appropriate collective redress system.

[25]The European Commission's actions related to FinTech may be found at: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/fintech_en.

[26]European Economic and Social Committee, Opinion *"Trust, privacy and security for consumers and businesses in the Internet of Things (IoT)"* [own-initiative report], INT/846, 19 September 2018, available at: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/trust-privacy-and-consumer-security-internet-things-iot-own-initiative-opinion.

3.1 The European Commission's Approach

The European Commission has taken numerous steps to fully comprehend and evaluate the FinTech phenomenon and its implications for the financial services sector. In its relevant Communication describing an EU FinTech Action Plan,[27] the Commission views FinTech as a domain where the themes of financial services and digital single market meet. According to the Commission, FinTech applications have the ability to provide better access to finance and improve financial inclusion, assist in the deepening and broadening of the EU capital markets, facilitate the achievement of compliance obligations for regulated entities, but at the same time create new challenges both to such regulated entities, and to regulatory authorities, and the markets at large as well.

One of the primary issues examined by the Commission in its FinTech Action Plan is the issue of the licensing requirements that may apply to FinTech providers and applications under the EU or respective national sector specific laws, which aim to allow effective supervision, consumer protection, and uniform operating conditions. Considering the fact that national regulators do not always adopt uniform approaches on the implementation of these requirements, and that new financial services may not always fall into the scope of the applicable EU law provisions, the Commission invited the ESAs to map the current authorizing and licensing approaches for innovative FinTech business models, and issue, where appropriate, guidelines on such approaches and procedures. As far as the national regulators are concerned, the practices of innovation hubs[28] and regulatory sandboxes[29] are also addressed. In this context, it was proposed that the ESAs continue mapping such FinTech facilitators, identify best practices, and even issue guidelines on these facilitators, whereas the Commission mentioned that it will issue within 2019 a report on best practices for regulatory sandboxes. What is important with respect to FinTech facilitators is that the Commission is seen to encourage their adoption by all the competent national regulators, despite the fact that not all of them accept these practices as falling within their scope of work and competences.

The Commission's Action Plan refers to other issues to be further addressed for FinTech solutions to be able to enhance the quality of the financial products and

[27]Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, *FinTech Action Plan: For a more competitive and innovative European financial sector*, COM (2018) 109/2, 08.03.2018, available at: https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

[28]In the sense of institutional arrangements where interested entities (either regulated or not) may discuss FinTech-related issues with the competent supervisory authorities, and seek the latters' opinion on whether a contemplated new business model would be compliant with the applicable regulatory requirements, or clarifications on such applicable requirements.

[29]Regulatory sandboxes constitute a controlled space/environment created by the competent supervisory authorities, within which regulated firms and FinTech providers may test their FinTech applications for a limited time to validate and test their contemplated business models.

services provided in the EU Single Market, and for any potential risks, such as cyber-related risks, data, consumer and investor protection, and market integrity issues to be effectively tackled. Such points include, among others, the development of common EU standards for FinTech solutions, the need to enhance interoperability, removing obstacles to the use of cloud computing services by means of EU guidelines, cross-sectoral self-regulatory codes of conduct or standard contractual clauses, strengthening the cyber-resilience of the financial sector, etc. The issue of technology neutrality of the applicable EU rules is also brought up, as it is mentioned that the enactment of the applicable EU rules precedes the technological innovations and, consequently, does not always encapsulate subsequent developments.[30]

Further to its FinTech Action Plan, the Commission also launched in February 2018 the EU Blockchain Observatory and Forum, with the aim to accelerate blockchain innovation and development within the EU to establish the EU as a global leading blockchain forum. In the context of its general mandate, the EU Blockchain Observatory and Forum monitors blockchain initiatives in Europe, gathers knowledge on blockchain solutions, constitutes an attractive and transparent forum for sharing information and opinions, and recommends actions to be taken at EU level.[31] In the context of its mission, the EU Blockchain Observatory and Forum has already issued a series of thematic reports on blockchain-related themes, including a report on Blockchain Innovation in Europe[32] and a report on Blockchain and the GDPR.[33] The Commission has organized relevant workshops on blockchain-related issues, such as its "Blockchain in Europe" Workshop hosted in Vienna on May 22, 2018, in which the current state of blockchain innovation in Europe is examined and proposals for future priorities are made.[34]

The Commission also noted in its FinTech Action Plan[35] that one of the important issues to be tackled is the fact that the competent national regulatory authorities do not have deep knowledge and understanding of the FinTech solutions, their operation, and their applications in the financial sector. In this relevance, the Commission established the EU FinTech Lab, with the aim to raise the level of

[30]The EU insurance law provisions on the disclosure of precontractual information are a characteristic example in this relevance, namely the relevant provisions of the Insurance Distribution Directive (IDD), according to which insurance distributors, as a rule, shall provide to their clients the necessary precontractual information in paper form, whereas another stable means or electronic provision of the information is permitted as an exemption and under specific conditions.

[31]More information on the EU Blockchain Observatory and Forum and its mission is available at https://www.eublockchainforum.eu/.

[32]The detailed report from this Workshop is available at: https://www.eublockchainforum.eu/sites/default/files/reports/20180613_workshop_report_blockchain_innovation_europe.pdf?width=1024&height=800&iframe=true.

[33]The detailed report is available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf?width=1024&height=800&iframe=true.

[34]First edition published on 27 July 2018 and revised on 21 August 2018, available at: https://www.eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf?width=1024&height=800&iframe=true.

[35]See pages 14 and 15 of the Commission's FinTech Action Plan.

capacity and knowledge on FinTech innovations and, in general the new technologies, of the national regulators, in the context of which the competent officers will be directly informed and trained by market participants, while relevant regulatory and supervisory issues will be discussed. The EU FinTech Lab met for the first time on 20 June 2018 and discussed the issue of cloud outsourcing in banking and insurance sectors.[36]

3.2 The European Supervisory Authorities' Actions

In combination with the actions taken at a general EU level, the European Supervisory Authorities (ESAs) also address the issue of the FinTech developments and their implications in the financial sector, from a more specific-oriented point of view.

EIOPA's Take on InsurTech

Particularly concerning the insurance market and FinTech's/InsurTech's impact thereon, the European Insurance and Occupational Pensions Authority (EIOPA) acknowledges that InsurTech's effects span across the value chain of the insurance market from the stage of product design and development, across pricing and underwriting, and until claims management. Considering this, according to EIOPA, InsurTech solutions create new opportunities for consumers, in the sense that they may result in more personalized products and services, better customer experience, enhanced transparency and competition; and for the insurance industry, as InsurTech developments can be more cost efficient, enhance the companies' risk assessment process, create direct access to customers, including targeted, individualized advertisements, and assist in the companies' compliance procedures ("RegTech") and their efforts against insurance fraud. At the same time, EIOPA's view is that InsurTech may also cause new risks to both consumers (such as, risks concerning the fair pricing treatment of consumers, privacy and data ownership issues, exclusion of non-digital customers, etc.) and to the industry (e.g. cyber-risk, IT flaws, entry of new competitive market players, etc.).[37]

In view of the importance of InsurTech according to EIOPA's view, EIOPA organized on 28 April 2017 its first InsurTech Roundtable, with representatives from supervisory authorities, consumers, incumbents, start-ups, consultancy firms, and IT

[36]The Agenda of this first meeting may be found at: https://ec.europa.eu/info/sites/info/files/180620-eu-fintech-lab-agenda_en.pdf.

[37]Fausto Parente, Executive Director of the European Insurance and Occupational Pensions Authority (EIOPA): *"Calibrating the Regulatory Approach on New Technologies"*, 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", 12 April 2018 Warsaw, Poland, available at: http://www.aida.org.uk/docs/2018-04-12%207thAIDAEuropeConferenceEIOPAsInsurTechActivitiesFaustoParente.pdf.

experts to discuss the benefits and risks of the digitalization of the insurance market, and any potential obstacles to effective financial innovation. The Roundtable addressed a number of issues,[38] such as the impact of digital technologies in the insurance value chain, the advent of new players, blockchain and smart contracts, peer-to-peer insurance, artificial intelligence, etc., most of which referred to the specific issue of Big Data and their importance for the insurance sector.[39] The significance of data and data processing for the insurance industry was directly linked to the emergence of IoT applications and their use in insurance, in particular in motor insurance, and in household and health insurance, which allows for more accurate prediction of risks and events, more personalized pricing, products and services, and may even have broader results, such as assist in the reduction of motor accidents by providing incentives for more safe driving habits. The participants also pinpointed potential downfalls from the use of IoT applications in insurance, such as the fact that personalized products may not permit comparison between the different products, or that high-risk consumers may face access issues. On 9 November 2017, EIOPA conducted a 2nd InsurTech Roundtable that addressed numerous issues, including the impact of InsurTech on underwriting, the relation between Big Data and risk management, and the relation between Big Data and pricing.[40]

Apart from the Roundtables, EIOPA established a multi-disciplinary InsurTech Task Force (ITF),[41] with the mandate to lead EIOPA's work in connection with the issues arising from the development of InsurTech, expected to complete its work by the end of 2020. According to the prioritization made by EIOPA, the ITF will, primarily, proceed with a thematic review on Big Data by insurers and intermediaries, map the innovation facilitators established by national insurance regulators, examine the current authorizing and licensing requirements and the application of the proportionality principle in the area of financial innovation in particular, and assess whether guidelines on the outsourcing to cloud service providers must be issued by EIOPA. It is noted in the ITF's Mandate that at a later stage it could also undertake other works, including further assessment of the design and use of algorithms to determine how such complex IT tools and processes may be best

[38]A summary of the discussions in EIOPA's first InsurTech Roundtable is made in EIOPA-BoS/17-165, *EIOPA InsurTech Roundtable: How technology and data are reshaping the insurance landscape*, 05 July 2017a, available at: https://eiopa.europa.eu/Publications/Reports/08.0_EIOPA-BoS17-165_EIOPA_InsurTech_Roundtable_summary.pdf#search=InsurTech.

[39]The role of Big Data for the financial services sector in general has been acknowledged by all three ESAs, the Joint Committee of which issued a Discussion Paper on the Use of Big Data by Financial Institutions, available, along with the responses to it, at: https://www.esma.europa.eu/press-news/consultations/joint-committee-discussion-paper-use-big-data-financial-institutions.

[40]A preliminary agenda of EIOPA's 2nd InsurTech Roundtable and further information may be found at: https://eiopa.europa.eu/Pages/Events/2nd-InsurTech-Roundtable.aspx.

[41]The Mandate of EIOPA's InsurTech Task Force, as published on 13 April 2018, EIOPA-BoS-17/258, may be found at: https://eiopa.europa.eu/Publications/Administrative/InsuTech%20Task%20Force%20Mandate%20-%20BoS.pdf#search=EIOPA%2DBoS%2D17%2F258.

supervised, examine and propose remedies to the supervisory challenges arising from new business models, and maybe even establish a European Insurance Innovation Hub.

ESMA's Input on the FinTech Problematic

The European Securities and Markets Authority (ESMA), acknowledging the importance and the effects of FinTech in the relevant markets, participated actively in the public consultation launched by the European Commission for the issuance of its FinTech Action Plan by submitting its responses and thoughts on a number of topics[42], such as crowdfunding, outsourcing and cloud computing, distributed ledger technology, the role of regulation and supervisors, etc. Furthermore, ESMA's third Financial Innovation Day on 10 February 2017 was dedicated to FinTech and its impact on regulation, the market, and the consumers.[43] ESMA's findings and actions may provide the insurance market with complementary insight to those of EIOPA in the FinTech area.

EBA's Activity in Relation to the FinTech Phenomenon

The European Banking Authority (EBA) has established a FinTech Knowledge Hub,[44] with the aim to enhance the cooperation between the competent authorities, and with FinTech firms, technology providers and regulated entities, the monitoring of financial innovation, knowledge sharing, and to ensure that any regulatory and supervisory approaches are consistent with the principle of technological neutrality. The FinTech Knowledge Hub was established by the FinTech Roadmap published by EBA following a public consultation,[45] which also sets out EBA's priorities for 2018–2019. Said priorities include the evaluation of licensing and authorization approaches towards FinTech companies and analyses the existing national FinTech facilitators (innovations hubs, regulatory sandboxes) to identify a set of best practices and assist in achieving consistent and coordinated supervisory practices, monitoring innovation and assessing the possible risks and opportunities arising from new business models, promoting best supervisory practices concerning the

[42]ESMA's responses to the Commission's public consultation are available at: https://www.esma.europa.eu/press-news/esma-news/esma-responds-commission-consultation-fintech.

[43]More detailed information on the topics discussed in the various panels of the third Financial Innovation Day may be found at: https://www.esma.europa.eu/risk-analysis/innovation-products/financial-innovation-day.

[44]The dedicated page of EBA's FinTech Knowledge Hub is: https://www.eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub.

[45]The *EBA's FinTech Roadmap, Conclusions from the consultation on the EBA's approach to financial technology (FinTech)*, published on 15 March 2018a, and available at: https://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf.

assessment of cybersecurity issues, examining consumer issues arising from FinTech applications, etc. Based on its FinTech Roadmap, EBA issued on 3 July 2018 two reports concerning the prudential risks and opportunities arising from FinTech,[46] and the impact of FinTech on the business models of credit institutions.[47]

4 Activities on National Level

The FinTech phenomenon and its impact in the financial services sector have been in the focus of national regulatory authorities as well, both within Europe and across the globe. A number of national authorities have established innovation facilitators, either innovation hubs or regulatory sandboxes, whereas other states have opted in favor of enacting new regulatory provisions to address specific issues arising from the rapid technological evolution (e.g. from the appearance and use of autonomous vehicles). There are also national authorities that operate a contact point to which FinTech companies may address their questions on licensing requirements, disclosure obligations, compliance obligations, etc. As it is beyond the scope of this paper to describe and refer to each one of the national initiatives, some indicative examples are presented below.

4.1 The United Kingdom example

On 7 August 2018 the Financial Conduct Authority (FCA) in cooperation with 11 more financial regulators and related organizations announced the creation of the "Global Financial Innovation Network" (GFIN),[48] aiming at promoting communication and interaction between FinTech companies and regulators, and cooperation between national regulators on innovation-related topics. A consultation was launched (until 14 October 2018) concerning the functions of the GFIN. Among the proposed main functions, there is the idea of the establishment of a "global sandbox" which will provide FinTech firms with an environment in which they will be able to test the solutions they intend to provide on a cross-border basis and receive respective feedback from the competent authorities.

[46]EBA Report on the prudential risks and opportunities arising for institutions from FinTech, published on 3 July 2018b, and available at: https://eba.europa.eu/documents/10180/2270909/Report+on+prudential+risks+and+opportunities+arising+for+institutions+from+FinTech.pdf.

[47]EBA Report on the impact of FinTech on incumbent credit institutions' business models, published on 3 July 2018c, and available at: https://eba.europa.eu/documents/10180/2270909/Report+on+the+impact+of+Fintech+on+incumbent+credit+institutions%27%20business+models.pdf.

[48]More detailed information is available at: https://www.fca.org.uk/news/press-releases/fca-collaborates-new-consultation-explore-opportunities-global-financial-innovation-network.

Other than engaging in the above initiative, UK authorities have also decided to address technological innovation issues by reviewing existing legislation and assessing whether changes need to be made. Namely on the introduction of autonomous vehicles, the UK Government has instructed a review of the existing driving laws to examine any legal obstacles thereto and identify any needs for regulatory reforms.[49] According to the publicly available information, the competent Law Commission of England and Wales and the Scottish Law Commission will examine crucial questions, including who is the "*driver*" or the responsible person, how to allocate civil and criminal responsibility in the event that there is some human control, the role of automated vehicles in public transport networks, whether there is a need for new criminal offenses, etc.

4.2 The Swedish example

Sweden is one of the largest hubs for FinTech innovation, with approximately 1/5 of the European FinTech investments. In this context, and for these statistics to remain, the Swedish Government gave a mandate in May 2017 to the Swedish Financial Supervisory Authority, which in turn established a FinTech Regulatory Sandbox, in which FinTech providers may submit their ideas and contemplated projects and request for regulatory guidance directly from the authority. The FinTech Regulatory Sandbox is expected to assist primarily the FinTech companies in obtaining the necessary information and guidance from the regulator and in ensuring that their proposed solutions are in line with any applicable regulatory requirements, as well as the Financial Supervisory Authority, which in this way will be in a better position to monitor the developments in the financial market.

The Swedish government is actively engaged in promoting innovation in Sweden, having established the Swedish National Innovation Council, presided by the Prime Minister.

4.3 The Hong Kong example

The Insurance Authority (IA) of Hong Kong has launched various initiatives to promote innovation and its application in the business models of authorized insurers.[50] In September 2017, an InsurTech Sandbox was launched, where

[49]"Government to review driving laws in preparation for self-driving vehicles", 6 March 2018, available at: https://www.gov.uk/government/news/government-to-review-driving-laws-in-preparation-for-self-driving-vehicles.

[50]Detailed information on the Insurance Authority's InsurTech initiatives may be found at: https://www.ia.org.hk/en/aboutus/insurtech_corner.html.

authorized insurers and technology companies cooperating with authorized insurers may test the innovative technological solutions they intend to apply in their business models, under the principles of the Sandbox's operation,[51] and collect market information, as well as user feedback, before launching their new products and services into the market. Also in September 2017, the IA launched a fast track procedure concerning exclusively applications for authorizations of new insurers using solely digital distribution channels. Considering that insurers authorized under the Fast Track procedure will not be permitted to accept business from non-digital channels, the IA also adopted general principles applicable on this special authorization procedure to safeguard the policyholders' interests.[52]

The IA has also established an "InsurTech Facilitation Team" to promote communication with InsurTech companies active in the field of developing and implementing InsurTech solutions. The Team's objective is to assist InsurTech providers in gaining a better understanding of the applicable insurance regulatory requirements, to act as a platform for the exchange of ideas, and to provide advice in InsurTech-related topics. Furthermore, the Future Task Force of the Insurance Industry[53] has been established and cooperates with the IA, with the aim to explore the future of the insurance industry in Hong Kong. One of its working groups is the Financial Technology—FinTech group, with a focus on promoting the application of FinTech in the insurance industry.

4.4 The Singapore example

One of the countries known as "homes" of innovation is Singapore. Singapore and its competent Monetary Authority (Monetary Authority of Singapore—MAS) is considered a progressive regulator, closely following up on technological innovation and even encouraging it. In this context MAS established, as early as August 2015, its Financial Technology and Innovation Group (FTIG),[54] as competent to form

[51] According to these principles, every trial must have a clearly defined scope (e.g. timing, duration, size and type of insurance business, target market, technology involved, etc.), adequate control procedures must be in place for the supervisory requirements to be met, adequate consumer protection safeguards must be also adopted, the insurer must have adequate resources and be able to demonstrate the InsurTech initiative is ready for testing, as well as have an exit strategy in place in the event that the trial has to be terminated, among others.

[52] Such principles include that all solvency, capital, and local asset requirements must be met, whereas any other requirements may be modified or non-applicable in the event that IA decides so, all policyholder protection measures apply, the IA may impose restrictions on the insurance products to be sold by Fast Track insurers, etc.

[53] Further details are available at: https://www.ia.org.hk/en/aboutus/task_force/introduction_of_future_task_force.html.

[54] FTIG comprises three divisions: (a) Payments & Technology Solutions Office, which engages with regulatory policies and strategies for simple, swift, and secure payments, (b) Technology Infrastructure Office, which is responsible for promoting safe and efficient technology enabled

regulatory policies and strategies to facilitate the use of technology and innovation to the benefit of the financial sector. MAS, furthermore, acknowledged the need for close cooperation between different competent authorities and established in May 2016 a FinTech office, the members of which include MAS, the Economic Development Board of Singapore, Infocomm Investments Pte Ltd, Info-communications Media Development Authority, the National Research Foundation, and SPRING Singapore.[55]

Moreover, MAS has adopted the regulatory sandbox practice, with the aim to prevent companies from not implementing their innovative solutions if they are not sure of such solutions' compliance with the applicable legal and regulatory regime. MAS's FinTech sandbox aims to enable financial institutions and FinTech companies to experiment with innovative financial products and services in a secure and controlled environment. The regulatory support provided by MAS[56] to innovations entering the sandbox consists in relaxing, for the duration of the experiment, specific legal and regulatory requirements, which would be otherwise applicable. MAS undertakes further initiatives and has become a hub in showcasing innovation in areas such as the future of banking, InsurTech, Blockchain and distributed ledger technology, RegTech, et al.[57,58]

5 Summary and Conclusions

The rapid developments in the InsurTech and, more generally, in the FinTech universe affect not only the operation of the insurance industry, but also the activities of the regulatory authorities that are competent for the supervision of the financial sector. Regulators face the challenge of adapting to the new market conditions, while it seems they will be required to exercise their powers and competences in a way that will balance between their mission to safeguard financial stability and consumer

infrastructure for the financial sector in areas such as cloud computing, big data and distributed ledgers, and (c) Technology Innovation Lab the object of which is to search for innovative technologies with potential application in the financial industry and to cooperate with the industry and relevant parties to test-bed innovative new solutions.

[55]See in this relevance: http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/MAS-Role.aspx.

[56]More details on the conditions and operation of MAS's FinTech Regulatory Sandbox may be found at: http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox.aspx.

[57]The also featured Global FinTech Hackcelerator is a competition for innovative start-ups looking to address problems from the financial industry. Detailed information is available at: https://fintechfestival.sg/.

[58]More information on the Global FinTech Hackcelerator 2018 can be found at: https://fintechfestival.sg/festival-line-up/hackcelerator/.

protection on the one hand, and, on the other, the need to foster innovation and free competition in the relevant markets.

In this regard, a number of fundamental questions arise. The scope of regulation in connection with the new FinTech/InsurTech services and providers, considering the relationship between said providers and financial services incumbents, will have to be defined. As various FinTech services may be made available across the financial sector, the question will arise as to who will be the competent regulator. In the same context, as the new FinTech/InsurTech services address the global market, the geographical scope of the regulators' competence will have to be addressed. Various other questions are of relevance, concerning the appropriateness and sufficiency of the available supervisory tools, methods, and resources.

International and EU organizations, authorities and fora, including FSB, OECD, IAIS, EIOPA, and the European Commission, as well as national regulatory authorities, are shifting their focus on the regulatory issues arising from the penetration and rapid evolution of technology, and on the potential benefits and risks it may cause. In this context, they have undertaken initiatives with the aim to better understand the FinTech/InsurTech phenomenon and to determine the appropriate regulatory approach to it.

To mention some significant actions, the FSB has identified a number of key issues for the national regulators, including three points that are considered priorities for international cooperation: (a) the management of operational risks from third-party service providers and the assessment of the adequacy of the existing regulatory frameworks, (b) the mitigation of cyber-risks, and (c) the monitoring of macrofinancial risks. The OECD has also specifically focused on examining the penetration and the impact of technology in the insurance sector. From an insurance point of view, the IAIS has examined the InsurTech impact on the insurance market and has defined some core themes and supervisory considerations that will need to be addressed.

On an EU level, the European Commission has assessed the impact of FinTech and has issued a relevant Action Plan, while also establishing the EU Blockchain Observatory and Forum. The European Supervisory Authorities are taking actions to determine their approach towards the FinTech phenomenon going forward. From a purely insurance point of view, EIOPA has established a multi-disciplinary InsurTech Task Force (ITF), with the aim to address the issues arising from the development of InsurTech.

A number of national regulatory authorities, such as the UK, Sweden, Hong Kong, and Singapore have taken specific initiatives, including the formation of innovation facilitators and dedicated working groups that aim to increase the communication and interaction between regulators and market players.

In the challenge of the rapidly evolving scenery, legislators, and regulatory bodies are called to invest on human talent and technology resources, while the inherently trans-border nature of the phenomenon calls for active international cooperation in the field of legislation and supervision.

References

Andresen S (Secretary General, FSB) (2017) Regulatory and supervisory issues from FinTech. Cambridge Centre for Alternative Finance conference on Navigating the Contours of Alternative Finance, 29 June 2017. Available at: http://www.fsb.org/wp-content/uploads/Cambridge-Centre-for-Alternative-Finance-Regulatory-and-Supervisory-Issues-from-FinTech.pdf

Carney M (2017) (Governor of the Bank of England and Chair of the FSB), *The Promise of FinTech – Something New Under the Sun*?, Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy", Wiesbaden, 20 January 2017. Available at: https://www.bankofengland.co.uk/speech/2017/the-promise-of-fintech-something-new-under-the-sun

Commission Communication to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, *FinTech Action Plan: For a more competitive and innovative European financial sector*, {COM(2018) 109/2}, 08 March 2018, available at: https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

EBA (2018a) FinTech Roadmap, Conclusions from the consultation on the EBA's approach to financial technology (FinTech), 15 March 2018. Available at: https://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf

EBA (2018b) EBA Report on the Prudential Risks and Opportunities arising for institutions from FinTech, 3 July 2018. Available at: https://www.eba.europa.eu/documents/10180/2270909/Report+on+prudential+risks+and+opportunities+arising+for+institutions+from+FinTech.pdf

EBA (2018c) EBA Report on the Impact of FinTech on incumbent credit institutions' business models, 3 July 2018. Available at: https://www.eba.europa.eu/documents/10180/2270909/Report+on+prudential+risks+and+opportunities+arising+for+institutions+from+FinTech.pdf

EIOPA (2017a) EIOPA InsurTech Roundtable: how technology and data are reshaping the insurance landscape, EIOPA-BoS/ 17–165, 5 July 2017. Available at: https://eiopa.europa.eu/Publications/Reports/08.0_EIOPA-BoS17-165_EIOPA_InsurTech_Roundtable_summary.pdf#search=InsurTech

EIOPA (2017b) Preliminary Agenda of EIOPA's 2nd InsurTech Roundtable. Available at: https://eiopa.europa.eu/Pages/Events/2nd-InsurTech-Roundtable.aspx

EIOPA (2018) Mandate of EIOPA's InsurTech Task Force, EIOPA-BoS-17/258, 13 April 2018. Available at: https://eiopa.europa.eu/Publications/Administrative/InsuTech%20Task%20Force%20Mandate%20-%20BoS.pdf#search=EIOPA%2DBoS%2D17%2F258

ESAs Joint Committee (2016) Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions, JC/2016/86, 19 December 2016. Available at: https://www.esma.europa.eu/press-news/consultations/joint-committee-discussion-paper-use-big-data-financial-institutions

ESMA (2017a) Third Financial Innovation Day. Available at: https://www.esma.europa.eu/risk-analysis/innovation-products/financial-innovation-day

ESMA (2017b) Responses to the Commission's public consultation on FinTech. Available at: https://www.esma.europa.eu/press-news/esma-news/esma-responds-commission-consultation-fintech

EU Blockchain Observatory and Forum (2018a) Thematic report – Blockchain and the GDPR, first edition published on 16 October 2018. Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf?width=1024&height=800&iframe=true

EU Blockchain Observatory and Forum (2018b) Workshop report – Blockchain Innovation in Europe, Rathaus Vienna, May 22, 2018, published on 13.06.2018. Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20180613_workshop_report_blockchain_innovation_europe.pdf?width=1024&height=800&iframe=true

EU Blockchain Observatory and Forum (2018c) Blockchain Innovation in Europe, first edition published on 27 July 2018 and revised on 21 August 2018. Available at: https://www.

eublockchainforum.eu/sites/default/files/reports/20180727_report_innovation_in_europe_light.pdf?width=1024&height=800&iframe=true

EU FinTech Lab (2018) 1st Session Agenda – Cloud Outsourcing, 20 June 2018. Available at: https://ec.europa.eu/info/sites/info/files/180620-eu-fintech-lab-agenda_en.pdf

European Economic and Social Committee (2018) Opinion "Trust, privacy and security for consumers and businesses in the Internet of Things (IoT)" [own-initiative report], INT/846, 19 September 2018. Availableat: https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/trust-privacy-and-consumer-security-internet-things-iot-own-initiative-opinion

FCA (2018) FCA collaborates on new consultation to explore the opportunities of a Global Financial Innovation Network, 7 August 2018. Available at: https://www.fca.org.uk/news/press-releases/fca-collaborates-new-consultation-explore-opportunities-global-financial-innovation-network

Financial Stability Board (2017a) Artificial Intelligence and machine learning in financial services: Market developments and financial stability implications, 1 November 2017. Available at: http://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/

Financial Stability Board (2017b) Financial Stability Implications from FinTech: Supervisory and Regulatory Issues that Merit Authorities' Attention, 27 June 2017. Available at: http://www.fsb.org/2017/06/financial-stability-implications-from-fintech/

Financial Stability Board – Working Group established by the Committee on the Global Financial System (CGFS) and the Financial Stability Board (2017) FinTech credit: market structure, business models and financial stability implications, 22 May 2017. Available at: http://www.fsb.org/2017/05/fintech-credit-market-structure-business-models-and-financial-stability-implications/

Gov.uk (2018) Government to review driving laws in preparation for self-driving vehicles, 6 March 2018. Available at: https://www.gov.uk/government/news/government-to-review-driving-laws-in-preparation-for-self-driving-vehicles

IAIS (2017) FinTech Developments in the Insurance Industry, 21 February 2017. Available at: https://www.iaisweb.org/page/news/other-papers-and-reports//file/65625/report-on-fintech-developments-in-the-insurance-industry

Insurance Authority of Hong Kong, *InsurTech Corner*, at: https://www.ia.org.hk/en/aboutus/insurtech_corner.html

J.P. Morgan Chase & Co. (2017) FinTech redefining the role of regulators. Available at: https://www.jpmorgan.com/global/ts/tf2017/fintech

Machler M (2018) Calibrating the regulatory approach on new technologies. In: 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", 12 April 2018, Warsaw, Poland. Available at: http://www.aida.org.uk/AIDAEurop/AIDA-Europe-Warsaw-presentations.asp

OECD (2017a) Technology and innovation in the insurance sector. Available at: https://www.google.com/url?q=https://www.oecd.org/pensions/Technology-and-innovation-in-the-insurance-sector.pdf&sa=U&ved=0ahUKEwiWj9f039PdAhUCgVwKHaXHAykQFggEMAA&client=internal-uds-cse&cx=012432601748511391518:xzeadub0b0a&usg=AOvVaw35pEXGS_a-RTBghdnkCRvf

OECD (2017b) Directorate for Financial and Enterprise Affairs, Statistics Directorate, Working Party on Financial Statistics, *FinTechs and the Financial Side of Global Value Chains – Statistical Implications*, 18 October 2017. Available at: https://www.google.com/url?q=http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/%3Fcote%3DCOM/STD/DAF(2017)1%26docLanguage%3DEn&sa=U&ved=0ahUKEwi415veqfndAhVSzKQKHdH4BwgQFggFMAA&client=internaludscse&cx=012432601748511391518:xzeadub0b0a&usg=AOvVaw2lHVjrXz5XPSN4oYW5EtK4

Parente F (2018) EIOPA's InsurTech Activities, 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", 12 April 2018, Warsaw, Poland. Available at: http://www.aida.org.uk/docs/2018-04-12%207thAIDAEuropeConferenceEIOPAsInsurTechActivitiesFaustoParente.pdf

Petrasic K (2017) The Role of Regulation in Financial Innovation: Does FinTech Need Regulation to Flourish?, 20 December 2017, first appeared in Chambers Professional Advisers: FinTech, and available at: https://www.whitecase.com/publications/article/role-regulation-financial-innovation-does-fintech-need-regulation-flourish

Shenglin B (2018) FinTech – Challenges to financial regulation and stability, Part of the IFF China Report 2018. Available at: https://www.centralbanking.com/central-banks/economics/3456571/fintech-challenges-to-financial-regulation-and-stability

Singapore FinTech Festival, at: https://fintechfestival.sg/

Stern G (2017) Can Regulators Keep Up with FinTech?, Published by Yale School of Management, Yale Insights, 13 December 2017. Available at: https://insights.som.yale.edu/insights/can-regulators-keep-up-with-fintech

Insurance in Today's Sharing Economy: New Challenges Ahead or a Return to the Origins of Insurance?

Margarida Lima Rego and Joana Campos Carvalho

1 Introduction

In the early twenty-first century, technology-based peer-to-peer (P2P) business models have been popping up, multiplying and succeeding. These business models set themselves apart from the traditional business-to-consumer (B2C) models. This paper aims at identifying and outlining the new types of technology-based business models in use in the insurance sector. We began our quest in search of the new challenges to the law of insurance brought about by such business models and found ourselves face to face with some new takes on the oldest forms of insurance known to humanity.

The new business models we have analysed can be broken down in three different classes: the broker model, the carrier model and the self-governing model.

The broker model and the carrier model rely on traditional insurance players but allow customers to take on part of the risks insured by the group they happen to fall into or choose to adhere to and take back a portion of their profits, or at least make customers feel like they are taking on those risks and taking back such profits. The industry is well-versed in such attempts: for many years, life-insurers have been

M. L. Rego (✉)
NOVA University's School of Law, Lisbon, Portugal

CEDIS – Centro de Investigação e Desenvolvimento sobre Direito e Sociedade, Lisbon, Portugal
e-mail: margarida.rego@fd.unl.pt

J. C. Carvalho
NOVA University's School of Law, Lisbon, Portugal

CEDIS – Centro de Investigação e Desenvolvimento sobre Direito e Sociedade, Lisbon, Portugal

FCT – Fundação para a Ciência e a Tecnologia, Lisbon, Portugal

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_2

giving back part of their surplus to their policyholders in the form of yearend bonuses. In fact, the leading characters in such models appear to play, to a large extent, the same roles traditionally ascribed to insurers and insurance intermediaries. Whilst they may incorporate P2P elements, they are not, in essence, true P2P models.

We deliver a brief outline of some of these existing models and provide a more detailed account of an example thereof. Since we have found great similarities between the broker model and the carrier model, our choice fell on an instance of the broker model, which is the most complex of the two models, the object of our more detailed account being the entity best known as *Friendsurance*.

We then move on to examine the self-governing model, where we believed the most innovative and challenging arrangements were to be found. We have found that the most innovative aspects of the broker and carrier models are also present in the self-governing model but have been further developed and brought to a different level by disposing of insurers and insurance carriers altogether and simply providing the platform and the assistance which enables end-users to come together and meet their own insurance needs. In this part of the paper we analyse the entity best known as *Teambrella*.

After identifying the contracting parties in the self-governing model and their roles, our attention falls on the new challenges this model brings forward: do contracts entered into through these platforms qualify as insurance contracts? Should insurance regulation apply to them? These questions, we find, have been asked and answered many times over in the past. Hence, our research ended up providing an excellent opportunity for a look back into the origins of insurance.

2 Insurance in the Peer-to-Peer Economy

In peer-to-peer (P2P) business models, unlike in business-to-consumer (B2C) models, a business is usually involved, but typically, it will act as an intermediary that facilitates direct interaction between relevant players. The contract is often made possible by a company operating an online platform but is concluded between two or more peers. Well-known examples of P2P businesses include *Airbnb*, *eBay* or *Craigslist*.

Such models are said to integrate the so-called 'sharing economy',[1] which includes any economic activity involving an online platform—a virtual marketplace—which provides information and facilitates direct contacts between supply

[1] Although much has been written about the subject, there is no consensus around the definition of, or even the conceptual suitability of the expression 'sharing economy' (see Codagnone and Martens 2016). Some authors have found evidence indicating that the term 'sharing' has positive connotations of equality, selflessness and giving and is used to attach these ideas of positive social relations to what in fact are highly profitable commercial transactions (Belk 2014, p. 10; John 2013, pp. 176–177). Nevertheless, although scientifically not very rigorous, the expression 'sharing economy' is by far the most commonly used to refer to the object of our study, so we have chosen

and demand, thus allowing for a collaborative optimisation of resources through an effective use of excess capacity.

The definition of peer is not yet entirely consensual in academic literature. Definitions that one commonly finds in a regular dictionary highlight the relativeness of the term: no one is intrinsically a peer, one may only be someone else's peer. That is to say, the word can only be properly used in the plural, even if such plural is merely implicit, as it is used to describe a relationship between two or more subjects. That relationship is one of parity or symmetry: generally, a peer is defined as "a person of the same age, status, or ability as another specified person."[2]

In the context of P2P relationships, a peer is sometimes portrayed as an individual: a natural person, as opposed to a legal person.[3] In other instances, a peer is identified as a non-professional[4]: someone who offers goods or services on an occasional basis.

The latter notion is narrower than the first in that it excludes natural persons acting as professionals.[5] However, it seems to be more to-the-point: the expression 'peer-to-peer' is habitually used to set these relationships apart from business-to-consumer relationships. What is thus important is to establish whether one acts as professional or non-professional. There is no symmetry in a contract where one of the parties is acting as a professional and the other one is not.[6] A professional almost always has more experience and knowledge about the business than a non-professional. This lack of symmetry is what justifies the need for special protection rules in B2C contracts.

We would argue, however, that even this second approach is not entirely comprehensive.

Symmetry is at the core of a P2P relationship. A P2P relationship thus exists whenever two players are acting on the same level, regardless of whether they are both professionals or both non-professionals. Returning to the idea of the relativity of the concept: both a professional and a non-professional can be qualified as peers; it will depend on the qualification of their counterparty. A non-professional will be qualified as a peer if their counterparty is a non-professional; a professional will be qualified as a peer if their counterparty is a professional. P2P relationships thus include both consumer-to-consumer (C2C) and business-to-business (B2B) relationships.

Nevertheless, when authors refer to P2P as opposed to B2C business models, they are oftentimes not at all concerned about whether contracting parties are actually

---

to use it, because it is the simplest and most immediate way of explaining what we are writing about (Sundararajan 2016, p. 27).

[2]English Oxford Living Dictionaries 2018, https://en.oxforddictionaries.com/definition/peer.

[3]Lougher and Kalmanowicz (2016), p. 2.

[4]Smorto (2015), p. 4.

[5]In another sense, it may also be characterised as wider than the first one if small and medium-sized companies are also allowed in, at least, when acting outside of their scope of business.

[6]Paisant (2015), p. 39; Carvalho (2018), p. 40.

peers. The term is often imprecisely used to refer to a model where there is an intermediary, usually a platform operator, between the parties, who is responsible for creating and managing a marketplace. For instance, Airbnb is frequently used as an example of a P2P business model. However, both professional and non-professional hosts and usually only non-professional guests operate on Airbnb.

In the insurance sector, the expression 'P2P insurance' is used to describe new technology-based business models which allow the insured to pool their risks and their capital, self-organise and self-administer so as to minimise their losses and maximise their gains.[7] P2P insurance is indeed about risk and capital pooling, given that in these models at least a part, sometimes the entirety of the risk is carried by the peers themselves. These models aim to reduce costs commonly associated with insurance underwriting and claims handling by their use of innovative digital technology,[8] as well as to cut or at least reduce the insurer's profit margin, typically by giving any excess premiums back to the policyholders in years when the total losses are lower than the aggregate premiums[9] and having the platform's retained funds or ultimately reinsurers pay for the excess losses in years where the opposite occurs.[10]

For centuries, this has been done by mutual insurers[11] and reciprocal insurance exchanges.[12] In today's sharing economy, online collaborative platforms provide regular people with new, apparently simpler means of pursuing this age-old end.[13] In this sense, "P2P represents as much a return to the old roots of insurance as a leap

[7]See National Association of Insurance Commissioners (2018). In July 2018, EIOPA published a "stakeholder survey on licensing requirements, barriers to InsurTech and InsurTech facilitation". In this survey, P2P insurance is defined as a "risk sharing digital network or platform where a group of individuals with mutual interests or similar risk profiles pool their 'premiums' together to insure against a risk/to share the risk among them, and where profits are commonly redistributed at the end of the year in case of good claims experience". The survey is available at: https://ec.europa.eu/eusurvey/runner/EIOPA_survey_licensing_barriers_to_InsurTech_InsurTech_facilitation.

[8]For Wilson (2017), p. 123, P2P insurance also provides an answer to the needs of a new generation that no longer wants a distant relation with the insurers, but seeks "personalized products, unrestricted access and assistance, and frequent and tangible benefits".

[9]On its website, *Friendsurance* claims that "so far more than 80% of users have received a cashback. In the property insurance line, the average cashback has been 30% of the paid premiums".

[10]Sagalow (2016), p. 6.

[11]Mutual insurance associations still play a very relevant role, especially in maritime insurance, where members of the International Club of P&I Clubs (protection and indemnity associations) purportedly provide in aggregate liability cover for "approximately 90% of the world's ocean-going tonnage" (https://www.igpandi.org/). According to Clarke (2005), p. 44, "the mutuals together insure the owners (and many of the charterers) of some 98 per cent of the world's ocean-going ships for their liabilities toward third parties – their traditional business". According to the same author, "[f]rom the beginning the clubs have been in the forefront of innovation, undertaking novel risks that others were too conventional to recognize or too cautious to rate" (p. 45).

[12]Reciprocal insurance exchanges have been around in the United States since at least the 1880s. See Fitzgerald (1920), Norgaard (1964) and Reinmuth (1964).

[13]Orlovácz (2016), p. 191, points out that "online communities have reached a large enough scale for the mutual insurance model to work efficiently, this time not bound by geographical barriers".

forward. Reflecting the very nature of the sharing economy, P2P insurance leverages the latest technological advances in social networking to best apply the model mutual insurance companies have basically used since the early days of insurance".[14]

But there is more to it than that. In addition to the above financial aspects of P2P business models, the latter are also said to help reduce conflicts at claim time, by avoiding existing conflicts of interest between insurance companies and their policyholders.[15] In traditional business models, paying more claims means a lower profit margin for the insurance companies. In a business model where the company's profit is based on commissions,[16] there is no incentive to delay or hinder the payment of claims.

Finally, yet most relevantly, new psychological insights are also explored, P2P models claiming that the insured's strong sense of community and of shared assets helps reduce loss ratio because of a significant decrease in low[17] or fraudulent claims.[18] The wrongness of fraud against one's peers is thus more stringently felt than that against an insurance company.[19] The same can be said of the wrongness of negligent loss, which means that the new models purportedly reduce moral hazard in general.[20] Some people also highlight the importance of giving insurance customers a sense of empowerment: making them feel in control of the product that they are actively creating rather than passively adhering to.[21]

Because of the reduced incentive to suffer negligent loss and to present low or fraudulent claims, P2P insurance business models are therefore said to have benefits not only for the customers but also—albeit arguably[22]—for insurance companies.

This sense of community is sometimes so strongly highlighted that in some models it outweighs the financial aspects, for instance when excess premiums are returned not to the policyholders themselves but to an NGO pursuing a common cause on the basis of which the risk and capital pool was prearranged, such as the protection of animal rights or the environment.

[14]National Association of Insurance Commissioners (2018).

[15]Holly and Greszta (2016), p. 58; Paperno et al. (2016), p. 1.

[16]This is the case especially in the carrier model that will be analysed in Sect. 3.2.

[17]This helps lower the administrative costs, Swiss Re (2016), p. 36.

[18]Holly and Greszta (2016), p. 59. See also Sagalow (2016), p. 7.

[19]Cappiello (2018), p. 40, stresses that "the knowledge and mutual trust of the members of the group means that there is a natural disincentive to fraud".

[20]Yan et al. (2017), p. 254; Huckstep (2015).

[21]See EIOPA (2017), pp. 12–13.

[22]Although no empirical study has yet been carried out to confirm it, many authors argue that this model has benefits for the insurance companies: Yan et al. (2017), p. 254; Soberón (2016), p. 53; Marin (2016), p. 42; Holly and Greszta (2016), p. 59.

> The core idea of P2P is that a set of like-minded people with mutual interests group their insurance policies together introducing a sense of control, trust, and transparency while at the same time reducing costs.[23]

We shall see that in most cases, P2P models do not entail the scratching of the insurer entirely out of the equation but rather a redefinition of its role.[24]

Currently, it is possible to distinguish between three different P2P insurance models: (i) the broker model; (ii) the carrier model; (iii) the self-governing model. We shall see that whilst some of them truly allow and promote the interaction between platform users and the conclusion of contracts between them, others are much closer to the traditional role insurers still play: their users do not conclude contracts between them at all, merely sharing—or having a sense that they share a risk, as a consequence of the type of contract they have concluded with the company.[25]

3 New Business Models in the Insurance Sector

3.1 The Broker Model

Examples: *Friendsurance*[26]*/Inspeer.*[27]

Companies that use this model act as intermediaries between the insurance companies and their customers. They organise the customers in groups, collect the premiums and hand over a part of them to the insurance company. The rest of the money is put into a pool. Throughout the year, claims presented by group members are paid using that pool. At the end of the year, some companies give what is left in the pool back to all the group members or use it to reduce the following year's premiums, others give it to a designated charity. If the money in the pool is insufficient to cover all claims, a contingency insurance will kick in.

Friendsurance is a German company founded in 2010. It has established partnerships with over 70 insurance companies. Customers choose an insurance product made available by one of these companies and pay the same price they would pay if they concluded the contract directly with the insurance carrier. Part of the money is handed directly to the insurer. *Friendsurance* then forms groups of people that have purchased the same kind of insurance and the rest of the money will be used to pay

[23]National Association of Insurance Commissioners (2018).

[24]Carballa Smichowski (2015), p. 62.

[25]Turcotte (2017), p. 81, argues that most of the start-ups that use the concept of P2P insurance do not present a pure P2P model and not even a new model. The majority integrates an existing model into a new technological environment, allowing the subscription and claim presenting processes to be faster, increasing transparency and lowering management costs.

[26]Friendsurance 2019: https://www.friendsurance.com. Friendsurance (Alecto GmbH) is a licensed broker in Germany and has announced its plan to expand to Australia.

[27]Inspeer 2019: https://ve.inspeer.me/. Inspeer (Avenir Factory) is a licensed broker in France.

the deductibles (or the claims if lower) throughout the year. At the end of the year, any amount that is left in the fund is divided amongst its members and used to pay a part of their premiums for the following year. *Friendsurance*'s business model will be further analysed in 2.

Inspeer is a French company operating since 2015. They began by offering a service where customers would keep the insurance they already had, but would join a group of people who would pay each other's deductibles in case of a claim. That meant that they could enter into insurance contracts with higher deductibles, thus lowering the amount of the premiums. In the meantime, its business model has evolved and *Inspeer* now focuses on insurance for electric vehicles only. They act as intermediaries but, unlike *Friendsurance*, they work with only one insurance carrier. Customers are not divided into groups. There is only one fund, called collaborative fund, where a portion of the premiums is kept which is then used to pay claims throughout the year. At the end of the year, what remains is paid back to the customers.

Although it does not provide a broker service like the ones presented above, *VouchForMe* also deserves a few words, as it fosters a change in the insurance ecosystem by allowing people to share the value of the deductibles, through a blockchain-based product. *VouchForMe* was founded in 2015 (as *Insurpal)*. They obtained an "MGA insurance license" (managing general agent license) to start a pilot project in the United Kingdom in 2018 and launched the first version of their product in December 2018.[28] They started by focusing on insurance, claiming to be the next generation of peer-to-peer insurance, with a business model that is based on social proof endorsements and uses the blockchain technology. The change of name in July 2018 meant a broadening of the company's scope, allowing for the model to be used outside insurtech.[29] VouchForMe provides an online tool, that helps someone who wants to conclude an insurance contract to ask for a guarantee from his/her friends. This allows the insurance client to agree to a higher deductible, which will be covered by these guarantees, thus lowering the insurance premium. The guarantor only pays in case the insured files an at-fault claim. Part of the risk is thus shared between them. The main idea behind the model is that people behave more carefully if they know that their behaviour will directly affect an individual, specific and identifiable someone else, rather than an abstract collective of others.[30]

[28]VouchForMe 2018: https://medium.com/vouchforme/first-version-of-the-vouchforme-live-678f1ac89d99.

[29]The company wanted to step away from a deep connection to insurance: "After all this time, there were many circumstances where we have been mistaken for an insurance company, thinking we're selling insurance policies or acting as a mediator between insurance companies. However, our brand represents a Blockchain based platform with an implemented social proof model, which can be used in various ways and through divergent industries". VouchForMe 2018: https://medium.com/vouchforme/more-than-a-name-change-c41421b57b17.

[30]VouchForMe 2018: https://medium.com/vouchforme/vouchforme-partners-with-swissdacs-55e089a3cb7c.

3.2 The Carrier Model

Examples: *Lemonade*[31]*/Hey Guevara*[32]*/Alan*[33]

The second model of P2P insurance is similar to the first in that policyholders are gathered in groups and a part of their premiums is put into a fund that is used to cover the claims presented throughout the year. However, in this model there is no intermediary. The insurance company sells its own policies and also forms the groups and manages the funds.

Lemonade is a licensed insurance company based in New York State.[34] Founded in 2015, it is the first American insurance carrier using the P2P insurance model.[35] They group people based on the charity they choose. At the end of the year, the remaining funds in the pool are given to the chosen charity. This strategy procures that people in the same group have some shared interests and ideally some shared values, as they have chosen the same charity to support.

Hey Guevara is a UK-based company founded in 2013. It closed its operations in September 2017[36] but has announced a comeback in 2018.[37] *Hey Guevara*'s business model is similar to *Lemonade*'s but it began by limiting its offer to motor insurance. It focused its business model on the feeling of affinity and placed a great importance on the choice of the group. It stresses the importance of having an association with the group you join because the model relies on keeping claim expenses down. Allegedly, if customers know their claims will directly affect friends or family, they are more likely to have a responsible attitude towards risk taking and to only claim what is necessary.[38] Premiums paid by the customers are split in two with one part going into the group's fund—the 'Protection Pool'—and the rest going into a collective pot that supports all groups. The claims customers present throughout the year are paid from the Protection Pool. If that is not enough then the collective fund is used. Lastly, in the event that the collective pot is not enough, reinsurance will jump in. *Hey Guevara* is reinsured by a traditional carrier.

---

[31]Lemonade 2019: https://www.lemonade.com.

[32]Guevara 2019: https://heyguevara.com.

[33]Alan 2019: https://www.alan.eu/.

[34]In 2017, *Lemonade* started expanding and offering services in several other states (https://www.lemonade.com/blog/lemonade-expansion-united-states/).

[35]See National Association of Insurance Commissioners (2018).

[36]See Shi and Geoghegan 2017: https://www.insuranceinsider.com/articles/114457/p2p-insurer-guevara-shuts-up-shop.

[37]Guevara 2019: https://heyguevara.com/. The website announces that a new website is coming soon and that they plan to shake up the way people do home, auto, life, motorcycle, and small-business insurance policies. *Uvamo* is another example of what was announced as a new U.S.-based tech-based start-up insurance carrier wishing to explore the P2P insurance model, but at this point, it is unclear whether it is still in existence. See a reference thereto in National Association of Insurance Commissioners (2018). See also Ben-Hutta 2017: https://coverager.com/end-line-uvamo/.

[38]Huckstep (2015).

Alan is a licensed health insurer based in France. It claims to be "the first digital health insurance company in Europe". It obtained its licence to operate as an insurance carrier in 2016. It is still at its early stages as an insurer, but in April 2018 it raised 28 million USD in 10 days in a fundraising operation led by *Index Ventures*.[39] It provides a health plan which complements the social security system to companies and self-employed individuals. Its sales strategy focuses on providing paperless, top quality customer service and improve customer experience: it markets the idea of health care made simple and accessible.[40]

3.3 The Self-governing Model

Example: *Teambrella*.[41]

The self-governing model appears to be the only true[42] P2P model. In this model, no insurer, reinsurer or insurance intermediary is allegedly involved. No premiums are paid and the risk is shared solely amongst the members of a group, according to the terms they define. The role of the platform operator is to provide the technological means for the model to work: the company merely provides a virtual marketplace through which anyone can communicate, enter into and perform contracts.[43]

Teambrella claims to be the first company using this model. It was founded by Russian developers in 2015.[44] It was not created as a Blockchain itself but it uses bitcoin wallets to make payments, which allows it never to be in possession of any actual funds. Participating peers are organised into self-regulating, self-governing groups, which means that the exact rules that apply to each will vary to some extent. Each group member is assigned a bitcoin wallet from which the reimbursements are made. This means that, at this point, the money still belongs to the group members themselves, although typically a minimum sum must be available in the wallet, according to the group rules, and a number of co-signatures by other group members is necessary to withdraw the coins, bringing it closer to an escrow-type account.[45]

Such sums are only used if a claim is made within the group, and to the extent that the money is needed to pay for the loss. Each time someone presents a claim, the group members vote to decide whether that claim should be accepted and how much should be paid to the loss sufferer under the pre-existing rules of the relevant group.

---

[39]Samuelian 2018: https://blog.alan.eu/our-toolkit-to-raise-28-million-in-10-days-b40dc936084d.

[40]Robert 2017: https://blog.alan.eu/changer-la-donne-en-assurance-santé-8d62cfb96cd0.

[41]Teambrella 2019: https://teambrella.com/.

[42]Zwack (2017), p. 108.

[43]Although pure P2P insurance models are predicted to be on the rise, especially the ones using blockchain technology (Gatteschi et al. 2018, p. 9), most customers still value personal interaction (Ernst & Young 2012, p. 13).

[44]Paperno et al. (2016).

[45]See National Association of Insurance Commissioners (2018).

All payments are made using bitcoins. Each member's exposure equals the sum available in its digital wallet.

4 A Closer Look at *Friendsurance*

4.1 Contracts Concluded with the Website's Visitors

Friendsurance is a brand name, the legal entities behind it being Alecto GmbH and Megara GmbH. The following description is based on information publicly available at www.friendsurance.com.

Alecto GmbH, the website's operator, provides its own terms of use in the form of a set of standard terms (in German *Allgemeine Geschäftsbedingungen*, hereinafter "AGB").[46] The AGB purport to regulate Alecto GmbH's relationship with the website's visitors. Thus, they include the terms of use of the website itself by such visitors, as well as the rules that purport to govern the relationship that ensues once such visitors enter into insurance contracts through that website. The AGB are neither aimed at regulating the dealings of the website's visitors with one another, nor between such visitors and any third parties, including the insurers, even if such relationships do take form by means of the website.

Contracts regulated by these AGB are concluded only after users sign up on the website. By concluding the sign-up procedure, each user issues a contractual offer.[47] By making the reserved area on the site available to the user, Alecto GmbH accepts this offer to provide online insurance intermediation and related services and the contract is concluded. After that, the user can start benefitting from the services offered by Alecto GmbH.

4.2 Services Provided by Alecto GmbH and by Megara GmbH

In Germany, an entity wishing to pursue the business of insurance mediation must obtain a license and register either as an insurance broker (*Versicherungsmakler*) or an insurance agent (*Versicherungsvertreter*).[48] The broker provides its services independently: it is bound to act solely in accordance with the best interests of its customers when selecting the most suitable products available on the market to recommend thereto, whereas the agent is contractually bound to distribute the

[46]Friendsurance 2019: https://www.friendsurance.de/agb.

[47]See § I.2-e AGB.

[48]See §§ 5 and 11 of the German Insurance Mediation and Advice Act (*Verordnung über die Versicherungsvermittlung und -beratung*). The law sets forth a third class of registered service provider: the insurance advisor (*Versicherungsberater*).

products of one or more insurers, there being no requirement that it act neutrally in its choice of products. Whenever a more flexible structure is preferred, economic groups will often resort to the incorporation of two different companies. This is the reason behind the coexistence of two different intermediaries acting under the trademark *Friendsurance*[49]:

Alecto GmbH is registered at the German Chambers of Industry and Commerce as an independent broker (*Versicherungsmakler*)[50] whilst Megara GmbH is registered thereat as an insurance agent (*Versicherungsvertreter*).[51]

From a contractual perspective, this circumstance does not appear to be of particular relevance. It suffices to say that such insurance intermediaries appear to be following a well-known path commonly found in more traditional offline distribution channels, the solution being unrelated to any challenge specifically derived from the new virtual environment giving rise to the sharing economy.

The AGB distinguish two types of services provided by Alecto GmbH, depending on the types of insurance on offer. In some cases, such as personal liability and household insurance, Alecto GmbH will provide classic insurance mediation services acting in its capacity as an independent broker. The most interesting feature of this model lies in the fact that the independent selection of the most suitable product is carried out by means of an algorithm: the user is asked to select a few set parameters and, based on user's selection, it is the system that automatically picks out the insurance products which best match the user's selection, from a relatively large number of potential insurance providers, and which then presents such products to the user. The most suitable products are then ordered based on different possible criteria, such as the cheapest option, the option that offers the best value for money or that which is offered by the most renowned insurer.

The website provides information about insurance and related services on offer by third parties, the actual insurance and related contracts being entered into between the users and third party insurers.[52] Alecto GmbH claims not to be responsible for loss arising from false or inaccurate information on the insurance products contained on its website.[53] Alecto GmbH claims that only the contents included in the contract entered into between a user and the insurer are binding, the information provided on its website not having any influence on the contract.[54]

Upon request by a user, namely by clicking on a certain product, Alecto GmbH will provide a contract form. The user can fill it out and submit it through the platform, Alecto GmbH conveying it to the relevant insurer.[55] Alecto GmbH's

[49]Kemnitz 2017: https://blog.friendsurance.de/friendsurance-und-die-megara-gmbh-wir-klaeren-auf/.

[50]See § I.5-a AGB.

[51]See § I.5-c. AGB.

[52]See § I.5-a AGB.

[53]See §§ I.5-f and IV.2 AGB.

[54]See § I. 5-k AGB.

[55]See § I.5-i AGB.

remuneration consists of a commission paid by the insurer, no sums being charged for this service directly from the website's users/policyholders by Alecto GmbH.[56]

In the second type of service provided by Alecto GmbH, it claims not to intermediate insurance at all.[57] Whenever this is the case, Alecto GmbH, which is the website's operator, presents itself as a simple messenger (*Bote*) between the website's users and its sister company Megara GmbH. The latter is acting in its capacity as a registered insurance agent (*Versicherungsvertreter*). This is the case, for instance, in the distribution of insurance of electronic goods, such as cellphones or laptops. In this case, the products of a single insurance provider are displayed on the website. Users may only choose between different packages (standard, comfort and premium) on offer by that single insurer, with differing levels of coverage and related optional services. In these cases, Alecto GmbH claims to act as the technical provider of the virtual platform used by Megara GmbH to display the products it distributes and to collect the users' contractual offers, once submitted, which it then conveys to Megara GmbH.

4.3 The Claims-Free Cashback

One of the most distinctive features of the *Friendsurance* business model is its integration of a solution that they call a "claims-free cashback". Now there is nothing intrinsically new about the contractual stipulation of a no-claims bonus. However, there is more to it than that, as this feature is what brings this business model much closer to a P2P model. Hence, we provide a more detailed breakdown thereof.

In some types of insurance, the website's users can choose to benefit from a so-called group principle (*Gruppenprinzip*).[58] This possibility is currently available for the following types of insurance: personal liability, household, legal protection and motor insurance. Users who opt for this possibility are placed in small groups: they are composed of approximately ten members. Users can handpick other group members—friends, relatives or other prior acquaintances—or choose to let the system automatically place them into a group. To enter the group, users must enter into a series of "assistance contracts" (*Beistandsvereinbarungen*) with the other group members. The contract terms for these agreements are provided by Alecto GmbH on the website (hereinafter "BV").[59] The conclusion of these contracts occurs through the *Friendsurance* platform. Any amendment or the termination of such contracts must also be carried out through the *Friendsurance* platform.[60]

[56]See § I.5-p and -o AGB.

[57]See § I.5-c. AGB.

[58]See § I.7-a AGB.

[59]Friendsurance 2019: https://www.friendsurance.de/beistandsvereinbarung.

[60]See §§ 6 and 7.1 BV.

The premium that will be paid by these users under the main insurance contract is lower than the one they would pay when entering into the insurance contract on their own, because the insurance contract includes a high deductible which will then be complemented by a stop-loss and deductible-buyback insurance.[61] No savings will originally occur because in addition to that main premium users must also pay the extra premium which is due under the stop-loss and deductible-buyback insurance, which eats up all the difference between the premium that would be payable in the main insurance contract if no deductible or the lowest available deductible were to be stipulated and the premium that would apply to the same contract with the highest possible deductible, added by fixed amount ranging between € 2 and € 7.5.[62]

Premiums paid under this extra insurance are eligible to the claims-free cashback: if no claims are filed during the relevant period, users will be entitled to claim their cash back. Whenever a group member files a claim, that claim eats up a portion of each group member's potential cashback, including the one filing the claim, because those sums will cover the high deductible applicable under the main insurance to the member filing a claim.[63] In the worst-case scenario, the cashback is exhausted and no cashback will be paid to group members when the year is over, but then the stop-loss insurance kicks in, making sure that under no circumstances will group members be called in to pay for someone else's or their own high deductible. Whenever this scenario does not materialise and at the end of the year, there is still money left in the cashback pool, such money will be reimbursed to the group members, who may then use it to partly cover the following year's premiums if they enter into new insurance contracts through *Friendsurance*.

When filing a claim, users are also given the possibility of waiving their right to collect the contributions from other group members, that is to say, their right to use up the group's cashback pool. In that case, they will be solely responsible to bear their own deductible in the main insurance contract.[64]

On their website, *Friendsurance* claims that the average cashback of their customers has been 30% of paid premiums.[65]

The above-mentioned insurance contracts are naturally entered into with insurers. The insurer in the main insurance contract can be one of the business' many insurance partners. There appears to be only one available insurer in the stop-loss and deductible-buyback insurance: Hübener Versicherungs-AG.

As the website operator, Alecto GmbH provides the platform that facilitates the conclusion of these insurance contracts, as well as the assistance contracts between group members.[66] These agreements only become effective if concluded through the

[61] See Friendsurance 2019: https://www.friendsurance.de/ausfallversicherung.

[62] See Friendsurance 2019: https://www.friendsurance.de/ausfallversicherung.

[63] See §§ 3.3 and 4.1 BV.

[64] See § I.8-b AGB.

[65] See Friendsurance 2019: https://www.friendsurance.com/.

[66] See § I.6-a AGB.

Friendsurance website.[67] Alecto GmbH provides the contract terms for these agreements on its website.[68] For instance, each user can issue a contractual offer by inviting another user to connect on the platform. If the other user accepts this offer, also through the platform, the assistance contract is concluded. The contract concluded between Alecto GmbH and the user determines that Alecto GmbH intermediates the conclusion of the assistance contracts between users but is otherwise not involved in the assistance contracts.[69] It allows users to contact each other but does not represent any of them.[70] This mediation service is free of charge.[71]

As we have seen above, Alecto GmbH also provides classic insurance mediation services acting in its capacity as an independent broker. When an insured event occurs, users can also submit their claims through the website.[72] Alecto GmbH informs other group members of the loss sustained and of how much their contribution to the deductible will be.[73] It also forwards the claim to the insurer with whom the user has concluded the main insurance contract.[74]

Megara GmbH is the agent intermediating the stop-loss and deductible-buyback insurance. It handles payments to and from the insurer in case of a claim, as well as any cashback reimbursements due to its customers at the end of the year.[75] Megara GmbH is also entrusted by the parties to the assistance contracts (BV) to verify whether claims should be deemed as covered, in cases where they are lower than the deductible.[76] Megara GmbH thus plays a significant role in every insurance contract where there is a cashback possibility, irrespective of whether the main insurance contracts are intermediated by Alecto GmbH in its capacity as an independent broker or by the agent Megara GmbH.

4.4 The Inosculation of P2P Elements onto a B2C Model

Having gone through the broker and the carrier business models in general and having analysed the *Friendsurance* contractual structure more closely, we have reached the conclusion that, to a large extent, the leading characters in such models appear to play the same roles traditionally ascribed to insurers and insurance

[67] See § I.6-c AGB.
[68] Friendsurance 2019: https://www.friendsurance.de/beistandsvereinbarung.
[69] See § I.6-b AGB.
[70] See § I.6-e AGB.
[71] See § I.6-f AGB.
[72] See § I.8-a AGB.
[73] See § I.8-b AGB.
[74] See § I.8-c AGB.
[75] See §§ I.7-d and I.8-g AGB.
[76] See § 2.4 BV.

intermediaries in ordinary B2C contexts.[77] They do, however, take advantage of new technologies by incorporating some P2P elements in their otherwise traditional insurance solutions.[78]

Apart from that, it is also important to note that these brokers assume a more prominent role than that of many, if not all traditional brokers. *Friendsurance*, for instance, is a strong brand, that people associate with an innovative type of insurance and a certain standard of quality, which may be decisive in the customer's choice of contract. In some cases, there may even be some confusion for the customer as to whom his or her counterparty in the insurance contract really is. This raises some questions around the liability of the broker (a platform operator), namely as to whether it may validly and effectively claim not to be liable for loss arising from false or inaccurate information on the insurance products provided by its website.[79] Although very interesting, this subject is beyond the reach of this paper.

Our next move is to examine a model that took this to a different level by getting rid of these structures completely, designing insurance solutions that take the insurance carrier out of the equation and allow customers to come together and meet each other's insurance needs.

5 Discussion: The Model Put Forward by *Teambrella*

The self-governing model offers insurance with a catch: the contracts it facilitates are technically not qualified as insurance contracts in the traditional sense because an essential element thereof is missing: the individuals entering into such contracts do not pay any insurance premiums.[80]

---

[77]Marano (2019), p. 13, suspects that if the new models of the so-called P2P insurance were to be scrutinised they might reveal an "emptiness of differences", proving to be, in essence, no different from traditional insurance models.

[78]See Turcotte (2017), pp. 80–81.

[79]See §§ I.5-f and IV.2 AGB.

[80]Insurance has not been easy to define. Many attempts at pinpointing the essence of insurance have been made in the past, there being no consensus as to the minimum elements that should be present for a contract to be qualified as an insurance contract. In 1971, Wälder (1971), p. 23, very aptly remarked that prior attempts at defining the insurance contract already formed a 'legion'. We are not closer to a consensual definition now than we were back then. Dismissing the need for a definition, Clarke famously remarked: "The English courts know an elephant when they see one, so too a contract of insurance". See Clarke et al. (2006), p. 1-1. In any case, the payment of a premium seems to be a necessity: "a common denominator of usual definitions would say that insurance is a contract whereby, in return for a (variable or fixed) premium, one party, the insurer, promises the other party (the policyholder) to give coverage (by money payment or otherwise) under the conditions and within the limits stipulated in the contract, upon the happening of the (contractually defined) uncertain event". Cousy (2012), p. 408. This is all but new. According to Dreher (1991), p. 37, the payment of a premium is unanimously characterised in Germany as a necessary element of an insurance contract. In Italy, see Scalfi (1960), p. 813.

However, its motto makes it extremely clear that the company wishes to cater for the exact same demands and needs as regular insurers do but using a different contractual vehicle: it reads 'Not insurance. A lot better'.[81]

From a regulatory point of view, this model raises one's eyebrows, as it is based on the questionable assumption that it falls outside existing financial markets regulation. It is somewhat contradictory that this model presents itself as a return to the origins of insurance whilst at the same time claiming to be something other than insurance. What is on offer might differ from an insurance contract in the traditional sense. Nonetheless, regardless of whether the self-governing model actually distributes insurance, its products are manifestly designed to meet market demand for insurance products: the economic needs they fulfil appear to be exactly the same.

Take Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution, known as the Insurance Distribution Directive ('IDD'). Unlike its predecessor, the IDD applies to all distribution channels: it applies to any natural or legal person who either is or wishes to be established in a Member State so as to take up and pursue the distribution of insurance and reinsurance products, including insurance undertakings selling their own products directly, as well as a variety of insurance intermediaries: insurance agents and brokers, bancassurance operators, ancillary insurance intermediaries such as travel agents and car rental companies, and even product comparison websites.[82]

'Insurance distribution' in this context means 'the activities of advising on, proposing, or carrying out other work preparatory to the conclusion of contracts of insurance, of concluding such contracts, or of assisting in the administration and performance of such contracts, in particular in the event of a claim, including the provision of information concerning one or more insurance contracts in accordance with criteria selected by customers through a website or other media and the compilation of an insurance product ranking list, including price and product comparison, or a discount on the price of an insurance contract, when the customer is able to directly or indirectly conclude an insurance contract using a website or other media'.[83]

The IDD neither put forward any definition of insurance, nor does it provide any clues as to which contracts should qualify as insurance contracts under the IDD. However, the IDD aims to level the playing field between all types of insurance distributors to ensure that consumers benefit from the same level of protection throughout the marketplace, regardless of their chosen distribution channel.[84] If

[81]The following are statements made on its website: "Do you have a license to operate in my country/state? No, *Teambrella* is not a 'business of insurance': There are neither contracts nor obligations between insurer and insured in *Teambrella*. *Teambrella* doesn't underwrite policies. *Teambrella* doesn't keep clients' funds; there are no money pools. *Teambrella* doesn't make any payments to its clients".

[82]See Recitals 8, 11, 12 and 16 and Articles 1(2) and 2(1)(1) and (2) of the IDD.

[83]Article 2(1)(1) of the IDD.

[84]See Recitals 6, 10 and 16 of the IDD.

ensuring fair competition between all types of distributors is high in the list of this directive's priorities, we believe that a lesson should be drawn from competition law's vast body of knowledge on the definition of relevant product market: "[a] relevant product market comprises all those products and/or services which are regarded as interchangeable or substitutable by the consumer, by reason of the products' characteristics, their prices and their intended use".[85]

The IDD, as any related legislative initiative, would fail miserably, were it to allow economic agents that cater for basic insurance needs to escape insurance regulation. However, this model's postulation that it can wholly escape insurance regulation is even more perplexing when one realises that it is not all that different from earlier forms of insurance-related enterprises such as mutual insurers[86] or, perhaps even more closely, it is submitted, reciprocal insurance exchanges.

> Mutuality has its origins in collective self-help: people doing things for themselves, their families and their communities because there is no one else to do it for them. Cooperatives were set up because there was a market failure in the availability of basic food and provisions (...). Friendly societies and mutual insurance were established when there was no access to support in times of personal misfortune (...) because there were no financial services available to them.[87]

As these authors so aptly put it, "[s]elf-help emerges; you cannot do it to people".[88] Self-insurance has been around for a few thousand years, in one form or another, starting from the *foenus nauticum* and evolving over the centuries into more organised mechanisms.[89] The digital era has provided the much needed technical means for everyone to expand their self-help on a global scale, but just as the people's needs have not experienced any dramatic change: they are still essentially the same insurance needs, the structures that the people resort to so as to meet them on their own are remarkably similar to pre-existing self-help models but in a different environment and on a much larger scale.

In the fifteenth century, when the Portuguese scholar Pedro of Santarém wrote the first ever insurance treatise, self-help insurance models were still seen as the norm, insurance contracts as we know them being a relative newcomer whose validity Santarém felt he had to assert against a backdrop of usury accusations:

> In truth, provident merchants do very often, after taking thought about dangers at sea, protect their things against the cruelty of fortune with the shield of assurance, and defend them by entering into agreement with others against cases of adverse fortune (...). About this agreement of assurance, it is usual for great dissensions among merchants to arise and grow. For this reason, we must first see whether the agreement whereby one person, having

[85] See Commission Notice on the definition of relevant market for Community competition law [Official Journal C 372 of 09.12.1997].

[86] See Turcotte (2017), p. 156; Scardovi (2017), pp. 170, 174; Swiss Re (2016); Marin (2016); Carballa Smichowski (2015), p. 68.

[87] Morrison and Mills (2016), p. 302. Specifically on mutual insurers, see Talonen (2016).

[88] Morrison and Mills (2016), p. 302.

[89] See Holly and Greszta (2016), pp. 53–66.

> agreed with another on the price of a risk, takes upon himself that other's misfortune, is licit in the manner in which it is normally practised.[90]

Reciprocal insurance exchanges differ from mutual insurers in that they are an unincorporated association of subscribing members who enter into indemnity agreements with one another so as reciprocally individually to cover each other's risks.[91] The absence of a separate legal personality and individual nature of the underlying agreements bring them closer to the new digital P2P models.

In the United States, reciprocals have been around at least since the 1880s in the liability and fire insurance lines of business. In this business model, the subscribers individually co-insure each other. The main purpose of such schemes appears to be to obtain insurance coverage at a lower cost.[92] The business is run by a manager with the powers to represent all subscribers in the execution of indemnity agreements and in claims handling. Subscribers initially hand over to the manager a sum which is not unlike an insurance premium but which at least in some if not all such schemes it does not qualify as an insurance premium because the manager holds that sum in trust, registering it in separate individual accounts in the name of each subscriber.[93] That money will pay for the scheme's expenses and for any loss sustained by each subscriber as needed.

In these schemes, when at the end of an insurance period there is surplus, usually that surplus is retained until the stipulated solvency margin is reached, the credit balance in excess thereof being returned each year in cash to the subscriber. When excess losses occur, existing solutions differ as to the limits of the subscriber's liability: in some initial schemes the subscribers' liability was unlimited, but that feature appears to be a thing of the past; subscriber liability is typically limited, sometimes to the amount initially paid, but usually to a fixed limit corresponding to a multiple of the initial sum. Herein lies an important feature of reciprocals: subscriber liability is typically separate and several, rather than joint and several.[94] Some schemes insure excess losses in the traditional way, an insurance contract being collectively entered into which in essence has the contents of an excess of loss reinsurance treaty.

> The reciprocal, compared to all other forms of insurance organizations, has four unique attributes: the separate and several liability of the subscriber, the individual ownership of the

[90] Santarém (1552), First Part, Paragraphs 1–2.

[91] On these schemes, see Fitzgerald (1920), pp. 92–103; Norgaard (1964), pp. 51–61; Reinmuth (1964), pp. 641–646.

[92] See, for instance, Fitzgerald (1920), p. 92. However, in the past empirical studies have examined the relative efficiency of stock versus mutual and reciprocal ownership structures, generally concluding that mutuals and reciprocals are less efficient than stock insurers. See Mayers and Smith (1988), pp. 352–353 (and references included in notes 6–9 thereof).

[93] Fitzgerald (1920), p. 95.

[94] See Norgaard (1964), p. 57. As Norgaard puts it, "Reciprocal, a dictionary states, 'implies a return in due measure by each of two sides. . .', whereas mutual '. . . stresses a sharing equally and jointly rather than a return'" (p. 53).

> surplus, the exchange of contracts, and the subscriber. In addition to these four, one other attribute, the attorney-in-fact, is common to all reciprocals.[95]

In other words: this is exactly what the InsurTech P2P business models appear to be doing, minus the Tech.

6 Conclusions

We do not dispute the disrupting potential of InsurTech's new P2P business models: the broker model, the carrier model and the self-governing model. From an industry point of view, they may well provide a very significant contribution to the revolution of insurance as we know it.[96] However, from an insurance law perspective, our main conclusion is that for the most part the new business models are simply recycling and optimising the potential of some old recipes by applying them in a new, digital setting that enables them at least potentially to reach out to the global stage, thus creating a global self-help community of sorts.

This is not to say that the new, digital setting will not bring about new challenges. Out-of-scope from our analysis were many of InsurTech's innovations. The focus of our analysis was on the new P2P business models. As to such business models, our conclusion is that the most relevant challenges do not appear to be insurance-specific. An example at hand would be that of data protection, which in the digital era is as vital in the insurance sector as in many other economic sectors.[97]

Hence, our earlier contention that, having begun our quest in search of the new challenges to the law of insurance brought about by such business models, we ended up face to face with new takes on some of the oldest forms of insurance known to humanity. In our view, the traditional scheme that most resembles the new P2P business models is that of reciprocal insurance exchanges. This provided an excellent opportunity for a look back into the origins of insurance. In its earliest forms, insurance was born out of self-help. The small scale of traditional self-help mechanisms proved too parochial to cater for the more sophisticated insurance needs and so various types of professional insurers arose and flourished. Finally, the digital revolution gave rise to a global self-help community thereby providing the earlier self-help mechanisms with a new stage where they can compete with stock-based insurers on an equal footing.

This being the case, the law of insurance's main challenges appear to be, firstly, that of ensuring that the new business models fall within, rather than without current and future insurance regulation and, secondly, that of adapting itself to the global nature of the new tech-based global self-help mechanisms.

---

[95] Norgaard (1964), p. 56.

[96] On InsurTech's potential for exponential disruption, see Naylor (2017), pp. 1–40.

[97] See Naylor (2017), pp. 272–274.

Insurance regulation would fail miserably, were it to allow economic agents that cater for basic insurance needs to escape it. If one accepts that the new business models must fall within insurance regulation, then such regulation must be brought up to speed with the new tech-based means of providing insurance. Namely, insurance regulation must get over the paradigm of the traditional insurer who is the sole designer of its ready-made mass products and embrace the notion that insurance customers will be increasingly called upon to play an active role in putting together their own tailormade insurance products, with the assistance of and by means of new tech-based instruments. Protection of such active customers must come in new forms, as the sharing of designer roles between the insurer and its customers should not entail the diffusion of the underlying responsibility—and potential liability—for the resulting insurance products.

References

Belk R (2014) Sharing versus pseudo-sharing in Web 2.0. Anthropologist 18:7–23

Cappiello A (2018) Technology and the insurance industry. Palgrave Pivot

Carballa Smichowski B (2015) Mutualisme et Économie Collaborative: Master Thesis. MAIF/Université Paris XIII

Carvalho JM (2018) Manual de Direito do Consumo, 5th edn. Almedina

Clarke MA (2005) Policies and perceptions of insurance law in the twenty-first century. Oxford University Press

Clarke MA, Burling JM, Purves RL (2006) The law of insurance contracts, 5th edn. Informa Law

Codagnone C, Martens B (2016) Scoping the sharing economy: origins, definitions, impact and regulatory issues. Digital Economy Working Paper 2016/01, Institute for Prospective Tecnhological Studies, European Commision. https://ec.europa.eu/jrc/sites/jrcsh/files/JRC100369.pdf

Cousy H (2012) Insurance law. In: Smits JM (ed) Elgar encyclopedia of comparative law, 2nd edn. Elgar, p 48 ff

Dreher M (1991) Die Versicherung als Rechtsprodukt. Die Privatversicherung und ihre rechtliche Gestaltung. Mohr Siebeck

EIOPA (2017) EIOPA InsurTech Roundtable. How technology and data are reshaping the insurance landscape. Summary from the roundtable organized by EIOPA on 28 April 2017 (EIOPA-BoS/17-165, 05 July 2017). https://eiopa.europa.eu/Publications/Reports/08.0_EIOPA-BoS17-165_EIOPA_InsurTech_Roundtable_summary.pdf

Ernst & Young (2012) Voice of the customer - time for insurers to rethink their relationships. Ernst & Young Report

Fitzgerald JA (1920) Reciprocal or inter-insurance against loss by fire. Am Econ Rev 10:92–103

Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V (2018) Blockchain and smart contracts for insurance: is the technology mature enough? Future Internet 10(2):20 ff

Holly R, Greszta E (2016) Self-insurance as a formula for risk management – a new perspective. Wiadomości Ubezpieczeniowe 4:53–66

Huckstep R (2015) Guevara, moral hazard and the future of P2P insurance. https://dailyfintech.com/2015/12/24/guevara-moral-hazard-and-the-future-of-p2p-insurance/

John NA (2013) Sharing and Web 2.0: the emergence of a keyword. New Media Soc 15 (2):167–182

Lougher G, Kalmanowicz S (2016) EU competition law in the sharing economy. J Eur Compet Law Pract 7(2):87–102

Marano P (2019) Navigating InsurTech. The digital intermediaries of insurance products and customer protection in the EU. Maastricht J Eur Comp Law 26(2):294–315. https://doi.org/10.1177/1023263X19830345
Marin ER (2016) Economia Compartilhada e o Mercado Segurador. Cadernos de Seguros 188:36–43
Mayers D, Smith CW Jr (1988) Ownership structure across lines of property-casualty insurance. J Law Econ 31:351–378
Morrison M, Mills C (2016) Expanding the role of cooperative and mutual enterprises in delivering public services: disrupting the status quo. In: Butcher J, Gilchrist D (eds) The three sector solutions: delivering public policy in collaboration with not-for-profits and business. Australian National University Press, pp 301–317
National Association of Insurance Commissioners (2018) Peer-to-peer Insurance. http://www.naic.org/cipr_topics/topic_p2p_insurance.htm
Naylor M (2017) Insurance transformed. Palgrave Macmillan
Norgaard RL (1964) What is a reciprocal? J Risk Insur 31:51–61
Orlovácz P (2016) The insurance opportunity. In: Barberis SCJ (ed) The Fintech Book. Wiley, pp 721–730
Paisant G (2015) Défense et Illustration du Droit de la Consommation. LexisNexis
Paperno A, Kravchuk V, Porubaev E (2016) Teambrella: a peer to peer insurance system (Whitepaper). https://teambrella.com/WhitePaper.pdf
Reinmuth DF (1964) What is a reciprocal? Comment. J Risk Insur 31:641–646
Sagalow TR (2016) Peer-to-peer insurance. Presented at the Insurance and Technology Event organized by the Center for Insurance Policy and Research in New Orleans, Louisiana, on 5 April 2016. http://www.naic.org/documents/cipr_events_spring_2016_p2p.pdf?51
Santarém P (1552) Tractatus de Assecurationibus et Sponsionibus. Originally written in 1488 and first published in 1552, translated into Portuguese, English and French by Instituto de Seguros de Portugal in 2007
Scalfi G (1960) Corrispettività e Alea nei Contratti. Milan
Scardovi C (2017) Digital transformation in financial services. Springer
Smorto G (2015) Verso la Disciplina Giuridica della Sharing Economy. Mercato Concorrenza Regole 2:245–278
Soberón BP (2016) Las Insurtechs Dedicadas a los Seguros Colaborativos Permiten al Consumidor Obtener Descuentos en su Póliza. Revista CESCO de Derecho de Consumo 19:52–55
Sundararajan A (2016) The sharing economy. The MIT Press
Swiss Re (2016) Mutual insurance in the 21st century: back to the future? 4/2016, Sigma
Talonen A (2016) Systematic literature review of research on mutual insurance companies. J Co-oper Organ Manage 4(2):53–65
Turcotte M (2017) L'Assurance sans Assureur ou le P2P. Assurances et Gestion des Risques/Insur Risk Manage 84(1–2):77–87
Wälder J (1971) Über das Wesen der Versicherung. Ein methodologischer Beitrag zur Diskussion um den Versicherungsbegriff. Duncker & Humblot
Wilson JD Jr (2017) Creating strategic value through financial technology. Wiley
Yan TC, Schulte P, Chuen DLK (2017) InsurTech and FinTech: banking and insurance enablement. In: Chuen DLK, Deng R (eds) Handbook of blockchain, digital finance, and inclusion. Elsevier, pp 249–281
Zwack T (2017) Peer-to-Peer-Geschäftsmodelle zur Absicherung privater Risiken. Springer

The Internet of Things and Insurance

Alkistis Christofilou and Viktoria Chatzara

1 Introduction: The "Internet of Things" Phenomenon

1.1 What Is the Internet of Things?

The Internet of Things ("IoT") has been defined in several ways, without there being a globally agreed definition for it.[1] It has been broadly described by the OECD as *"an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world."*[2] Alternatively,[3] "*IoT is a wide-ranging ecosystem of physical objects connected to the Internet, capable of identifying themselves and communicating data to other objects with the help of a communication network for digital processing*."

The authors thank Lydia Polyzou for her valuable contribution to this chapter.

[1]See a compilation of definitions by Rod Freeman–Cooley, and Brigitte Acoca in OECD's recent publication "Product Safety in the Internet of Things", OECD Secretariat, OECD Digital Economy Papers, March 2018 No. 267, available at: https://www.oecd-ilibrary.org/deliver/7c45fa66-en.pdf?itemId=%2Fcontent%2Fpaper%2F7c45fa66-en&mimeType=pdf.

[2]OECD (2016), "The Internet of Things: Seizing the Benefits and Addressing the Challenges", *OECD Digital Economy Papers*, No. 252, OECD Publishing, Paris, https://doi.org/10.1787/5jlwvzz8td0n-en.

[3]EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication Building a European data economy {COM(2017) 9 final} 10.1.2017, p. 41, available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy.

A. Christofilou (✉) · V. Chatzara
Rokas Law Firm, Athens, Greece
e-mail: a.christofilou@rokas.com

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_3

The IoT European Research Cluster (IERC/ITU) goes further to define IoT as "*[A] dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols, where physical and virtual "things" have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*"[4]

The IoT includes devices and objects, whose state can be altered via the Internet, with or without the active involvement of individuals. This includes laptops, routers, servers, tablets and smartphones, often considered part of the "traditional Internet." However, these devices are integral to operating, reading and analysing the state of IoT devices and frequently constitute the "heart and brains" of the system. Thus, it would not be correct to exclude them.[5]

Whatever the precise definition, unequivocally, the IoT represents the next major economic and societal innovation wave enabled by the Internet. With the IoT, any physical (e.g. a thermostat or a bike helmet) and virtual object (i.e. a representation of real object in a computer system) can be connected to other objects and to the Internet, creating a fabric between things, as well as between humans and things. The IoT can combine the physical and the virtual worlds into a new smart environment, which senses, analyses and adapts, and which can make our lives easier, safer, more efficient and more user-friendly.[6] The IoT inaugurates a new age of ubiquitous connectivity and intelligence, in which **components, products, services and platforms** connect, virtualise and integrate everything in a communication network for digital processing.

Its exponentially expanding applications can be divided into consumer, commercial, industrial and infrastructure ones. The IoT should be understood as an ecosystem where areas that have been developed as vertical silos (manufacturing, transport, healthcare, devices etc.) can relate to each other, owing to common platforms and innovation across areas. IoT ecosystems are, therefore, based on bringing together multiple sectors and stakeholders to cover an increasingly complex value chain.

As will be analysed below, most of these applications are of direct interest to insurers, for having the ability to facilitate in many aspects the insurance operations and to grant a competitive advantage to insurers integrating them in their functions, and the foreseeable size of the IoT expansion renders their involvement an imminent necessity. By creating new risks, IoT broadens the market for insurance.

[4]Available at: http://www.internet-of-things-research.eu/about_iot.htm.

[5]OECD (2015), *OECD Digital Economy Outlook 2015*, OECD Publishing, Paris, available at: https://doi.org/10.1787/9789264232440-en.

[6]Commission Staff Working Document "Advancing the Internet of Things in Europe" {COM (2016) 180 final} 19.4.2016, p. 4, available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe.

1.2 Size Considerations

Between 2012 and the end of 2016, publicly available data showed that the number of actual Machine-to-Machine (M2M) SIM cards in use in tracked countries grew from 72 million to 149 million (OECD, 2017). Shodan, the search engine for Internet-connected devices, has established that in 2018 there were 363 million connected devices around the world, with approximately 84 million in the People's Republic of China, 78 million in the United States, 18 million in each of Korea, Brazil and Germany, and 8–10 million in each of Japan, Spain, the United Kingdom and Mexico. Furthermore, the International Data Corporation estimates that the market value of the IoT will reach USD 1.29 trillion in 2020. McKinsey estimates that in 2015, the size of the IoT market was USD 900 million but it will grow to USD 3.7 billion by 2020. This growth could generate a potential impact of USD 11.1 trillion a year in economic value by 2025 if policy makers and businesses overcome crucial technical, organisational and regulatory hurdles that impede it.[7] General Electric estimates that by 2025 this "industrial internet" will touch 43% of the global economy, spanning across the engines of global economic growth: energy, healthcare, transportation and manufacturing. The market for complementary technologies is also a useful metric for estimating the overall impact of the IoT. The Analysis Group estimates that, if augmented and virtual reality are fully adopted by 2020, this could affect the global economy by as much as USD 126 billion. Other analysts predict that the combined market will be USD 162 billion by 2020, with augmented reality accounting for most of the growth. Bank of America projects that the virtual reality industry alone could be valued at USD 150 billion, with more than 300 million users, by 2022.[8]

1.3 IoT Key Features and Components

IoT is currently evolving into a new stage - the "Internet of Everything". This refers to the seamless connection of devices, sensors, machines, objects, vehicles, rooms, etc, that interact through communication between machines (M2M), between people and machines (P2M) and between people (P2P) *"to deliver new or enhanced services, provide improved and broader contextual awareness, and allow for better informed and faster decisions"*.[9]

[7] See Sect. 1.4 of this chapter.

[8] Source: Consumer Product Safety in the Internet of Things, OECD Digital Economy Papers, March 2018 No. 267, p. 14, with numerous references to sources.

[9] See Thomas Hoppner/Anastasia Gubanova, Regulatory challenges of the internet of things, Computer and Telecommunications Law Review (C.T.L.R.), 2015, referring to Europol, "The Internet Organized Crime Threat Assessment (iOCTA)" (2014), p. 61, available at: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta.

As eloquently expressed,[10] *"[T]here will be so many IP addresses, [. . .] so many devices, sensors, things that you are wearing, things that you are interacting with, that you won't even sense it. [. . .] It will be part of your presence all the time. Imagine you walk into a room and the room is dynamic [and] you are interacting with the things going on in the room."*

The IoT is currently probably the largest driver of technological innovations. Connected sensors collect data from objects (e.g. a car, a phone etc.), which are analysed either through embedded systems or through cloud-based and Internet systems enabling the creation of new services and big data analytics. Wearables, equipment parts in business, and smart city environments are examples of solutions put forward in this sense. Innovation is data and product driven. The data provided by connected sensors and objects allows single and networked objects to perform specific functions derived from sensing, analysis and intelligence gathered, as for example in factory automation, logistics and robotics. Through the application of complex systems, sensors and smart connected objects become part of a bigger connectivity network that creates new opportunities to combine more intelligence and actuation across vertical markets, to provide a whole new set of services and to coordinate smart objects in their original or other functions. Technical and semantic interoperability are key factors for success, so that these systems deliver complete IoT solutions, e.g. at home, in cities, between industries. Connected objects of all sorts may then self-improve and become autonomous, using artificial intelligence (AI) to learn.

Thus, the key features of the IoT comprise not only the **object** itself and the **sensors** on it, but also the **software** that programmes its interplay with other sensors, as well as **interconnectivity**, comprising **interoperability** and the telecommunication **networks** combining it with the exterior world, while the huge amount of **data** generated in this process is also of paramount importance.

1.4 Technology and Other Challenges to IoT Penetration

Considering the global nature of the IoT system, a number of challenges could impede its advancement, and these can be both technological and regulatory.

In terms of M2M connectivity, there is **no universal or pan-European standardisation**. Equally, access to such varying standards is not available through free licensing of the respective intellectual property rights. The system is currently operating based on self-regulated standards. In its efforts to foster technology integration and validation of business models and standards on an EU-scale and the IoT potential for expansion, the European Commission will invest more than 100 M€ in demand-driven large scale IoT pilots in areas such as smart living

[10]By Eric Schmidt, then Executive Chairperson of Google Inc., in the World Economic Forum in Davos, January 2015.

environments for ageing well, driverless cars, wearables, smart city, agro-food and manufacturing.[11]

Devices can be connected through a fixed telecommunications line using protocols like Ethernet, or through a variety of wireless protocols. In this, **spectrum availability and network coverage** need to be secured. There are no global harmonisations for the use of spectrum as of yet. The EU Commission recently issued a Decision aiming at harmonising the allocation of the 900 and 1800 MHz frequency bands for services of the Internet of Things.[12]

Another potential obstacle can ensue from **numbering regulation**. For example, certain connected items such as smart cars, carry embedded telecommunication systems bearing SIM cards with numbers assigned from the national numbering system of their country of origin. Once exported and circulating in other countries, they will be in a permanent roaming status, which as a general rule and even within a number of EU Member States, is not an acceptable mode of operation. The current numbering schemes seem to be too limited to support the wide range of future M2M applications and should be further developed.[13]

Governments wishing to boost technological advance seek to resolve these impediments by promoting regulation and financial or operating initiatives, and so does the European Union, the USA, as well as Singapore and Hong Kong.

1.5 Data: A Particular Challenge

IoT devices collect and exchange data, including **personal data**, automatically, and often without the data subjects being aware of it. The active growth of global data, measured in zetabytes, developed from 1.2 ZB in 2010 to 7.9 ZB in 2015 and is expected to reach 44 ZB in 2020.[14] This challenges the ethical values, the data protection imperative and the information security promoted by national and supranational data protection frameworks, such as the EU General Data Protection

[11]See Commission Staff Working Document SWD(2016)110 final "Advancing the Internet of Things in Europe" {COM(2016) 180 final} 19.4.2016, p. 17.

[12]See Commission Implementing Decision (EU) 2018/637 of 20 April 2018 amending Decision 2009/766/EC on the harmonisation of the 900 and 1800 MHz frequency bands for terrestrial systems capable of providing pan-European electronic communications services in the Community as regards relevant technical conditions for the Internet of Things, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.105.01.0027.01.ENG&toc=OJ%3AL%3A2018%3A105%3ATOC.

[13]See Commission Staff Working Document "Advancing the Internet of Things in Europe" {COM (2016) 180 final} 19.4.2016, p. 15.

[14]Fausto Parente, Executive Director of the European Insurance and Occupational Pensions Authority (EIOPA): *"Calibrating the Regulatory Approach on New Technologies"*, 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", 12 April 2018 Warsaw, Poland, available at: http://www.aida.org.uk/docs/2018-04-12%207thAIDAEuropeConferenceEIOPAsInsurTechActivitiesFaustoParente.pdf.

Regulation (GDPR)[15] which is accompanied by a set of complementing directives and implementing rules. The GDPR does not permit profiling without the data subject's consent or another valid legal basis, e.g. a legitimate interest. However, such profiling may still take place in the data subject's ignorance in the case of smart devices. The billions of data produced via IoT operations are subject to the risks of hacking and misuse. Particularly, the high volume and low cost devices that have been produced during the last decade do not make provisions for safety and protection against data violation risks. It is a rather novel requirement, introduced by the GDPR, that devices are data-protection-designed ("privacy by design"). However, this does not guarantee adequate protection in massive operations.

Besides, hacking does not only pose the risk of breach of data confidentiality and violation of privacy, but may also result in the intrusion into the systems and their operations in a damaging or even catastrophic manner.

In another context, the **sharing and re-use of non-personalised data in a commercial context** is crucial for the deployment of IoT. For example, there are developed markets for financial data,[16] marketplaces for commercial data,[17] and industrial market platforms that operate as virtual environments, facilitating the exchange and connection of data among different companies and organisations through a shared reference architecture, common governance rules and within a secure business ecosystem. Data trading is generally not regulated and relies on contract and on the platform rules. Data as such are protected in limited ways and in different manners in the various jurisdictions. In the EU, there is a complex set of regulations providing specific protection to data from a number of angles.[18]

Sector-specific legislation regulates the access to privately-held, non-personal or anonymised data in certain contexts, e.g. the access to in-vehicle data for opening up the market for after-sales services (maintenance and repair).[19] Such data does not have to be provided for free, but is subject to a regulated

[15]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, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1539081472490&uri=CELEX:32016R0679.

[16]According to the (EU) Commission Staff Working Document SWD(2017) 2 final of 10.01.2017 on the free flow of data and emerging issues of the European data economy, accompanying the Communication Building a European data economy {COM(2017) 9 final}, the market for financial markets data is expected to reach € 5.94bn by 2018 (p. 13).

[17]Such as the DAWEX platform, Commission Staff Working Document as immediately above, p. 17.

[18]E.g. the GDPR on protection of personal data and the e-Privacy Directive 2002/58/EC regarding electronic communications, the Database Directive 96/9/EC, which does not as such apply to machine-generated data, the Trade Secrets Protection Directive (2016/943), as well as unfair competition laws.

[19]Regulation (EC) No 715/2007 as amended. The European Parliament only recently accepted new EU legislation on the free flow of non-personal data, referred to as "EU's fifth freedom"; the new Regulation is due to be approved by the EU Council of Ministers on 6 November 2018—see in this

regime. Similarly, the EU Payment Services Directive 2[20] opens up access to "payment information" under certain conditions, and thus acts as an enabler for FinTech companies.[21] The necessity of access to non-personal data can be visible in the case of the energy grid operators, who need smart grid real-time information to balance the energy supply and demand. The EU Internal Electricity Market Directive[22] aims, among others, at improving such access.

As a general rule, there is no comprehensive legislative framework on what rights can be exercised and on which conditions, with respect to processing and access to non-personal or anonymised data, in particular with respect to data created by computer processes or collected by sensors processing information from equipment, machines or software. In the EU, the European Commission, having identified the importance of such regulation for the facilitation of the digital economy, is exploring the need to introduce a relevant regulatory instrument.

1.6 IoT and Insurance

The emergence of IoT and, in general, the rapid technological developments, are heavily affecting the insurance industry. According to available information,[23] the financial sector is one of the most disrupted sectors in the global economy. Technological change and over-regulation are considered the two most disruptive factors. Insurtech[24] and, particularly, the IoT applications which are designed with the aim to be used in the insurance industry, are affecting and are expected to progressively

---

relevance: http://www.europarl.europa.eu/news/el/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom.

[20]Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366.

[21]See detailed presentation and other valuable relevant information in Commission Staff Working Document SWD(2017) 2 final of 10.01.2017, *ibid*.

[22]Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1539082041756&uri=CELEX:32009L0072.

[23]See in this relevance information included in the Key Note speech *"Addressing International Change: The Agenda of the Global Insurance CEO"* of Stephen T. O'Hearn, Leader of the PwC Global Insurance Practice, at 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", Warsaw, 12 April 2018, available at: http://www.aida.org.uk/docs/Agenda%20of%20The%20CEO%20March%202018_Warsaw.pdf.

[24]*Insurtech* as a section of Fintech refers to the use of technology innovations designed to squeeze out savings and efficiency from the current insurance industry model. The belief driving InsurTech companies is that the insurance industry is ripe for innovation and disruption. InsurTech is exploring avenues that large insurance firms have less incentive to exploit, such as offering ultra-customised policies, social insurance, and using new streams of data from internet-enabled devices

more and more affect all aspects of an insurer's operations, from product design and development to pricing and underwriting, and from sales and distribution to post-sales services and claims management.[25]

With respect to internal operations, IoT is seen by insurance executives as an opportunity to cut down on costs, and as a tool for the creation of more personalised insurance products, more effective risk assessment, premium pricing, claims management and claims prevention. Access to technology is gained either by purchasing the technology, of by acquiring the technology company itself. The vividly discussed entry of internet platforms and technology giants into the insurance game is another expression of the market transformation.

Technology advancements have a further important use: they are expected to assist insurers to deliver on their demanding regulatory compliance requirements, as the new notion of RegTech implies.

2 IoT-Driven Evolution of the Insurance Value Chain

2.1 General Remarks

This Section discusses certain parameters of the IoT impact on the insurance value chain, namely how IoT influences the insurance undertaking's relation with the customer, its approach of risk, its claims management function, and certain liability issues. While the use of innovative technological solutions by incumbents is usually seen as an opportunity to strengthen their relations with their customers and, in general, as beneficial to the insurance business, it may also have downfalls and may present challenges that need to be addressed by insurers.

2.2 Product Design

More Data Means More Targeted Products IoT applications and the massive amounts of (customers') data produced by them and transmitted to insurers shall enable the latter to better understand the identity of their clients and their needs and demands at a more granular level, thus altering the product design function. In this sense, the continuous IoT data analysis is expected to result into more segmented customer target groups,[26] more individualised insurance products and covers, or new

to dynamically price premiums according to observed behaviour. https://www.investopedia.com/terms/i/insurtech.asp#ixzz5SavxNHkW.

[25]See more detail in Fausto Parente, op. cit.

[26]Ernst&Young, "The Internet of Things in insurance: Shaping the right strategy, managing the biggest risks", © 2016, available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&

product-service bundles (such as home insurance along with home monitoring technology[27]), and generally, more personalised, targeted and frequent insurer–customer interactions, albeit not necessarily in person.

IoT Impact on Product Oversight and Governance (POG) The above effects of IoT applications may assist insurers in their compliance with the relevant Insurance Distribution Directive (IDD)[28] requirements, which require insurance undertakings, when designing their products, to adopt and maintain a process of approval,[29] aiming to ensure that insurance products are designed to meet specific insurance needs, and that they are marketed only to the customers having these needs. The development and integration of appropriate IoT tools into the product approval and product monitoring procedures shall grant insurers access to more data, necessary for their efficient implementation. IoT solutions may provide the insurance undertaking with continuous information on the evolution of the customer's needs, preferences, habits, etc., thus enabling the insurer to assess whether its products need to be amended.

Rise of On-Demand and Usage-Based Insurance: Risks and Challenges IoT use is anticipated to also increase the request for on-demand insurance, which nowadays represents only 1% of the global insurance market.[30] Also for usage-based insurance (UBI), which is already known in motor vehicle insurance covers[31] and in insurance for personal belongings. A number of customers value the flexibility of such

---

source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwiRxa7m_uTdAhUrqIsKHWhyCAYQFjABegQICBAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2FEY_-_The_internet_of_things_in_insurance%2F%24FILE%2FEY-the-internet-of-things-in-insurance.pdf&usg=AOvVaw1goOD-Xd5_fmZyY34wqakR.

[27]Offering such product-service bundles would also affect other stages in the insurance value chain, as the bundles would be used as a means to reduce the likelihood for the insured risk to occur and lower the overall risk for policyholders and insurers – see in this relevance Isabel Harner, Director of Marketing @ IoT for All, Leverage, *How will IoT transform the insurance industry?*, January 22, 2018, available at: https://medium.com/iotforall/how-will-iot-transform-the-insurance-industry-609f89a12bf1.

[28]Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1539082539478&uri=CELEX:32016L0097 (IDD).

[29]Article 23 of IDD on product oversight and governance requirements (POG) is of relevance, as well as the more detailed provisions of the Commission Delegated Regulation (EU) 2016/2358 of 21 September 2017 supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32017R2358.

[30]Paul Merrey and Artur Kokins (2017), *Will on-demand insurance become mainstream?* available at: https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2017/09/will-on-demand-insurance-become-mainstream.pdf.

[31]Currently, nine of the top 10 insurers are offering UBI motor vehicle insurance commercially or in various stages of pilot, where customers purchase insurance only for the time they use their vehicles or for the miles they have driven, according to in-vehicle sensors.

insurance products and the fact that the premium only corresponds to the cover they absolutely need. Insurance covers for small risks and minimal duration are also emerging on the markets, like small "service gadgets" handy to the policyholders. However, given that the premiums for on-demand insurance/UBI are expected to be higher than the premiums for the same risk to be covered on a regular basis, these may be restricted to a niche target market and, thus, not become the prevalent type of insurance products. In the same relevance, not all insurers would be inclined to adopt such insurance solutions, considering that customers would be able to activate and de-activate insurance upon request to pay the minimum premium possible, close to the time of risk occurrence, thus increasing the risk of fraudulent claims. Furthermore, the development of on-demand insurance products/UBI could risk harming the insurer–customer relationship if customers hesitate to provide the necessary information, fearing that they would reveal aspects of their risk profiles that would render them uninsurable.

2.3 Sales and Distribution

IoT May Alter the Traditional Insurance Distribution Model IoT applications can result in more direct and more frequent access of insurers to customers and to the relevant raw data, which can be further used for direct sales of insurance, through various channels. Customers are now able, through traditional electronic communications means such as e-mails, or via more sophisticated tools such as chat boxes or *"help-me"* functions on websites, or even via their smartphones and social media applications, to establish a direct contact and dialogue with their insurers, ask for more information on their policies or, more generally, on the products offered by the insurer, and provide data to the insurer that are necessary for the preparation of a specific product that will be offered and priced. This direct access and sales, although not new and already regulated under IDD, is a significant novelty, particularly for insurers that used to rely on networks of insurance intermediaries for the promotion of their products, where the insurance intermediaries were the only personal contact of the customers, entrusted with their insurance needs and demands.[32] It remains to be seen if and to what extent traditional insurance mediation networks will become obsolete and how they will have to amend and adapt their operations, to catch-up with the change. In this relevance, and in the context of their IDD obligations,[33] insurers will have to choose and review their cooperations to ensure that their distributors have the ability to duly and effectively collect, process and report accurate and useful data, as well as to work with the IoT tools implemented by the insurers in their operations.

[32]Ernst&Young, *The Internet of Things in insurance: Shaping the right strategy, managing the biggest risks*, op. cit.

[33]See Article 8 of the Commission Delegated Regulation (EU) 2017/2358.

Regulatory Aspects and IoT Distribution Strategy In the EEA, the IDD and the Commission Delegated Regulation (EU) 2017/2358 provisions on POG requirements foresee that insurance distributors (i.e. insurance undertakings included) must adopt and implement a product distribution strategy, which shall be compatible with the needs and demands of each identified target market.[34] Consequently, for an insurer to be able to employ IoT communication tools to market its insurance products directly to the target customers, it must be able to show that the use of such tools is consistent with the characteristics of the specific target market. The same tools may not be used horizontally for the distribution of any insurance product to all target groups. Insurers shall be facing increased costs of investment in IoT solutions, to ensure that the POG requirements are met for the identified target markets, while the tools employed shall be regularly revisited and amended when necessary.

IoT Solutions May Facilitate the Provision of Obligatory Precontractual Information Across the legislative framework, a number of provisions regulate the information to be made available to customers at the pre-contractual stage. Depending on the type of insurance being offered, information shall be provided to ensure an informed choice of the insurance product. There is more information required by other laws.[35] Thus, potential customers are being overwhelmed by a bulk of pre-contractual information and documentation, while the aim of a really "informed choice" is highly unlikely to be achieved. IoT solutions can, however, assist insurers not only to comply with their increasing information obligations, but also to provide the necessary information in an understandable, user-friendly way, and further enhance the insurer–customer relation and the trust between the parties, with the use of the available technological advancements (such as pop-ups, layered information, icons, etc.). Nevertheless, insurers must be able to prove that the use of such tools is appropriate in the context of their relationship with the customer, or the customer must ask/consent to the electronic provision of such information, as in many jurisdictions the applicable insurance regulation still requires that the pre-contractual information is provided in paper form.

2.4 Underwriting and Pricing

Underwriting and pricing may be the part of the insurance value-chain most heavily affected by the penetration of IoT applications. The relevant departments and functions must become quickly acquainted with the new reality and develop new methods of risk evaluation and premium pricing, considering the massive amount of customer data that is becoming available to them.

[34] See Article 10 of the Commission Delegated Regulation (EU) 2017/2358.

[35] Such as the GDPR.

IoT May Result in Better Pricing and in More Ample Insurable Groups The quantity and precision of the customer related information becoming available to insurers with the use of IoT tools will enable their operations departments to more accurately evaluate the insured risks in the case of each customer, propose a fairer premium that is more adequately balanced to the risk and profit margin, and all this more quickly than with the traditional risk evaluation methods. It may also be that cover may become available for previously non-eligible customers or even non-insurable target groups,[36] owing to their high-risk profile, as the risk components may be granulated to finer chunks and their evolution more predictable. For example, customers with chronic diseases, such as diabetes, who were either not accepted by health insurers or obliged to pay significantly higher premiums, may benefit from the use of IoT tools, showing that they meet certain activity or behavioural goals and so increase their insurability.[37]

IoT Effects on Regulatory Obligations Connected with Risk Evaluation and Pricing From a regulatory point of view, the impact of IoT applications upon the pre-contractual obligations of potential customers and respective rights of the insurers remains to be seen. Although the relevant legal issues may vary from one national jurisdiction to another, it would be interesting to pose some questions on the example of the Greek Insurance Contract Act (ICA, Law 2496/1997). Under the Greek ICA[38], before the conclusion of the insurance contract the policyholder has a duty to disclose to the insurer any and all information or circumstances that are objectively material for the risk assessment process, of which he is aware, and to answer any relevant question of the insurer. If the insurer has relied upon written answers, under the ICA it should be presumed that the information and circumstances to which the written questions related constitute the sole ground, upon which the insurer has based its risk assessment. If, for any reason beyond the control of the policyholder or the insurer, any objectively material information or circumstances have not been notified to the insurer, the latter has the right to terminate the insurance contract or ask, within one month from becoming aware of this fact, that the contract is amended.

If IoT applications are used at the pre-contractual stage for the risk assessment process, the practical implementation of the above provisions could be very limited. Would the insurer's access to customer data concerning his/her daily activities and habits, fully cover the customer's duty of disclosure? As the insurer will actually collect and choose which information to use, could this qualify as "written questions", in which case the insurer could not argue that the customer has not provided all the necessary information? If this were the case, the design of the IoT applications

[36]Julianne Callaway (2017), *The Internet of Things: Key considerations for Life Insurers – Five Questions with RGA's Julianne Callaway*, December 20, 2017 available at: https://www.rgare.com/knowledge-center/media/articles/the-internet-of-things-key-considerations-for-life-insurers.

[37]Isabel Harner, *How will IoT transform the Insurance Industry?*, op. cit.

[38]Namely the provisions of Article 3 thereof.

used would be crucial, as the insurer would have to ensure that all the objectively material information would be collected and processed. Furthermore, the insurer's right to terminate or amend the insurance contract could become irrelevant: should any information or circumstances not be collected and processed by the IoT tools applied and, thus, not calculated in the risk assessment, such omission would hardly qualify as a reason beyond the insurer's control.

IoT Means Continuous Risk Evaluation The use of IoT tools is not only destined for the precontractual stage, but shall rather create a continuous connection between the customer and the insurer, thus providing the latter with the possibility to monitor the customer's behaviour, as well as the evolution of the insured risks and their related circumstances. Insurers will be able to examine whether the circumstances following the conclusion of the insurance contract are in line with the conclusions drawn at the risk assessment and premium pricing stage, or if there is a need to re-evaluate the insured risk and re-calculate the premium. Such applications have already emerged, particularly in the motor insurance industry[39], while health insurance applications follow. Considering that such continuous monitoring and review may result in benefits for them, the vast majority of customers would be willing to provide personal data concerning their habits and lifestyle by means of IoT devices (such as sensors, wearable devices, etc.), if this would mean that they could benefit from a lower premium and better protection[40], let alone the additional benefit of being incentivised to follow better habits in their daily life. In this relevance, the issue of general policy terms that confer to the insurer the right to regularly re-calculate the premiums is of significance.

2.5 After-Sales Service and Claims Management

With respect to the insurer–customer relationship after the conclusion of the contract, IoT solutions can render claims notification almost automatic, and claims assessment procedures faster and more efficient, thus resulting in better after-sales services and more satisfied customers. Damage evaluations will become more accurate and fairer, and their results should be less likely questioned by insureds.

Risk Prevention Insurance business can transform into risk prevention operations, as IoT applications are being used by insurers as a means to reduce the likelihood of the risk occurrence: insurers are rewarding customers (e.g. by lowering premiums)

[39]One of the many examples in motor vehicle insurance industry is the TrueMotion company, which provides smartphone telematics to insurers, for them to identify the best drivers and, thus, price them more profitably. Smartphone applications such as accelerometers, gyroscopes, GPS and other sensors, may be used by insurers to provide insight on driving habits and result in more accurate pricing methods.

[40]Stephen T. O' Hearn, Key Note speech: *Addressing International Change: The Agenda of the Global Insurance CEO,* op. cit.

for a certain behaviour, whereas adverse effects may result for customers following adverse behavioural patterns. The corresponding downfalls would concern a good amount of privacy given up by customers, and the creation of new questions from a regulatory point of view.

The applications just described can be used to limit, to the extent possible, the occurrence of the insured risk and, thus, the need to compensate a relevant claim,[41] The monitoring of driving behaviour and the provision of discounts for safe driving habits could be also considered as a risk prevention program, and so would the use of embedded environmental sensors, which could detect hazardous weather conditions and dispatch automatic alerts to the in-car units of vehicles moving in the relevant area, thereby alerting drivers to be cautious and reduce the risk of accidents.

The use of connected devices and network of sensors is also expected to act as a risk-prevention mechanism in home insurance, as well as in insurance of industrial buildings. Such sensors are capable of detecting temperature, smoke, toxic fumes, earthquake motions and other dangerous conditions, and thus enable the detection of circumstances that may lead to risk occurrence and the implementation of appropriate preventive measures. It is expected that, in the future, said IoT sensors could communicate with other devices and issue automatic alerts where such hazardous conditions are detected.[42]

Risk Occurrence and Claims Notification IoT applications may similarly alter the way of risk occurrence notification and claims notification to the insurer. Vehicle embedded sensors are programmed to automatically connect with emergency centres in case of an accident and send the exact location of the vehicle, so that assistance may be dispatched,[43] while embedded diagnostics sensors can send accurate data on the damages incurred to the vehicle. The same technology could be used to forward automatic alerts to insurers in case of a road accident. Similarly, sensors installed in houses and industrial properties will be able to dispatch automatic alerts in case of fire, flood or other insured risk,[44] as well as information on the damages caused.

[41]John Hancock is one characteristic example, as it incentives customers to stay fit, thus reducing the likelihood of them filing a claim, by offering entertainment, shopping and travel rewards and discounts. See more details on its "Vitality Program" at: https://www.johnhancockinsurance.com/vitality-program.html?cid=US_JH_BR_IR_JohnHancock_Other_LifeInsurance_SV_CS_LK_00_BF_00_00_AW_00_20180925_LifeInsuranceWithVitality_HowItWorks-CTA.

[42]Robert Reiss, *5 Ways the IoT will transform the insurance industry*, February 1, 2016, available at: https://www.forbes.com/sites/robertreiss/2016/02/01/5-ways-the-iot-will-transform-the-insurance-industry/#47b1782e66d0.

[43]The integration of such embedded sensors and the relevant utilities connecting them with emergency centres are obligatory in the EU.

[44]Such IoT solutions are already being used, for example, by the US insurer Liberty Mutual, which in cooperation with Google's Nest implements smoke alarms in homes, free of charge, and reduces the insurance premiums upon the installment of the Nests. Nest informs the customers of any smoke or carbon monoxide, see: https://www.libertymutualgroup.com/about-lm/news/news-release-archive/articles/liberty-mutual-insurance-and-nest-partner-to-reward-customers-for-protecting-their-homes-with-innovative-technology.

Wearable devices could notify the insurer in case of a severe health incident, such as a stroke or heart attack, whereas, particularly in cases of elderly or disabled people, they could alert close relatives, emergency contact persons, or even insurers, if no activity is monitored in a day, so that the status of the insured would be checked.

The question arises as to how the above applications could affect the obligations of the policyholders/insureds in the event of risk occurrence. Insureds are required to notify the insurer of the occurrence of the event within a limited time, with severe consequences in case of delay in some jurisdictions. In the example of Greek law,[45] the policyholder has a legal obligation to notify the insurer within eight days from becoming aware of the risk occurrence, otherwise the insurer is entitled to ask for compensation for any damage it has incurred from the delay.[46] In insurance covers where IoT devices automatically alert the insurer upon risk occurrence, such as a car accident or a health incident, the application of said provisions would be perhaps obsolete. If the insurer is automatically notified, is the policyholder still obliged to notify it within the prescribed time limit, given that the law does not provide for any exceptions? If the policyholder does not notify the event, could the use of IoT applications constitute an effective counter-argument against the insurer that claimed compensation because of the absence of notification? Would the widespread use of such IoT solutions trigger the need for these provisions to be modified?

Obligation to Provide Information The same provisions of the Greek ICA state that the policyholder must, at the insurer's request, provide the insurer with any information, data and documents concerning the circumstances and the consequences of the occurrence of the insured risk. The need for insurers to ask for information and data on the exact damages may be reduced if the insurer is granted access to information deriving from connected devices and sensors that would accurately depict the extent of such damages. An innovative example of IoT use to this direction is provided by the US Erie Insurance, which uses drones for property inspections in case of damage claims.[47] In the same relevance, the insurers' requests for information could also be modified; insurers can, instead of asking for specific information and data, request that they are granted access to information collected by appropriate sensors. For example, in cases of road accidents, the databases created by vehicle diagnostics sensors would contain accurate and objective information on the actual damage. Environmental and status sensors in industrial properties could also provide useful information on the post-event status of the property, to efficiently measure the actual damages.

The question that arises is whether policyholders will be **obliged** to provide insurers, upon request, with access to their connected devices and sensors and

[45]See Article 7 par. 1 and 2 of the Greek ICA.

[46]See *Ioannis Rokas*, in I.Rokas, Commentary on Insurance Contract Act (ICA), op.cit., p. 132 et seq.

[47]Doug Drinkwater, *10 real-life examples of IoT in insurance*, May 24, 2016, available at: https://internetofbusiness.com/10-examples-iot-insurance/.

relevant databases, or if they will have the right to completely or partially object to such requests, and what would be the consequences of such objection. Would a policy term stand which would provide that such denial shall result in non-compensation or limited compensation? A particular example is home insurance, where access to home monitoring devices would be equal to access to information on the private life of the home owners/residents. In the same vein, and from the angle of personal data and privacy protection, how would insurers ensure that they only collect and process such information and personal data that are adequate, relevant and limited to what is necessary to evaluate the insurance claim? Where would the line be drawn for the data minimisation principle to be satisfied, which requires that only so much data is processed, as is necessary for the particular cause?

Damage Mitigation IoT applications can be of use in mitigating the damage caused if the risk occurs and, thus, reduce the insurance indemnity. From a preventive point of view, smart sensors may issue alerts notifying the possibility of a hazardous event and allowing for preventive measures to be taken. After the risk occurs, IoT solutions may also assist for the loss to be minimised. A simple example would be the "find your iPhone" app that tracks down your stolen or lost iPhone. A respective vehicle embedded sensor is expected to be in use for nearly half of the vehicles in circulation by 2025.[48] Embedded sensors issuing automatic alerts in case of road accidents and providing the exact location of the vehicle involved in the accident allow emergency services to quickly and accurately locate and reach the vehicle and its passengers and assist them faster, which reduces the effects of injuries and may prove life saving.

Regulatory questions may also arise. As a rule, policyholders are required to take all the necessary measures to avoid or mitigate the insured loss and to comply with the instructions of the insurer, whereas in the event of a negligent breach of said obligation, they may be obliged to indemnify the insurer.[49] IoT applications could enable insurers in case an insured risk occurs to directly and immediately send (e.g. in the form of alerts or messages to the mobile phone or to another connected device of the insured) instructions for the avoidance or mitigation of the damages caused by the insured event. In such case, how far would the policyholder be obliged to follow the insurer's instructions? In addition, what would the implications be in the event of false alert or wrong instructions?

Claims Evaluation and Management IoT-provided information can accelerate the claims management procedure as a whole and leave customers more satisfied by the insurer's efficiency. It can also render it safer, particularly in cases of claims deriving from insured risks related to natural disasters, or from industrial insurance risks. For example, the use of drones for the collection of information on damages caused to insured properties because of fire or flood enables insurers to collect on-time

[48] A.T. Kearney (2014), *The Internet of Things: Opportunity for Insurers*, available at: https://www.atkearney.com/financial-services/article?/a/the-internet-of-things-opportunity-for-insurers.

[49] See for example Article 7 par. 3 of the Greek Insurance Contract Act Law 2496/1997.

information on the extent of the damages caused, without risking the involvement of technical experts in situations that could be perilous to them.

Because of the above, the integration of IoT solutions into the insurance business is radically transforming the operations of insurers in all their aspects, spanning from the design and pricing of insurance products, to their distribution and claims handling. The insurers' fundamental characteristics are being altered by the use of IoT applications, as, to reduce their risks, insurers are focusing more on risk prevention methods. Insurer–customer relations are becoming more direct, more frequent and generally more personal, particularly in health insurances, where insurers are gaining knowledge of their customers' daily routines and habits. However, this may not always come without pitfalls. As insurers gain access to more information and personal data, customers may also grow more cautious with respect to the data they are willing to provide to insurers and make use of the enhanced rights they are granted under the applicable data protection and privacy laws. In this relevance, could the use of IoT in the insurance industry result in a new group of uninsurable customers? Would a new divide be created with respect to customers not willing or unable to use such applications or to provide access to their devices to insurers? Would these customers not be insured? If so, could such discrimination be acceptable under the applicable laws? Another ethical aspect could also arise, concerning the degree to which insurers can make use of the possibilities made available to them by the IoT technological advancements: up to which point can insurers provide guidance and influence the customers' habits and daily life, even if that were to result in a more healthy lifestyle according to state of the art? To what degree can insurers monitor activity within their policyholders' homes and process the personal data deriving from such monitoring? How can it be ensured that the information and data collected and processed via connected devices and sensors is actually necessary for insurance purposes and not for more?

3 IoT and Insurance Risk

Risk is the inherent raw material on which the entire financial organisation of the insurance undertaking is based. The selection of the risks, which the insurer will assume, their assessment and the calculation of the corresponding premiums are the principal functions of the insurance undertaking. IoT applications and their introduction in the insurance industry affect the risk-related parameters of the insurance business. New risks arise from the use of new technologies, deriving from numerous components of the IoT solutions, and create new insurance needs. IoT has a further impact on the way insurers are calculating their regulatory quantitative requirements, as provided in the applicable regulation.

An example of regulation that treats risk as the starting point and weaves around it the entire governance requirements for insurance undertakings is the Solvency II

Directive,[50] the insurance supervisory framework that is in force from 2016 for insurers and reinsurers in the European Economic Area. In introducing this risk-centred approach, Solvency II requires insurance undertakings to hold sufficient economic capital to protect the insureds and beneficiaries and to eliminate the risk that the insurer becomes unable to meet its financial obligations towards them. The capital requirements primarily consist of the so-called solvency capital requirement (SCR), which has to cover all the risks an insurer faces.

EU Member States are required to ensure that insurance and reinsurance undertakings establish technical provisions with respect to their insurance and reinsurance obligations.[51] The value of the technical provisions shall be equal to the sum of a best estimate and a risk margin, while the calculation of the best estimate shall be based upon up-to-date and credible information and realistic assumptions, and be performed using adequate, applicable and relevant actuarial and statistical methods. Such information shall only be considered as credible where insurance and reinsurance undertakings provide evidence of its credibility, considering its consistency and objectivity, the reliability of the information sources and the transparency of the way in which the information is generated and processed.[52] Such best estimate shall be calculated in a transparent manner and in a way, which ensures that the calculation method and the results that derive from it are capable of review by a qualified expert.

When calculating best estimates, the relevant cash-flow projections shall take account of the needs to settle insurance and reinsurance obligations over their lifetime.[53] As a default position, the cash flow projections used in the calculation of best estimates obligations shall be made separately for each policy. Where the separate calculation for each policy would be an undue burden on the (re)insurer, it may carry out the projection by grouping policies. Where a calculation method is based on grouped policy data, the reinsurer shall ensure that the grouping of policies creates homogeneous risk groups that appropriately reflect the risks of the individual policies included in these groups. Such grouped calculation methods are admitted when there is homogeneity of the individual risks.[54] Such homogeneity is ensured when certain criteria are met. In the case of life insurance, for instance, the grouping shall comply with all of the following requirements: (a) there are no significant differences in the nature and complexity of the risks underlying the policies that

[50]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) (recast).

[51]Solvency II Directive, Article 76.

[52]Commission Delegated Regulation (EU) 2015/35 of 10 October 2014 supplementing Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II), Article 27.

[53]Solvency II Directive, Article 77.

[54]For example, segmentation and sub-segmentation could involve males under the age of 25, people with a family history of certain illnesses, single women who fall into a particular income bracket, et. al. http://www.insurancecompanies.com/insider-information-how-insurance-companies-measure-risk/. Economic forecasting, wage and industry trending and market stability assessments all are part of the data that is ultimately used to calculate the insurance premium.

belong to the same group; (b) the grouping of policies does not misrepresent the risk underlying the policies and does not misstate their expenses; and (c) the grouping of policies is likely to have approximately the same results for the best estimate calculation as a calculation on a per policy basis, particularly in relation to financial guarantees and contractual options included in the policies.

Specific requirements also apply to non-life insurances, in which the best estimate for non-life insurance obligations shall be calculated separately for the premium provision and for the provision for claims outstanding.[55]

Furthermore, of all risks an insurance undertaking faces, the underwriting risk is one of the main components for calculating risk and capital. It corresponds to the risk of loss borne by an underwriter and may arise from an inaccurate assessment of the risks associated with writing an insurance policy, or even from uncontrollable factors. Consequently, the insurer's costs may significantly exceed earned premiums and disrupt all the calculations taken into account the regulatory capital obligations. An insurer's profitability depends on how well it understands the risks it insures, and how well it can reduce the costs associated with managing claims. The amount an insurer charges for providing coverage is also a critical aspect of the underwriting process. The premium must be sufficient[56] to cover expected claims, but must also consider the possibility that the insurer will have to access its capital reserves.[57] It seems that a regulatory tendency and the risk-based approach adopted by the Solvency II is shared among the largest and most developed underwriting jurisdictions in the world.

In this relevance, the penetration of IoT solutions in the insurance relationship is expected to affect the insurer's ability to appropriately assess the risk it underwrites; the combination of personal data deriving from the various IoT devices and sensors may enable insurers to build larger and more accurate profiles, to adequately assess the risks in more than one sectors, and to properly price them, while offering

[55]Commission Delegated Regulation (EU) 2015/35, Articles 34–36. To be noted, that the risk margin for the entire portfolio of the insurance undertaking shall be calculated on the assumption that it is taken over by another insurer as set in Article 38.

[56]EIOPA defines the SCR of an insurance or reinsurance company as the value-at-risk (VaR) of the basic own funds subject to a confidence level of 99.5% on a 1-year period.

[57]The insurer's calculation and monitoring of risk and capital must be reflected in its so-called "Own Risk and Solvency Assessment" (ORSA), which is a self-assessment exercise lying at the heart of the Solvency II approach. This approach as a framework has also been incorporated into the International Association of Insurance Supervisors (IAIS) list of Insurance Core Principles, which in practice shows a global endorsement of the ORSA method. In few words, ORSA is an internal assessment of the risks associated with an insurer's strategic business plan that determines whether it has the capital resources to support these risks. The board and senior management are required to take responsibility for ORSA, which must encompass all reasonably foreseeable and relevant material risks. It is very much like an enterprise risk management framework because an ORSA must be forward-looking and must assess risk and capital resources. It is expected by certain analysts that most major jurisdictions will have an ORSA-like approach implemented by the end of the decade, https://risk.thomsonreuters.com/en/risk-solutions/solvency-ii.html#request-details.

diversified and competitive products and services.[58] At the same time, insurers will have to calculate the impact of the corresponding occasional premium payments on their solvency status, and may even end up having to reserve more capital under the applicable provisions regulating the solvency capital requirements.

The question in the particular context of IoT then arises, whether IoT contributes to a better assessment of the insurance undertaking's risk profile with respect to underwriting, and whether it does so in a reliable manner.

On the one hand, IoT is said to *"introduce a layer of technology"* on the business, providing the insurer with an indispensable tool for approaching and measuring such risk. On the other hand, IoT is itself a major factor that may contribute to the creation of the risk and its magnification, thereby still providing tools to mitigate the consequences of the risk occurring. Is then IoT a blessing or a curse for underwriters?

One significant element in the operation of these emerging data-based products and services has been described to entail the highly complex interdependencies, which are being formed between their different layers: the data layer, which includes data collection and processing; the software layer, whether embedded or not; the applications layer, which encompasses different apps, sensors and actuators, data services and tangible or connected automated systems devices; and finally, the connectivity layer, such as the network connectivity, the interconnected data platforms and the digital infrastructures.[59]

3.1 What Kinds of Risks Are There?

IoT essentially makes everyday devices "smart" by connecting them to the internet and to each other. In the home, this could include coffee machines, washing machines, lighting and garage door openers. In business, it can be used for warehouse equipment, oil refineries and turbine engines. While IoT can improve operations, especially by enabling more data analysis, it can also significantly affect businesses and the property and casualty insurance industry.[60]

[58]See also Rachael Gore, FC Business Intelligence 2015, *Insurance, Innovation and IoT: Insurers have their say on the Internet of Things*, available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjtuOzilufdAhUPElAKHRPrAtcQFjADegQIBxAC&url=https%3A%2F%2Fwww.the-digital-insurer.com%2Fwp-content%2Fuploads%2F2015%2F09%2F581-c53e2110-846b-4993-a476-c863188bc3e5_4346_Whitepaper_1_FINAL.pdf&usg=AOvVaw28c6BGebeZb7j-c5aw0JMQ.

[59]See Commission Staff Working Document on the free flow of data and emerging issues of the European data economy Accompanying the document Communication Building a European data economy, SWD/2017/02 final, op. cit.

[60]Brent Rieth, Aon Risk Solutions at RIMS 2017 conference, accessible at https://www.rims.org/RIMS2017/Attendee/Pages/Sessions-Events-By-Day.aspx.

There are potential safety, privacy and product liability issues connected to the IoT technologies. Objects equipped with software have so far been subject to simple damages to the object itself or to related IT equipment, owing to their malfunction. They have also been responsible for data connected damages including data leaks, data losses or hacking. It is now being realised that IoT device malfunctions may cause much more severe damages not only to property, but also to humans.

3.2 Where Does the Risk Lie?

Millions of Internet connected 'things', i.e. devices with embodied communications sensors, have been produced for almost a decade, without being configured to preclude and attend to the various risks which their malfunction could cause, least of all the software leak or hacking possibility.

A primary source of risk is their **software**. The software may be hacked, or may malfunction, or fail to update or upgrade. Software vulnerabilities are inherent and unavoidable: there are immense amounts of code produced every year with clearly augmenting trend, and the degree of reported flaws inevitably increases as well. Equally, data may be hacked and result in a very large scale of leaks or ransomware; devices may be hacked and then be subject to intentional reprogramming with the effect of malfunctions and disruption of personal devices to major industrial units. To get a flavour of the extent that software malfunctions can take, one can recall the cease of operations of the Heathrow airport in July 2018, which rendered a considerable part of the airport's facilities, including the air traffic control tower, unavailable. In addition, there have already been examples of smart objects malfunctions, for example in the medical devices market.[61] Serious malfunctions have been also documented in the industry of autonomous vehicles; the Tesla examples, where fatal accidents occurred while the vehicles were in autopilot mode, are the most characteristic.[62] In Greece, some malfunctions have been noticed in the driverless buses in public transportation[63], but they have passed the pilot phase.[64]

[61]E.g. Implantable drug infusion pumps have been recalled over multiple occasions as allegedly a malfunction in their software could lead to imbalance the medicine doses, see https://www.fda.gov/medicaldevices/safety/listofrecalls/ucm546558.htm.

[62]See relevant information at: https://en.wikipedia.org/wiki/Tesla_Autopilot#Incidents.

[63]See http://www.ekathimerini.com/201509/article/ekathimerini/community/driverless-bus-on-the-way-in-trikala, 14.09.2015.

[64]Current research on software reliability does not provide sufficiently apt tools to quantitatively assess the risk posed by a piece of life-critical software such as a medical device. For example, black-box software reliability models are too general and make too many assumptions to be applied on confidently to assess the risk of life-critical software, see Jeffrey M. Voas, Larry K. Voas and Keith W. Miller, *A Model for Assessing the Liability of Seemingly Correct Software*, accessible at https://www.cigital.com/papers/download/iasted92.pdf.

Further malfunctions may occur in relation to connectivity. A failure in the provision of the telecommunications network or dedicated platform may result in large-scale disruptions of the function of the 'thing', and may require, for example, that the operation be reprogrammed. This could cause severe flaws, especially in consumer related applications, as would be the case for example with medication schedules for patients and the ensuing disruptions of their routines, with lighter to very severe potential effects.

Apart from the above, the **user** himself may cause the damage, for example by violating the instructions or the protocols of use of the object. External **random** factors may also trigger a malfunction of the device, simply because the device was not wise or knowledgeable enough or because it was insufficiently programmed to recognise and deal with the specific event that occurred. This has been obvious in the recent cases of autonomous car accidents, where in one example the autopilot sensors failed to recognise the white tractor crossing the highway against the bright sky, and consequently the car failed to apply the brakes.[65] In other cases, the autopilot sensors seem to have demonstrated difficulties in appropriately distinguishing road surface markings, stationary objects on highways, or highway barriers, thus resulting in related accidents.[66]

3.3 Consequences for the Insurance Industry

Insurers, as discussed, are required to assess their technical provisions based on a best estimate, calculated with reliance on up-to-date and credible information and realistic assumptions. When developing risk assessment models, insurers and actuaries rely among others on statistical information. However, such emerging risks cannot yet be validated by historical data, as the historical knowledge is not sufficient at this stage. Even applying by analogy the knowledge obtained from any comparable risk situation is not undisputedly possible because of lack of comparability. In contrast to most traditional insurance products, the understanding of the emerging risk situation in IoT is not confirmed yet.[67]

[65] See Danny Yadron and Dan Tynan at The Guardian, *Tesla Driver dies in first fatal crash while using autopilot mode,* 01.07.2016, https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk.

[66] See in this relevance the example of an accident in Greece: Philip Chrysopoulos, *First Tesla 3 Road Accident in Greece*, 28.03.2018, available at: https://greece.greekreporter.com/2018/05/28/first-tesla-3-road-accident-in-greece/.

[67] Andreas Haas, Markus Haas, Markus Weinert, *The Internet of Things is already here, but who bears the risks?*, Working Paper for Presentation at the World Risk and Insurance Economics Congress (WRIEC), July 2015, available at http://www.wriec.net/wp-content/uploads/2015/07/6J3_Haas.pdf, with a multitude of examples of risks affecting consumer and industrial applications, including industrial plants, transportation and smart cities.

The risks in the examples discussed above have as a common denominator that it is difficult to delimit producer's liability between the manufacturer of the object ('thing') and of the software, on the one hand, and sometimes also of the connectivity provider on the other. In other words, it is not only the volume but also the party who caused the risk that is uncertain, so that the subrogation of the insurer in an eventual claim of the client against a third party may have reduced chances of success. This can lead to a larger exposure for the insurer, which could harm profitability.

Nevertheless, engaging the customer in understanding and dealing with the risk drivers that influence their risks, their potential damages and, thus, their premiums, may, next to providing valuable data, enhance the customers' loyalty and preparedness to be insured, as they will be more convinced of the appropriateness of the cover they are purchasing. This will allow a better distribution of the risk. It is the gathering of data and their accumulation and feeding into pricing models, together with the ever-increasing big data processing, that will result in a better risk prediction and assessment by the insurer via the evolving information that will be produced.

In this relevance, in terms of products creation and pricing, IoT can provide to insurers the possibility to offer alternative bundled opportunities, as for example an industrial property fire insurance bundled with environment monitoring technology, which can work as a win-win combination: the probability of risk occurrence is in this way reduced, and so is the premium. Similar patterns can be followed in the insurance of accommodation complexes, where IoT can be integrated in the hotel management system and, for example, issue alerts in the event a risk occurrence is threatened (e.g. smoke is traced, or earthquake movement is detected), or the system receives relevant alerts from public emergency mechanisms (e.g. alert that a tsunami may hit the area, or that a fire is approaching). This can increase both the insurability of the respective risks, while at the same time reducing the possibility of risk occurrence—or at least the anticipated extend of the damage. Alternatively, in health insurance, insurers could monitor an insured's compliance with a rehabilitation protocol (e.g. in case of disability claims) or with a medication treatment.[68] New products, and new market possibilities could arise from the development of "ubiquitous" or "smart" cities, i.e. cities where computers are built into the buildings and streets, allowing residents to video-conference with their neighbours, attend classes remotely, control lighting, heating and air conditioning with the push of a button on a control panel, use sensors to gather information on traffic flow and energy use, etc., as well as alerting authorities when a crime is taking place.[69]

In these cases, occurrences of traditional risks seem to be much mitigated, and if a risk happens (even if of very high impact), IoT solutions could be deployed to reduce

[68]See relevant examples mentioned by Robert Reiss, *5 Ways the IoT will transform the insurance industry*, op. cit.

[69]For example, Songdo IBD has been designed and created to be such a "ubiquitous" or "smart" city in South Korea. See more information at: See https://en.wikipedia.org/wiki/Songdo_International_Business_District ; http://bginvestors.com/master-plan/songdo-ibd/.

such impact. Thus, with the installation of security standards and prevention measures, risks and liabilities can be reduced. For example, how will the premium be affected, when a house is already monitored day and night for break-ins, and the chance of a fire or flood decreases incrementally because the owners are constantly monitoring their appliances, water and heat systems via a remote device? In addition, how will the premium for the third party liability and own damages policy of the transportation system of a smart, connected city be priced, if it is constantly monitored by automated control programs?[70]

As a token of the opportunities that IoT offers in customising and at the same time segmenting covers, it is reported that an Italian insurer has attracted 100,000 new customers in a little more than a year by allowing consumers to design and build their own policies based on 13 specific "building blocks" from P&C, life and health insurance lines. Consumers could see exactly what each policy component costs and how much coverage each one provides. The key to success according to company executives was "*revolutionising the product architecture and pricing techniques, and integrating P&C and life insurance*."[71]

From a market perspective, and as is analysed in Sect. 2 of this Chapter, it is claimed that IoT-based data, carefully gathered and analysed, might help insurers evolve from a defensive posture, i.e. from spreading risk among policyholders and compensating them for losses, to an offensive posture: i.e. to helping policyholders prevent losses and insurers avoid claims in the first place.[72] In this direction, IoT is described as a technology architecture stitching together existing technologies in a specific way so that new benefits can be achieved. Examples as to how IoT technology may reshape the insurance industry's perspective of risk are as follows[73]: the movement toward usage-based insurance models is likely to reduce the risk and decrease claims numbers and volume; insurance companies would not only calculate risk, but also work with appliance, automobile, and other equipment manufacturers to reduce actual risk; loss rates should then decrease markedly; for example, the US

[70]To be noted in this regard, that the preparedness of the producer to install such measures not only depends on cost, but is also commensurate to the producer's own alertness and endorsement of the potential risks, the relevant legal and social environment, its mentality, and the degree to which it shall be faced with sanctions if it fails to take the measures. So is also the purchase of insurance. This is especially the case with respect to startup producers of innovative products or services, and has the consequence that the risk is transferred to third parties, i.e. their customers.

[71]E&Y, *The Internet of Things in Insurance. Shaping the right strategy, managing the biggest risks, 2016*, op.cit.

[72]Deloitte, *Opting-In: Using IoT Connectivity to drive differentiation*, 2016, available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjggOvyovndAhUB-qQKHSP4C8AQFjAAegQICRAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2Finsights%2Fus%2Farticles%2Finnovation-in-insurance-iot%2FDUP2824_IoT_Insurance_vFINAL_6.6.16.pdf&usg=AOvVaw2t-wsLlfa6xE5P66YGQx0U.

[73]Erik Sandquist QA: *The impact of the Internet of Things on insurance*, Accenture, 2018, available at: https://www.accenture.com/gr-en/insight-perspectives-insurance-internet-things-transform.

Department of Energy is reported to have forecast that the IoT's ability to enhance predictive maintenance of assets could eliminate up to 70% of breakdowns.

Further, there is opportunity to develop and price real-time micro-insurance packages to meet shifting demand. In this sense, IoT is said to offer insurance carriers a chance to depart from the product commoditisation trend that has left many personal and commercial lines competing primarily on price rather than coverage differentiation or customer service. The downfall for this may be that as actual risk levels are reduced through smart automation, the requirement for purchasing insurance may also decrease. On the other hand, taking into consideration that the use and expansion of connected devices and sensors inherently entails new risks, new insurance products are expected to emerge.

It derives from the above analysis that, as the insurance product itself is being transformed, so will the ways employed by insurers to assess and price the risk, and calculate their respective regulatory capitals, have to be transformed and become more customised. Safety, privacy and product liability issues derive from the use of IoT devices, which in turn correspond to new risks. Practically all the features that are inherent to the IoT notion and operation may constitute the sources of such new risks; software malfunctions, failures of the necessary connectivity, human errors, and even external random factors may result in loss-making events. At the same time, IoT applications grant insurers with the ability to better familiarise themselves and their customers with the factors affecting their risks and the pricing of their premiums, resulting in enhanced customer loyalty, as well as to offer advanced insurance products, even bundled with other products/services, aiming at risk minimisation.

4 Effects on the Civil Liability Model

It has been discussed that the IoT environment is characterised by the highly complex interdependencies between its various components, including the object itself, the software, the data collected and generated, the applications, and the connectivity. Human error and random instances added up, damages can occur which are not restricted to the 'thing' itself, but can expand to massive property damages as well as to bodily injury and death.

The Challenge of Allocating Liability In view of the interdependence between these factors, the velocity and sophistication of the interchanges between them, and the potential complexity of the operational parameters, especially in view of larger IoT systems such as industrial operations or smart cities, it may be a challenging exercise to allocate the responsibility for the occurrence of the damage. The existing liability models either refer to a strict extra-contractual liability structure where the producer of the object is ultimately responsible to indemnify the damaged person irrespective of fault, and if the harm cannot be attributed to another factor in the

value chain or the misuse of the object by the final user[74], or to a pooling structure where a fund is set-up and financed by the principal operators of a hazardous activity, which shall account for indemnifying damages that would be too large to cover by a single operator.[75] Both models are introduced by international conventions or by law, as they impose onerous security schemes on the originators of the hazardous activity in their capacity as the main financial beneficiaries, while such activity is acceptable and endorsed by the society for the actual benefit and life conditions improvement it distributes to it.

An inherent problem in the IoT environment can be that, depending on the complexity of the system, it may prove difficult to allocate responsibility, as it may be that neither the fault nor the causation can be clearly established and attributed to a specific party. For example, will the producer of the object be liable or the providers of the software, if these are separate? Would the segregation of liability be clear among them? How will the sequence of causation be established?

The responses to these questions, the extent to which the introduction of new legislation is needed, and the appropriate legislative solutions cannot be provided in a blanket manner to all IoT applications. They depend on the kind of the IoT system, its complexity, whether it is addressed to consumers or to industry, the extent of its technological advancement, and other factors.

Proposed Legislative Solutions Legislators have started to introduce solutions with regard to the more advanced systems, as can be seen in the example of the **German law** on motor third party liability which was amended on 21 June 2017 to provide for vehicles with auto-pilot mode. For these cases, the law added the manufacturer of the vehicle as well as the IT-provider to the jointly and severally liable parties, next to the owner and the driver of the car. Once one party indemnifies, it has the right of recourse against the others *pro rata* to their liability in causing the accident. The new provisions include certain safeguards for the allocation of liability: self-driving cars must include technical equipment that allows the driver to take back the control of the car at any time and continue to drive manually. They must include a device in the sense of the airplanes' "black box", that gathers data of the journey. This provision helps to ensure that drivers shall not rely on technical failures of the automated car system to rule out any negligence of their own. If the data retrieved from the black box evidence that multiple IT-service providers are liable, the liability of those service providers is calculated *pro rata*. Failures of the car system from frequency disturbances (i.e. through mobile phone networks) or data flow disturbances, as well as hacking incidents and generally any event that is not

[74] See as an example for such a liability structure the EU Directive on Defective Products Liability - Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, as modified by Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999.

[75] For example, the fund created by the International Convention for the Prevention of Pollution from Ships (MARPOL), which is the main international convention covering prevention of pollution of the marine environment by ships from operational or accidental causes.

caused by a malfunction of the autopilot are treated as force majeure incidents for triggering the car keeper's no-fault liability, and thus the insurer's.

A debated issue is the question, whether the manufacturer of vehicles with auto-pilot mode should be treated as a "co-driver" and therefore bear the same degree of liability as the human driver in the case of an accident. There are two scenarios that can be distinguished[76]: in cases where vehicles with auto-pilot mode are controlled manually by the driver, the vehicle manufacturer shall not qualify as a co-driver of the vehicle. However, in cases where the self-driving car is operating in auto-pilot mode, the car manufacturer may be recognised as a co-driver, in which case they would have to be included in the scope of the motor liability insurance. It remains to be seen how the German legislator, as well as German court case law will treat this scenario.

The UK has recently enacted the Automated and Electric Vehicles Act (AEVA) 2018. An automated vehicle is a vehicle that can safely and legally drive itself. The section on automated vehicles, which applies only to accidents on a road or other public place in Great Britain, relies on the premise that the liability shall lie with the insurer if the vehicle is insured. Insurers may exclude or limit liability if the accident results from either prohibited software alterations or a failure to install critical software updates. However, the owner or insurer is not liable where the person in charge of vehicle, who can be different from the owner, should not have allowed the vehicle to begin driving itself when it was not appropriate to do so.

Following the enactment of the AEVA, which contains a Commencement Order requiring that most sections be complemented by a statutory instrument, the Law Committee has launched a preliminary consultation on the regulatory framework for the safe deployment of automated vehicles, which aims inter alia to define the notion of user-in-charge and automated driving system entity (ADSE) as well as civil and criminal liability issues.

"Knock-for-Knock" Agreements or Mutual Indemnity Hold Harmless Clauses Depending on the case, it may be that IoT may be operating under inherently hazardous conditions, high financial stakes and probability of catastrophic consequences. This can be the case for example in large industrial installations or maritime operations, where the complexities and interdependence of the various components are very high and the apportionment of liability is uncertain, complicated, costly and long.

A different model, which has been tested in practice in situations with similar difficulties of allocation of liability, is the so-called "*knock-for-knock*" agreements, widespread use in offshore maritime oil and gas industry. The reasons that led to

[76]See the description of the law and the analysis by Prof. Dr. Robert Koch, *Verteilung des Haftpflichtversicherungs-/Regressrisikos bei Kfz-Unfällen während der Fahrzeugführung im Autopilot-Modus gem § 1 a Abs. 2 StVG* (in English: "Distribution of liability insurance risk and third party liability risk in accidents of cars driving in autopilot-mode according to par. 1 a el. 2 StVG"), VersR 69/2018, pp 901 et. seq.).

such use also seem to be applicable to the IoT industry: hazardous operations, impracticability of fault-based allocation of liability because of complexities, and delays, as well as lower insurance premiums for the parties involved, because of the contractual limitation of the liability to certain operational aspects.

Under a knock-for-knock agreement, each party assumes responsibility and indemnifies the other parties for liabilities relating to the indemnifying party's own property and personnel and those of its subcontractors, regardless of which party is negligent and whether there is causation. In other words, each party is responsible for its own damage, irrespective on whose fault the damage was caused, and whether the necessary causal links are established. The damaged party shall not seek recourse against any damaging party or their insurer. As "*own damage*" is understood the damage to the respective party's group, which includes its employees, subcontractors and the party's property and estate. The damage may consist of bodily injury or death, or property damage or environmental liability. Such arrangements focus on the redistribution of risk and liability by way of mutual indemnity clauses in the agreement, concluded based on freedom of contract.

Knock-for-knock agreements are not viable if there is no insurance. However, as there is no subrogation in the indemnified party's rights, the insurers of the parties must also refrain from seeking recourse against the damaging parties.[77] As the insurer's consent to the scheme is a prerequisite for the backing of the knock-for-knock contracts, such agreement must be sought in advance. In assessing their consent, insurers including P&I clubs, seek to establish that there is balance of the powers of the contracting parties in the contracts and for assurances that the contracts are enforceable; also, that their liability shall not exceed their client's. To be admissible to the P&I pool, knock-for-knock contracts must be balanced and must not include liabilities that members incur voluntarily. In addition, for knock for knock liabilities to be poolable, P&I Clubs require contracts to incorporate indemnity clauses which protect the party if it is sued by a third party who is not bound by the contract.

Although this kind of arrangement may resolve the highly problematic apportionment of liability and establishment of causation in large damages in a pragmatic way, there are a number of downsides that prejudice its application. The agreement will not stand if in the jurisdictions involved a contractual limitation of liability is not valid for gross negligence or intent, as is the case in continental jurisdictions. The waiver of obligations relying on strict liability or public policy will be similarly problematic. The treatment of indirect or consequential losses differs in common law and civil law jurisdictions. The ambit itself of the indemnity has been very often

[77] Variations of the knock-for-knock concept apply in several jurisdictions. The Greek private pool of motor third party liability claims management is an example, where the pool works as a facilitator for the rapid settlement of disputes in favour of the customer: the customer is indemnified by its insurer, and then the insurers settle the claims among them in the pool. The difference to the knock-for-knock model described above is that there is still recourse and subrogation of the indemnifying insurer against the liable party and, principally, its insurer. In this sense, the downsides of knock-for-knock agreements described in this section are eliminated.

contested in litigation. Not least, the balance of powers between the contracting parties is extremely important, as the weaker parties should not be called to indemnify for faults of the stronger ones.[78]

More specifically, existing legal practice has shown that knock-for-knock agreements may not be recognised in all jurisdictions. Even in jurisdictions that are favourable to such agreements, such as US, UK and Nordic Countries, a number of questions arise. Above all, the legal nature of knock-for-knock agreements is disputed: Are mutual indemnity clauses liability allocation/limitation or liability exclusion clauses? The answer to this question might have far-reaching consequences for the enforcement of knock-for-knock clauses, given that a contractual exclusion of liability might be subject to several statutory restrictions, not least the nullity of agreements excluding liability for gross negligence or intent. This is however not an agreement to exclude or avoid legal responsibility, but one to redistribute it.[79]

In addition, major accidents that have given rise to litigation reveal that the reach of knock-for-knock-agreements is not always clear. One of the preliminary issues to be determined is the property, personnel, etc., that is subject to the cross-indemnity clause in case of damage or loss.[80] Moreover, there has been extensive case law on the question whether the cross-indemnity clause, in the absence of clear wording, is to be construed as relieving a party of the consequences of its own gross negligence or wilful misconduct.[81] In addition, it has been debated whether the protection of the indemnified party from liability for gross negligence or wilful misconduct is contrary to the public policy[82] or whether a breach of contract invalidates a knock-for-knock agreement.[83] Lastly, some decisions have called into question the bargaining power of the parties and the contractual equilibrium in case of knock-for-knock agreements.

Such uncertainties have become more evident following BP's huge pollution liabilities because of the *Macondo* disaster, which led involved parties to revise their policy in respect of knock-for-knock agreements.[84] Therefore, although knock-for-

[78]See for example LeRoy Lambert, *Knock-for-knock contracts are enforceable in the US*, Standard Bulletin October 2011, p. 10, where mention is made to the 'Anti-indemnity' statutes passed by the states of Texas and Louisiana, the home of much of the offshore oil exploration industry in the US, following the Deepwater Horizon incident in the Gulf of Mexico, as a consequence of attempts by major oil companies to contractually require local providers of supplies and services in the oil industry to assume all liabilities, even if caused by the fault of the oil company. In effect, the local suppliers would indemnify the oil company even if the oil company's fault caused the damage.

[79]Ugwuanyi (2012), pp. 136–146.

[80]*cf. Caledonia North Sea Ltd v London Bridge Engineering Ltd* [2002] UKHL 4.

[81]*cf. E E Caledonia Ltd v Orbit Valve Co plc* [1994] 1 WLR 1515; Lord W. Douglas Cullen, *The Public Inquiry into the Piper Alpha Disaster* (1990), Vol 1 (November 1990, HMSO Publications Centre).

[82]cf. *HIH Casualty and General Insurance Ltd & Ors v Chase Manhattan Bank & Ors* [2003] UKHL 6.

[83]*A Turtle Offshore SA v Superior Trading Inc* [2008] EWHC 3034; *Smedvig Ltd v Elf Exploration UK Plc(The Super Scorpio II)* [1998] 2 Lloyd's Rep 659.

[84]See for example Egbochue (2013).

knock agreements might be, in principle, able to resolve complicated liability allocation issues related to the deployment of IoT, a pragmatic legislative framework in respect of such agreements would be necessary to ensure the terms of their enforcement as well as their smooth operation in view of the lessons learnt in the aftermath of major accidents, where liable parties had concluded mutual indemnity agreements. Another matter is the extent to which the contractual allocation of the indemnity adequately covers third party damage.

Because of the inherent potential of IoT to result in cross-border liability and the ensuing conflicts of law and jurisdiction, policy makers could contemplate the possibility to adopt a European/regional legal instrument or even a convention relating to the use of IoT, which could, among others, protect knock-for-knock agreements as a mechanism to allocate liability where fault-based liability regimes cannot work properly, and not as a waiver/release from liability system. Such an instrument should safeguard, at least, that knock-for-knock agreements could not be invalidated on grounds of public policy but should be interpreted in light of their object and purpose.

The particularities and high complexity of the Internet of Things naturally raise questions and concerns on the effects of IoT to the civil liability model. More specifically, the issue of allocating responsibility arises: the use of IoT systems inherently incommodes the application of traditional liability models, as neither fault nor causation can be allocated to one party with certainty. Certain jurisdictions have already taken legislative action to provide solutions to this predicament, as in the case of the German law on third party motor liability, which was amended to include provisions on vehicles in auto-pilot mode, and the UK Automated and Electric Vehicles Act. In the case of operation of IoT systems in extremely hazardous conditions, high financial stakes and probability of catastrophic consequences, a solution can be sought in applying models that are used in scenarios where the allocation of liability is equally difficult. The introduction of "knock-for-knock" or mutual indemnity hold harmless clauses, which have been widely used in the offshore maritime oil and gas industry, and according to which each party shall assume responsibility for damages relating to the indemnifying party's own property and personnel, regardless of fault or causation, could be explored to establish if it could offer a viable solution, as such or with moderations, taking into account the legal and enforcement downsides in its application.

5 Summary and Conclusions

The Internet is present in all aspects of our daily lives and creates a constant need for connectivity, communications and interactions. Considering this new reality, the technological evolution has led to the development of the Internet of Things (IoT), a network of connected to the web, interconnected and interacting devices and sensors, rapidly evolving into the "Internet of Everything" notion, covering and affecting almost every form of communication, be it between machines (M2M) or between

people and machines (P2M), or between people (P2P). Existing and developing IoT solutions create multiple new business opportunities for market participants across all economy sectors.

The figures depicting the exponential growth of IoT correspond to a growing, already massive, amount of data being constantly collected, analysed and transferred from IoT devices. The availability of real-time, significant amount of data, in combination with new, sophisticated data analysis tools are of utmost interest for the insurance industry; appropriate, up-to-date and accurate data are necessary for insurers to understand the needs and demands of their target customers, manufacture and offer insurance products that meet these needs (standalone or bundled with other non-insurance products and services), and appropriately price the related insured risks. At the same time, the use of IoT, as well as external factors that may adversely affect the proper functioning of IoT devices, generate new issues and corresponding safety, privacy and product liability risks that also need to be properly understood and priced by the insurance industry.

At the pre-contractual stage, IoT solutions are capable of enhancing the trust between insurers and their customers, as they may facilitate and render more user-friendly the provision of information on the insurance product and its characteristics to the customers. IoT applications do not only affect the preparatory stage of the insurance contract. Their implications are visible throughout the term of a policy, up to the claims notification and evaluation stage, which is expected to be essentially affected by IoT solutions that result in automatic or semi-automatic notifications, and in easier, safer, more direct and fast collection of information related to the event and the damage to be compensated. In this context, IoT devices are also creating the need for re-assessment and possibly modification of the traditional civil liability models, as new challenges arise, particularly with respect to the allocation of liability between the different parties involved in the IoT constellation.

Apart from its effects on the insurance value chain, IoT is seen to alter the character of insurers as a whole: with the use of IoT, insurers can transform from damage compensating to risk preventing organisations, as they focus more and more on employing IoT applications that may help reduce risk occurrence events and/or mitigate the damages caused. Given that insurance risk is one of the more crucial elements for the insurance undertaking, IoT solutions are evolving into a useful tool towards the more accurate calculation of risk and compliance with their regulatory quantitative requirements.

References

Callaway J (2017) The Internet of Things: Key considerations for Life Insurers – Five Questions with GRA's Julianne Callaway, 20 December 2017. Available at: https://www.rgare.com/knowledgecenter/media/articles/the-internet-of-things-key-considerations-for-life-insurers

Chrysopoulos P (2018) First Tesla 3 Road Accident in Greece, 28 March 2018. Available at: https://greece.greekreporter.com/2018/05/28/first-tesla-3-road-accident-in-greece/

Deloitte (2016) Opting-In: Using IoT Connectivity to drive differentiation. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjggOvyovndAhUB-qQKHSP4C8AQFjAAegQICRAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2Finsights%2Fus%2Farticles%2Finnovation-in-insuranceiot%2FDUP2824_IoT_Insurance_vFINAL_6.6.16.pdf&usg=AOvVaw2t-wsLlfa6xE5P66YGQx0U

Drinkwater D (2016) 10 real-life examples of IoT in insurance, 24 May 2016. Available at: https://internetofbusiness.com/10-examples-iot-insurance/

Egbochue C (2013) Reviewing 'Knock for Knock' indemnities following the Macondo Well Blowout. The Piper Alpha, Montara and Macondo oil rig disasters. Const Law Int 7(4):7

Ernst & Young (2016) The Internet of Things in insurance: shaping the right strategy, managing the biggest risks. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwiRxa7m_uTdAhUrqIsKHWhyCAYQFjABegQICBAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2FEY_-_The_internet_of_things_in_insurance%2F%24FILE%2FEY-the-internet-of-things-in-insurance.pdf&usg=AOvVaw1goOD-Xd5_fmZyY34wqakR

EU Commission Staff Working Document, *Advancing the Internet of Things in Europe*, {COM (2016) 180 final}, 19 April 2016. Available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-advancing-internet-things-europe

EU Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, Accompanying the document Communication Building a European data economy, {COM(2017) 9 final}, 10 January 2017. Available at: https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy

Gore R (2015) Insurance, innovation and IoT: insurers have their say on the Internet of Things. FC Business Intelligence. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjtuOzilufdAhUPElAKHRPrAtcQFjADegQIBxAC&url=https%3A%2F%2Fwww.the-digital-insurer.com%2Fwp-content%2Fuploads%2F2015%2F09%2F581-c53e2110-846b-4993-a476-c863188bc3e5_4346_Whitepaper_1_FINAL.pdf&usg=AOvVaw28c6BGebeZb7j-c5aw0JMQ

Haas A et al (2015) The Internet of Things is already here, but who bears the risks? In: Working Paper for Presentation at the World Risk and Insurance Economics Congress (WRIEC), July 2015. Available at: http://www.wriec.net/wp-content/uploads/2015/07/6J3_Haas.pdf

Harner I (2018) How will IoT transform the insurance industry? Available at: https://medium.com/iotforall/how-will-iot-transform-the-insurance-industry-609f89a12bf1

Hoppner T, Gubanova A (2015) Regulatory challenges of the internet of things, Computer and Telecommunications Law Review (C.T.L.R.), 2015, referring to Europol (2014). The Internet Organized Crime Threat Assessment (iOCTA), 2014. Available at: https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

Kathimerini Newspaper (2015) Driverless bus on the way in Trikala, 14 September 2015. Available at: http://www.ekathimerini.com/201509/article/ekathimerini/community/driverless-bus-on-the-way-in-trikala

Kearney AT (2014) The Internet of Things: opportunity for insurers. Available at: https://www.atkearney.com/financial-services/article?/a/the-internet-of-things-opportunity-for-insurers

Koch R (2018) V erteilung des Haftpflichtversicherungs-/Regressrisikos bei Kfz-Unfällen während der Fahrzeugführung im Autopilot-Modus gem § 1 a Abs. 2 StVG (in English: "Distribution of liability insurance risk and third party liability risk in accidents of cars driving in autopilot-mode according to par. 1 a el. 2 StVG"), VersR 69/2018

Lampbert R (2011) Knock-for-knock contracts are enforceable in the US. Standard Bulleting, October 2011

Merrey P, Kokins A (2017) Will on-demand insurance become mainstream? Available at: https://assets.kpmg.com/content/dam/kpmg/uk/pdf/2017/09/will-on-demand-insurance-become-mainstream.pdf

Monetary Authority of Singapore, *MAS' Role in a Smart Financial Centre*, at: http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/MAS-Role.aspx

O'Hearn S (2018) Addressing International Change: The Agenda of the Global Insurance CEO. In: Key Note speech at 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", 12 April 2018, Warsaw, Poland. Available at: http://www.aida.org.uk/docs/Agenda%20of%20The%20CEO%20March%202018_Warsaw.pdf

OECD (2015) OECD Digital Economy Outlook 2015. OECD Publishing Paris. Available at: https://doi.org/10.1787/9789264232440-en

OECD (2016) The Internet of Things: Seizing the Benefits and Addressing the Challenges. OECD Digital Economy Papers No. 252, OECD Publishing, Paris. Available at: https://doi.org/10.1787/5jlwvzz8td0n-en

OECD (2018) Product Safety in the Internet of Things. OECD Digital Economy Papers, March 2018 No. 267. Available at: https://www.oecd-ilibrary.org/deliver/7c45fa66-en.pdf?itemId=%2Fcontent%2Fpaper%2F7c45fa66-en&mimeType=pdf

Parente F (2018) EIOPA's InsurTech Activities. In: 7th AIDA Europe Conference, "De-Mystifying InsurTech: a Legal and Regulatory Approach", 12 April 2018, Warsaw, Poland. Available at: http://www.aida.org.uk/docs/2018-04-12%207thAIDAEuropeConferenceEIOPAsInsurTechActivitiesFaustoParente.pdf

Reiss R (2016) 5 Ways the IoT will transform the insurance industry. 1 February 2016. Available at: https://www.forbes.com/sites/robertreiss/2016/02/01/5-ways-the-iot-will-transform-the-insurance-industry/#47b1782e66d0

Rieth B (2017) Aon Risk Solutions at RIMS 2017 conference. Accessible at: https://www.rims.org/RIMS2017/Attendee/Pages/Sessions-Events-By-Day.aspx

Rokas I (2014) Collective work, Commentary on Insurance Contract Act (ICA). Nomiki Bibliothiki, 2014

Sandquist EQA (2018) The impact of the Internet of Things on insurance. Accenture, 2018. Available at: https://www.accenture.com/gr-en/insight-perspectives-insurance-internet-things-transform

Schmidt E (2015) In the World Economic Forum in Davos, January 2015

Ugwuanyi CS (2012) Examining the exclusionary nature of oil and gas contract mutual indemnity hold harmless clauses. Int Energy Law Rev 4:136–146

Voas JM et al. A Model for Assessing the Liability of Seemingly Correct Software. Available at: https://www.cigital.com/papers/download/iasted92.pdf

Wikipedia, at https://en.wikipedia.org/wiki/Internet_of_things

Wikipedia, at https://en.wikipedia.org/wiki/Tesla_Autopilot#Incidents

Wikipedia, at https://en.wikipedia.org/wiki/Songdo_International_Business_District;http://bginvestors.com/master-plan/songdo-ibd/.

Yadron D, Tynan D (2016) Tesla Driver dies in first fatal crash while using autopilot mode, 1 July 2016. Available at: https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk

The Challenges for Regulation and Control in an Environment of Rapid Technological Innovations

Simon Grima, Jonathan Spiteri, and Inna Romanova

1 Introduction

The last two decades have brought about a 'digital shift' into an information era, with the power to own, control, regulate, and access information/data in a short span of time. In the same way that control over the means of production shaped the industrial era, this power to control information will determine the new evolutionary dynamics of today and the future. The emergence and rapid proliferation of network technologies have revolutionized how we capture and share creative works, altering in perceptible ways the value of information and its significance in our lived experiences. Therefore, more than ever before, regulations, controls, and policies that ascribe rights and protect privileges in relation to these valuable resources, play a key role in both allocating power and controlling its flow. In this era, these controls will need to continue, albeit in an innovative manner, to play the usual role of controlling rights and behavior in relation to the resource of information.[1]

The insurance industry is not spared from this new era and the changes it brings with it. The hype surrounding the proliferation of technology in insurance markets has been significant. Blockchain-based technology, the creation of Bitcoin and other cryptocurrencies and robo-advice, to mention a few, have complicated and disrupted the landscape of yesterday's financial services providers[2] and their ancillary services

[1] Craig (2017).

[2] Romānova et al. (2018).

S. Grima (✉) · J. Spiteri
University of Malta, Msida, Malta
e-mail: simon.grima@um.edu.mt

I. Romanova
University of Latvia, Riga, Latvia

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_4

such as auditors, underwriters, advisors, actuaries, lawyers, and regulators. These new technologies offer tremendous opportunities for innovation and development, but are also uniquely suited to facilitate illicit behavior and are disrupting the role, structure, and competitive environment for financial institutions and the markets and societies in which they operate.

With this paper, we aim, through a review of the literature, to highlight the challenges for regulations and control in an environment of rapid technological innovation, specifically focussing on InsurTech and RegTech, offering logical solutions to insurance companies. We do this by integrating the basic utility model of behavior, the underlying regulatory, and control principles as a benchmark, as well as emerging developments in the economy, to make suggestions intended to support or at least not impair the technological innovative potential in the insurance services industry.

2 Technological Innovations in Insurance and Related Regulation

InsurTech is an amalgamation of "insurance" and "technology", and it refers to the emerging market of digital technologies, which are aimed at the transformation of the current insurance industries, by offering innovative ways to access, propose and administer insurance products and services at lower costs, in a more efficient and effective manner, with high quality and security.

InsurTech specialists are now looking at collaborating with insurance companies. These new players are offering innovative technology to lower operational costs and boost customer satisfaction to traditional insurance institutions. Moreover, they are strengthening biometrics authentication and identity verification solutions, new methods of assessing risks or customer spending patterns, and many others.

RegTech fits perfectly into this concept if it is aimed to help businesses comply with the mushrooming numerous regulations and reporting requirements within this industry. These companies integrate 'technology' with 'regulation'. In fact, RegTech companies can strengthen the position of insurance services providers by helping them to adapt faster to the changing regulatory requirements by integrating and automating all processes and in doing so enabling them to manage their legal risks in a flowing and timely manner, reducing tremendously the costs of doing this. They are offering numerous legislative monitoring, compliance, management, activity monitoring, regulation gap analysis, reporting, case management, and other technological tools that can reduce the massive manual work and manipulation and recording of data to enable the resolution of issues regarding compliance and reporting obligations.

Several key themes have emerged in this challenging control environment. Insurance firms, along with other financial institutions, are facing an increase in regulatory and control challenges to allow safe and legitimate innovation. Regulators

and internal controllers around the world are continuously focusing their efforts to develop comparable frameworks across multiple jurisdictions for insurance conduct and supervision. Moreover, insurance firms themselves are working to implement a risk-based structural approach to this technological innovation.

The expanding use and collection of so-called 'Big Data' brings about several benefits but creates risks and challenges. The term 'Big Data' refers to large amounts of collected data that need to be stored securely in line with standards and the General Data Protection Regulation (GDPR) and can be analyzed and evaluated to determine trends, consumer behaviors and patterns. There has been an exponential growth in this collected data in the last two decades, driven mainly by technological innovations in communication mediums such as mobile devices, websites, and social media.

The traditional tools to analyze and evaluate this information efficiently are no longer effective, calling out for innovative tools to enhance the analytic capabilities of the insurance firms. All of this should be done in a way that improves the customer experience, by creating more efficiency in the underwriting, pricing and claims process, identifying new marketing opportunities, and streamlining processes and operations. Therefore, recognizing the benefits of this information, data controllers' concerns in this area should focus primarily on protecting consumer privacy.

Moreover, insurance firms can benefit from these new sources of data and analytics by using better information for their risk management/risk taking and underwriting opportunities (that is, giving more attention to trends and expectations, helping to prevent fraud, and identifying areas of significant claims activity).

However, this makes insurance firms the likely target of cyber-attacks, jeopardizing highly confidential personal data. However, on the flipside, InsurTech or rather RegTech firms are introducing innovative technology approaches not only to market and design insurance products to consumers but also to make the processes (underwriting, claims, and distribution) and controls (Risk Management, Compliance, Internal Audit and Legal) more efficient, effective, and compliant.[3]

Therefore, as Kasinow (see footnote 3) suggests, controls should focus on three key areas: (1) consumer privacy; (2) security of customer data; and (3) appropriate use. He notes that managing these risks along with the right application of the data can drive an opportunity for competitive advantage.

Marian[4] proposes a conceptual framework for controlling transactions involving cryptocurrencies that do not impair their innovative potential but disrupts their illicit utilization. Essentially, cryptocurrencies are protocols that allow for the validation of transactions without any intermediation from a trusted third party such as for example a bank, credit card company, escrow agent, or recording agency. Cryptocurrencies reduce transaction costs associated with value transfers, allow access to sectors of the population that do not normally have access to traditional financial institutions, help to avoid the pitfalls of monetary systems, and allow for the

[3] Kasinow (2017).

[4] Marian (2015).

creation of smart contracts that do not rely on financial institutions, lawyers, or accountants for their execution.

In October 2008, Satoshi Nakamoto published a whitepaper called "Bitcoin: A Peer-to-Peer Electronic Cash System" on an internet mailing list and by January 2009, he released the first version of the Bitcoin software on Sourceforge.[5] Although not backed by governments, given that it was a purely digital product, without intrinsic value, nonetheless it traded for goods and services with a real value at a price of just under $10 USD, spiking to over $1000 in late 2013, then spiking to around just over $19,000 by December 2017 and now, until April 2018, hovering between just over $7000 USD and $11,000 USD.[6] Lee[7] notes that the price of Bitcoin appears to be driven by both financial speculation and a rise in ransomware attackers demanding payment in Bitcoin.

However, Marian (see footnote 4) notes that although cryptocurrencies offer tremendous opportunities for innovation and development, they are also uniquely suited to facilitate illicit behavior. Using a basic utility model of criminal behavior as a benchmark, he proposes a control framework wherein costs are imposed on those cryptocurrencies characteristics, which are most likely useful for criminal behavior, for example, anonymity, while maintaining no costs on those characteristics that are at the core of cryptocurrencies' generative potential (specifically, the decentralization of value transfer processes). He proposes as an example of an elective anonymity tax in which one party is not anonymous.

Benton and Radziwill (see footnote 5) note that this thrill around Bitcoin brought a lot of attention to the foundation technological platform: the Blockchain. In recent years, there has been significant hype surrounding the proliferation of Blockchain-based technology. However, it still has to be determined what practical utility might lie in the adoption of Blockchain by insurance firms. The blockchain is capable of supporting more than just the cryptocurrency creation, and forward-thinking software quality professionals are prompting some of the newer development platforms to engage in innovation in this domain. The ability to automate mechanisms of trust without a central authority is the essential virtue of Blockchain, creating a number of efficiencies in human interaction; for example, "smart contracts" that facilitate the exchange of goods and services. It is seen as a disrupter that will "usher in a new wave of efficiency on a scale not seen since the internet boom of the last two decades."[8]

BlockGeeks[9] outline other potential uses of Blockchain technology, which can be of use to insurers. These include helping with the management of governance within firms, supply chain auditing, personal data management, crowdfunding, and anti-money laundering.

---

[5]Benton and Radziwill (2017).

[6]Coindesk.com. Available at: https://www.coindesk.com/price/.

[7]Lee (2017).

[8]Gupta (2017).

[9]BlockGeeks (2017).

Simply put, Blockchain is a shared 'digital ledger', which uses algorithms to verify and record transactions and once this is done, it cannot be changed. A copy of this ledger is maintained by all parties to the transaction and a significant number of ostensibly neutral third parties. This means that it would be very difficult to commit fraud by altering every copy of the ledger globally. This 'digital ledger', has "no central repository or canonical version of the ledger. Every member of the network possesses an equally legitimate version of that ledger."[5] This is mainly what makes Blockchain attractive, however simultaneously challenging to regulators and internal controllers. In fact, as one can note, not all is a bed of roses and some key caveats do exist:

- The existence of a transaction in a Blockchain is no guarantee of representation of the interaction between two persons or organizations, since all may be susceptible to being tricked, careless, or misled into carrying out an otherwise legitimate transaction.
- There is no guarantee of retribution, remuneration, sanction, punishment, or any other consequence, in the event that "*the societal mechanisms of enforcement fail to operate, such as corruption, apathy, or simply being overwhelmed*"—i.e. proof does not necessarily mean that your right can be enforced[5].

Brenton and Raziwill (see footnote 5) note that proper design and implementation is required to minimize these problems. For example, authentication of parties to a transaction should use two, three, or four-factor authentication, as well as IP address verification, and a 48-h waiting period that accompanies email verification. A key development needed involves "automating the means of enforcing or reverting a transaction should one of the parties fail to live up to their side of the bargain" (see footnote 5). Another technological innovation that is transforming the insurance industry with an accelerated pace is cloud computing. This is another delivery model that can facilitate or accelerate business processes. New systems and processes offered by cloud technologies can help develop services and act on insights ahead of the competition. This is a technology that hosts the applications, data storage, and software in a cloud, which can be accessed through the internet so that it is made available to multiple users and reduces the local storage. "*The data or applications could be shared by multiple resources, even at the same time, irrespective of the geography or physical distance. This also addresses the problem of redundancy, improves ease of access, and maintains consistency and reliability of the resources.*"[10]

Cloud technology is being driven in firms mainly because of the cost reduction, business growth, and agility. The shared resources can effectively maximize computer power, allowing firms to expand geographically and introduce new business functions and processes at a faster pace.

In this digitally transforming world, large amounts of data are being captured in real-time through smart devices and chips. As Salam (2012) notes, large amounts of

[10]Sirigada (2015).

data need to be stored and analyzed. Moving to the cloud will allow centralization of data, making it available for all stakeholders across the globe. Insurance firms can enjoy:

- Reduced cost and maintenance
- Infrastructure and location independence
- Multi-tenancy through centralization, utilization and efficiency
- Monitored Performance
- Increased productivity by providing simultaneous access to multiple users to work at the same time
- Reliability of data maintained across all access points
- Improved security through data centralization
- Elasticity as per demand or usage

However, as Salam[11] notes, cloud computing comes with risks and rewards and it could make or break a company, depending on the implementation. The most basic drawback of cloud computing is its dependency on internet infrastructure. Another is the fact that being a centralized system, there is a dependency on a provider of this service. Further, the constant transfer of large amounts of data opens up new avenues for cyber-attack. Better encryption is required, but technology is always evolving and hackers will surely come up with a way to break it. Privacy is another big concern in data integrity since data is handed over to a third party (see footnote 10).

Ralf,[12] in an article in the Financial Times, states that '*Robots learn the business of covering risk*', highlighting that the underwriting of life insurance "*previously requiring an in-depth assessment of the customer by a qualified underwriter using a well-worn set of actuarial models*," is now being replaced by a 'selfie' emailed by customers. He notes that computers analyze thousands of different regions of the face, and with this information plus a few other details received from customers, the computers, in a few minutes can come up with an accurate prediction of life expectancy.

Moreover, he explained how business applied artificial intelligence to aerial photos of farms to help provide crop insurance and machine learning could strengthen the efficiency of the services being offered. However, he also highlights that currently, artificial intelligence is a tool that helps insurance and not a disruptive threat and the focus of technology is on upgrading the data-processing capabilities, or rather improving the way that they communicate internally and with customers.

As one can note, a key feature that all of these technologies have in common is the ability to collect and store large amounts of data. For example, technology can be used in tandem to provide the emergency services with the exact location of the car, the speed of impact, number of persons on board, the gender and ages of those on board, improving the speed of response and maybe increasing the survival chances of those involved. In the same manner, the surveillance capabilities of a drone may

[11]Salam (2012).

[12]Ralf (2017).

allow the police force to proactively prevent and/or detect crimes. However, this might affect the privacy of individuals.

Where there is storage and processing of personal data, controls need to be installed to ensure that this is done and used in a correct and fair manner. Robots are different in terms of how we interact with them, the trust and confidence we might place in them and the expectations we have of how they will learn from the information they are fed. We need to consider how best to protect consumers from malicious operators and the applicable risks of these technologies, ensuring a balance while allowing for innovation.[13]

In summary, as one can note, the insurance market is constantly evolving. Technology has aided to speed this up. Although controls and regulations are needed, there needs to be a balance between the benefits gained from more timely and accurate risk evaluations and pricing, making the industry more efficient—creating new and the innovative models and markets—and the inherent new risks. Technology is only good and reliable as its design and therefore controls and regulations need to protect consumers and the industry against, for example, cyber-attacks, algorithmic bias, red-lining, unclear culpability, opaqueness, and obscurity of increasingly complex processes and reification of autonomous machines. Moreover, ensuring privacy, protection of data, and consumer rights must be maintained at all costs.[14] Controls and regulations, with the assistance of RegTech solutions, need to be as effective and efficient as they are innovative. Table 1 summarizes the challenges, risks, and benefits for controllers and regulators.

Setting the right dose of controls is a daunting task and requires going back to the drawing board whenever new disrupters and forces are encroached to ensure the right balance between controls for a well-functioning consumer protection framework and financial stability and innovation. The control must be technology neutral.

What is the optimal dose of controls that ensures that the insurance industry serves its role in society? As already highlighted above, 'over-controls', which in the context of this article we label as prescriptive controls (i.e. Regulations), impose unnecessary costs, stifle market innovations, and make products and services unaffordable. However, 'lower-controls', which in this article we label as high-level controls (i.e. soft law), may impose safety issues[15] and as noted above, no dose of control is infallible and perfect, each extreme has its strengths and weaknesses. However, the process of ensuring the optimal dose means having to choose among imperfect alternative solutions (given the knowledge of the insurance and technological environment) and rebalancing once new knowledge is obtained. Figure 1 depicts this process. This brings us to the question of the promptness of society, regulators, and the insurance market to react to, implement, and accept these controls.

[13]Holder et al. (2016).

[14]Chandler (2013).

[15]Vaughan (2014).

Table 1 Innovative technologies used/potentially used by the insurance industry

	Benefits	Risks	Challenges for regulation/ control
Big Data (storage of consumer personal data)	Better information for risk-taking/management and underwriting opportunities	Consumer privacy	Partially (already addressed by GDPR)
	Reduction of transaction costs	Cyber-attacks	Yes
	Opportunity for competitive advantage	Illicit utilisation	Yes
Blockchain technology	Automated mechanism of trust	No guarantee of the representation of interaction between two parties	Yes
	No central authority	No guarantee of retribution Anonymity (Laundering and Funding of Terrorism Threat)	Yes
	Enabling smart contracts		Yes
Cloud technology	Ease of access	Dependency on the Internet infrastructure	Yes
	Maintains consistency of the resources	Dependency on the provider service	Yes
	Supports the the reliability of the resources	Cyber-attacks	Yes
	Reduction of costs	Data privacy	Partially (already addressed by GDPR)
	Centralization of data		
	Improvement of operational efficiency and performance		
Artificial intelligence	Ability to collect and store large amounts of data	Consumer privacy	Partially (already addressed by GDPR)
	Ability to deliver precise and timely information	Security of consumer data	Yes
		Appropriate use of information	Yes

Source: Table elaborated by the authors of this Chapter

3 Behavioral Insights

The existing debate surrounding the design of appropriate regulations and control frameworks for technological innovation can be described as a delicate balancing act between the social costs emanating from high-level or laissez-faire control, and the

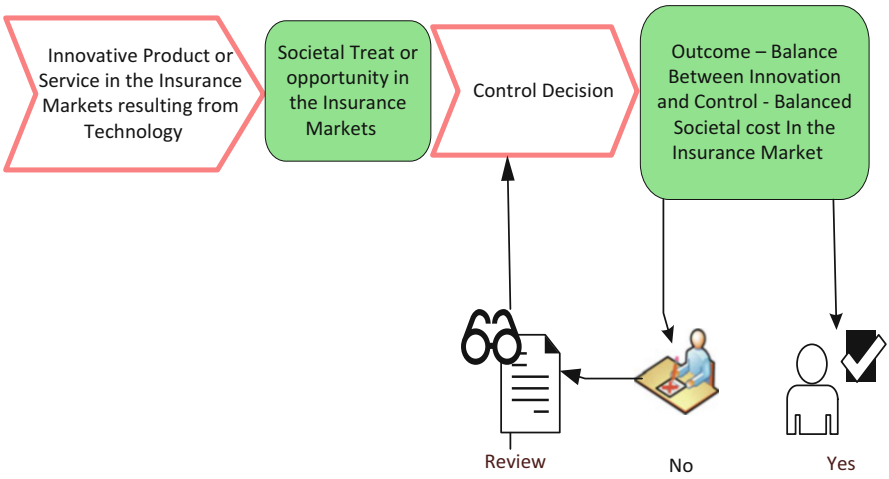

Fig. 1 The strategy to developing and calibrating controls and regulations. Source: Figure elaborated by the authors of this Chapter

social costs from prescriptive impositions, which may stifle private initiative.[16,17] In their now-infamous report on the conduct of the New York Federal Reserve in the wake of the 2008 Financial Crisis, Beim & McCurdy[18] found significant issues with banking regulations in the U.S., which in turn helped to foster a culture of regulatory capture. On the other hand, Duff & Phelps's Global Regulatory Outlook[19] reports that financial institutions in Europe on average spend 4% of total revenue on compliance, with this figure expected to increase to 10% by 2022. Therefore, the onus is on regulatory institutions to ensure that controls on new technologies foster trust and security in the financial services industry, without imposing unnecessary financial burdens.

Amidst these competing arguments, the rise of behavioral finance has introduced a new way of looking at the formulation of regulations and controls within the financial industry. Firmly rooted in the cognitive psychology literature popularized by Nobel laureates Kahneman & Tversky[20] and Thaler,[21] these ideas provide regulators with a new yet complementary set of tools that can be used to improve the design and implementation of control frameworks. For example, Herbert Simon's seminal work on bounded rationality[22,23] and Newell & Simon's work[24]

[16]Djankov et al. (2003).
[17]Shleifer (2005).
[18]Beim and McCurdy (2009).
[19]Duff & Phelps (2017).
[20]Kahneman and Tversky (1979).
[21]Thaler (1980).
[22]Simon (1955).
[23]Simon (1957).
[24]Newell and Simon (1972).

has helped to shed light on the various cognitive constraints that may inhibit individuals from making optimal decisions, because of limited attention, lack of time availability, problems dealing with uncertainty, etc. This has also been linked to the oft-observed phenomenon of choice overload, whereby people make suboptimal choices when faced with a large number of options,[25] together with a general distaste or aversion for ambiguity.[26]

These findings have important implications for regulators since they suggest that any control frameworks should prioritize simplicity and clarity as opposed to stringency. Prescriptive controls may work better if they help to reduce ambiguity and simplify compliance to certain goals like transparency and security while limiting the options available to reach these aims, although clearly, such an approach is not without its potential pitfalls. Another two behavioral phenomena that have received significant academic attention are status quo bias or the notion that people are often reluctant to independently seek change because of inertia and the costs involved,[27] as well as present bias, which describes people's tendency to focus on short-term gains rather than longer-term well-being.[28] Again, both of these processes suggest that consumers and organizations alike require external pressure and inducement to alter their behavior, which is more consistent with a prescriptive approach to internal controls.

Given the inherent complexity entailed by certain technological innovations, including Blockchain, perhaps a natural presumption would be to impose controls to ensure maximum information disclosure to clients to assist in their financial decisions, as suggested by standard rational choice theory. However, research suggests that buyers may be overwhelmed when presented with a large amount of information, particularly if their initial level of knowledge is low, leading them to select the so-called 'path of least resistance' which in turn makes them susceptible to manipulation by the seller.[29] These findings are already having a tangible impact on financial regulation—for example, the UK's Financial Conduct Authority (FCA) recently opted against sweeping regulations intended to increase information disclosure, opting instead to focus on various aspects of seller behavior like placing undue pressure on clients and the design of financial products.[30]

Nonetheless, it is also important to acknowledge the various potential pitfalls associated with more prescriptive control and regulatory framework. Apart from the typical issues surrounding complexity and resistance to change, findings from behavioral finance also suggest that prescriptive as opposed to higher-level controls may alienate organizations by effectively crowding-out private compliance incentives, which may actually backfire and result in superficial compliance.[31] The reason

[25] Iyengar and Lepper (2000).

[26] Ellsberg (1961).

[27] Samuelson and Zeckhauser (1988).

[28] O'Donoghue and Rabin (1999).

[29] Agnew and Szykman (2005).

[30] Dambe et al. (2013).

[31] Bénabou and Tirole (2006).

for this is that organizations may have initially sought their own internal policies and controls to cultivate a good reputation amongst customers and ensure maximum satisfaction, both of which are internal motivators and act as signals to attract and retain clients. With the imposition of externally-mandated prescriptive controls, these signals are diluted, thereby paradoxically reducing the incentive to comply.[32] Thus, what emerges from the various findings in the behavioral finance literature is the importance of clarity and simplicity of any controls framework, striking a balance between consumer protection through careful monitoring of seller practices while ensuring that these controls do not stifle private initiatives and incentives.

4 Controls vs Technological Innovation

To maximize on global innovation, the insurance industry will need to develop mechanisms to encourage controls that are more contributing and less detracting to innovation. Robust innovation is essential for economic growth and social progress. For example, progressive contributing controls can be policies to support education and research.[33] These, in turn, will ensure the presence of features required for economic stability, amongst other, security, uniformity, acceptability, trust, profitability, competition, enforceability, affordability, and transparency, if the research and education is directed correctly and to the right sources. Therefore, we see that innovation does not 'fall from the sky', but is a product of complex control policies and strategies that affect the capacity and ability of both private and public actors to effectively innovate.

The basic premise of this control versus innovation is that all of these strategies for control of innovation due to technology in insurance markets are imperfect and that optimal institutional design involves a choice among these imperfect alternatives. This 'control theory' specifically recognizes a basic trade-off between two social costs of each choice of control: Prescriptive Control and High-Level Control. Prescriptive controls to try and achieve more security, uniformity acceptability, trust, profitability, competition, enforceability, affordability, and transparency but may stop innovation efficiency and result in more bureaucracy and more costs. On the other hand, high-level controls may result in more innovation, less uniformity but still achieve the results of prescriptive controls from self-regulation while being more efficient. However, this depends much on the culture of the insurance industry and may result in being more vulnerable and less secure.

This dilemma suggests that we should as much as possible balance out between the social losses (for example of security, uniformity, acceptability, trust, profitability, competition, enforceability, affordability, transparency, and innovation) due to prescriptive controls and social losses due to high-level controls to arrive at a control

[32] Ariely et al. (2009).

[33] Ezell et al. (2016).

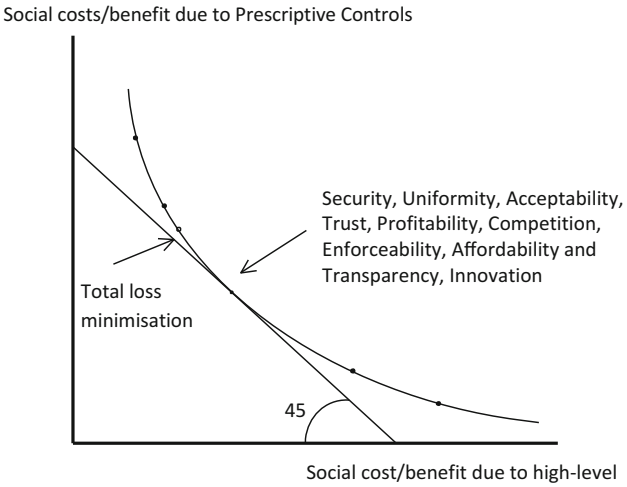

Fig. 2 The control efficient frontier. Source: Figure elaborated by the authors of this Chapter

framework efficient frontier, which provides us with the most effective and efficient imperfect control alternative.

In fact, one of the lessons learnt from the large losses and crisis in the financial and economic areas is that regulators will do mistakes. There is no perfect guaranteed regulatory system. Regulations may help flag things to regulators but fail to flag most issues. In addition, what if they flag them, but the regulator draws the wrong conclusions about how to address the issue or the regulation is so prescriptive that it becomes difficult to address the issue in the correct manner. Moreover, regulations and their respective guidelines may require the collection of loads of unnecessary information, tending to lead to familiarity or/and alienation about the behavior of the firm (see footnote 15) (Fig. 2).

5 Uniformity of Regulations vs Technological Innovation

Another concern is the central regulation system calling for uniform Insurance Regulations across Europe and the United States. The advantage of such a system is that since decisions are decentralized, issues can constantly emerge from these different countries and states, uncovering, what is known in risk management as ‘unknown uncertainties’, issues that certain countries might not have ever been able to experience and identify. Therefore, uniformity and centralization of decisions on regulations will help identify these ‘unknown uncertainties’ and create an appropriate antidote. However, on the flip-side, is that this same advantage gives rise to other problems, such as bureaucracy at the detriment of efficiency in decisions and implementation because of the different cultures and terminology and the various

discussions before implementation. This seemingly chaotic situation slows down the development of technological innovation but allows for the understanding and adaptation and to identify any unintended consequences to ensure less social costs (see footnote 15).

6 Conclusions

The proliferation of innovative technologies in financial services, including the insurance industry is already significant and constantly growing. The use of innovative technologies such as Big Data, Blockchain technology, cloud technology, and artificial intelligence brings both benefits and additional risks. Storage of consumer personal data (Big Data) ensures better information for risk-taking/management and underwriting opportunities, allows reduction of transaction costs and creates an opportunity for competitive advantages. Blockchain technology in the context of the insurance industry provides an automated mechanism of trust without any central authority, enabling smart contracts. Wider use of cloud computing maintains consistency of the resources and supports the reliability of the resources, centralization of data and reduction of costs, as well as improvement of operational efficiency and performance. Artificial intelligence allows for collecting and storing large amounts of data, delivering precise and timely information for the insurance products. Although the issues relating to consumer data privacy are partially covered by the new General Data Protection Regulation (GDPR), the use of innovative technologies creates additional risks related to consumer data privacy, illicit utilisation, money laundering, and cyber-attacks.

Innovation is a product of complex control policies, and different control strategies can have a real effect on the capacity and ability of both private and public actors to effectively innovate. To maximize on global innovation, the insurance industry will need to develop mechanisms to encourage controls that facilitate rather than hinder innovation, for example, progressive contributing controls such as policies to support education and research. If the research and education is directed correctly and to the right sources, these will ensure the presence of features required for economic stability and long-term security, while creating a virtuous cycle for innovation to prosper.

The basic premise of this control versus innovation dilemma is that all of these strategies for control of innovation due to technology in insurance markets are imperfect. The optimal institutional design involves a choice among these imperfect alternatives. This 'control theory' specifically recognizes a basic trade-off between two social costs of each choice of control: prescriptive control and high-level control. Prescriptive controls to try and achieve more security, uniformity, acceptability, trust, profitability, competition, enforceability, affordability, expectations, and transparency; but may stop innovation efficiency and result in more bureaucracy and higher costs.

On the other hand, high-level controls may result in more innovation and less uniformity, but still, achieve the results of prescriptive controls from self-regulation while being more efficient. Nonetheless, this depends much on the culture and the maturity of the insurance industry, stakeholders, and the customers, and may result in more vulnerability and less security, if analyzed and calibrated incorrectly. Here, RegTech can help to offer solutions to collect, analyzes, and store information efficiently to enable quick and knowledgeable decisions by controllers/regulators on the dose of controls to prescribe. However, in this ever-changing world characterized by information asymmetries, the implications of new technologies on loss frequencies and severity, and the increasing dependencies of systems through connectivity must be considered. In particular, efficiently managed controls are required that are flexible enough to allow for quick recalibration whenever this is deemed necessary, perhaps with Artificial Intelligence or other RegTech solutions. In addition, some form of experimentation needs to be allowed, providing for a dynamic and quick responsive regulatory system.

As one can note from above, dealing with the balance between highly prescriptive controls and social losses from high-level controls leaves an impact on society and any decisions taken may have a detrimental effect on social welfare. Therefore, it is important that the calibration/rebalancing trigger should be left in the hands of efficient authorities, who are fast to address all the stages as suggested and noted in Fig. 1 above.

The dilemma that currently exists is whether we should deal with this situation by addressing issues centrally and pushing for a level playing field, as is currently being done in Europe and the United States. There is no correct way of doing this but the advantages gained from the system are many since one can specialize in a specific field of knowledge and disseminate such information among the rest. On the other side is the argument that we are dealing with very different cultures and a 'one size fits all' can never be the correct answer. In addition, the insights provided by the emerging field of behavioral finance yield decidedly-mixed prescriptions, since although uniformity may facilitate and automate decision-making by removing ambiguities, these controls may also reduce compliance by crowding-out private incentives and initiatives.

Therefore, as much as we can see, the value in having a central system and 'level playing field' to identify issues (unknown uncertainties) and help address these together, the arguments described in this paper point towards a non-highly prescriptive system of regulation within boundaries embedded on specific common requirements. There is a need to have the basic requirements set in stone, but with the liberty for each country to address these within boundaries and in the light of the country's prevailing cultural landscape.

References

Agnew JR, Szykman LR (2005) Asset allocation and information overload: the influence of information display, asset choice, and investor experience. J Behav Finance 6(2):57–70

Ariely D, Bracha A, Meier S (2009) Doing good or doing well? Image motivation and monetary incentives in behaving prosocially. Am Econ Rev 99(1):544–555

Beim D, McCurdy C (2009) Report on systemic risk and bank supervision. Federal Reserve Bank of New York, Discussion Draft. Available at: http://www.propublica.org/documents/item/1303305-2009-08-18-frbny-report-onsystemic-risk-and.html. Accessed Jan 2018

Bénabou R, Tirole J (2006) Incentives and prosocial behavior. Am Econ Rev 96(5):1652–1678

Benton MC, Radziwill NM (2017) Quality and innovation with blockchain technology. Software Quality Professional, December. Available at: https://qualityandinnovation.files.wordpress.com/2018/01/2017-benton-radziwill-quality-and-innovation-with-blockchain-technology.pdf

BlockGeeks (2017) What is blockchain technology? A step-by-step guide for beginners. Available at: https://blockgeeks.com/guides/what-is-blockchain-technology/

Chandler D (2013) Technological or media determinism. Available at: http://www.aber.ac.uk/media/Documents/tecdet/tecdet.html

Coindesk.com. Available at: https://www.coindesk.com/price/

Craig CJ (2017) Technological neutrality: recalibrating copyright in the information age. Osgoode Legal Studies Research Paper No. 5/2017. Available at: https://doi.org/10.2139/ssrn.2852385

Dambe K, Hunt S, Iscenko Z, Brambley W (2013) Applying behavioural economics at the Financial Conduct Authority. Occasional Paper 1, FCA

Djankov S, Glaeser E, La Porta R, Lopez-de-Silanes F, Shleifer A (2003) The new comparative economics. J Comp Econ 31(4):595–619

Duff & Phelps (2017) The global regulatory outlook 2016. Duff & Phelps, New York

Ellsberg D (1961) Risk, ambiguity, and the savage axioms. Q J Econ 75(4):643–669

Ezell SJ, Nager AB, Atkinson RD (2016) Contributors and detractors ranking Countries' impact on Global Innovation. Information Technology & Innovation Foundation (ITIF), January 2016. Available at: http://www2.itif.org/2016-contributors-and-detractors.pdf

Gupta V (2017) A brief history of blockchain. Harv Bus Rev. February 28, 2017. Available at: https://hbr.org/2017/02/a-brief-history-of-blockchain

Holder C, Khurana V, Harrison F, Jacobs L (2016) Robotics and law: key legal and regulatory implications of the robotics age (Part I of II). Comput Law Secur Rev 32:383–402

Iyengar S, Lepper M (2000) When choice is demotivating: can one desire too much of a good thing? J Pers Soc Psychol 79:995–1006

Kahneman D, Tversky A (1979) Prospect theory: an analysis of decision under risk. Econometrica 47:263–291

Kasinow R (2017) Key regulatory challenges facing the insurance industry in 2017, Americas FS Regulatory Center of Excellence. KPMG. Available at: https://assets.kpmg.com/content/dam/kpmg/us/pdf/2017/04/facing-the-insurance-industry-in-2017.pdf

Lee TB (2017) Bitcoin's price keeps breaking records. Here's what's driving its growth. Vox, June 6, 2017. Available at: https://www.vox.com/new-money/2017/5/26/15687062/bitcoin-bubble-explained

Marian OY (2015) A conceptual framework for the regulation of cryptocurrencies (October 23, 2014). Univ Chic Law Rev Dialogue 82:53. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2509857

Newell A, Simon HA (1972) Human problem solving, vol 104, no 9. Prentice-Hall, Englewood Cliffs

O'Donoghue T, Rabin M (1999) Doing it now or later. Am Econ Rev 89(1):103–124

Ralf O (2017) Insurance: Robots learn the business of covering risk. Financial Times, May 16, 2017. Available at: https://www.ft.com/content/e07cee0c-3949-11e7-821a-6027b8a20f23

Romānova I, Grima S, Spiteri J, Kudinska M (2018) The Payment Services Directive 2 and competitiveness: the perspective of European Fintech companies. Eur Res Stud J XXI(2):5–24

Salam A (2012) The risks and rewards of cloud computing. August 13, 2012, CloudBuzz. CloudTweaks.com. Available at: https://cloudtweaks.com/2012/08/the-risks-and-rewards-of-cloud-computing/

Samuelson W, Zeckhauser RJ (1988) Status quo bias in decision making. J Risk Uncertain 1:7–59

Shleifer A (2005) Understanding regulation. Eur Financ Manage 11(4):439–451

Simon HA (1955) A behavioral model of rational choice. Q J Econ 69(1):99–118

Simon HA (1957) Models of man; social and rational. Wiley, Oxford, England

Sirigada AR (2015) Eight reasons why Insurance Companies should move to Cloud. 19th Jun '15, 11:23 PM in Banking/Finance. Available at: http://bigdata-madesimple.com. http://bigdata-madesimple.com/eight-reasons-why-insurance-companies-should-move-to-cloud/

Thaler R (1980) Toward a positive theory of consumer choice. J Econ Behav Organ 1(1):39–60

Vaughan TM (2014) Observations on insurance regulations – uniformity, efficiency, and financial stability. In: Biggs JH, Richardson MP (eds) Modernizing insurance regulators, New York University Stern. Wiley Finance Series, ch. 4, pp 31–41

Part II
Insurance Contracts in a Digitalized World

Smart Contracts in Insurance: A Law and Futurology Perspective

Angelo Borselli

1 Introduction

The interlinkage between technology and insurance, commonly referred to as "InsurTech", has clearly gained momentum, in the wake of a trend that has spread, more generally, throughout the entire financial services sector. The number of venture capitalists investing in InsurTech has made a fourfold increase from 53 in 2012 to 217 in 2017.[1] In 2015, investments into technology-enabled insurance solutions came to $2.7 billion, registering a significant year-over-year growth since 2011.[2] After a slowdown in 2016,[3] the total value of funding reached $2.32 billion in 2017, which is a 32% increase on the previous year,[4] and the amount invested is expected to increase even more as technology has the potential to bring innovation benefits in insurance.[5] Smart contracts are undoubtedly among the major innovations that are taking place in the insurance sector. From a legal perspective, the term "smart contract" refers to the possibility of representing a legal contract in programming code that gets automatically executed on a blockchain or other

[1] Willis Towers Watson Securities (2018), p. 5.

[2] Catlin et al. (2017); OECD (2017), p. 13.

[3] IAIS (2017), p. 14 (noting that the decline in funding in 2016 was mainly due to uncertainties related to global market conditions).

[4] Jubraj (2018).

[5] OECD (2017), p. 14 (noting that some of the larger insurers have set up specific funds to invest in InsurTech, and that the likelihood of greater investments in years to come is high).

A. Borselli (✉)
Bocconi University, Department of Legal Studies, Milan, Italy

University of Connecticut School of Law, Hartford, CT, USA
e-mail: angelo.borselli@unibocconi.it

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_5

distributed ledgers. In principle, the contract becomes self-executing, since once a pre-programmed condition is met the relevant action is performed.

The connection between automation—which is the hallmark of smart contracts—and insurance is intriguing for its possible impact particularly in terms of operational efficiencies and certainty in the implementation of transactions, but also as regards the legal issues that it poses, as smart contracts have the potential to transform how insurance transactions are carried out.

This paper investigates the scope for the application of smart contracts in insurance both in the near and longer term, exploring the legal challenges that they raise. In particular, after identifying potential applications of smart contracts in the near-term and examining how they may operate at law, the paper discusses the prospect of the automation of the entire insurance contract in the farther-distant future. To this end, it adopts what might be broadly regarded as a futurology perspective, building on current technological developments to consider possible future advances in the use of smart contracts and explore how smart contract automation will interact with law.

The study rests on both practical and theoretical grounds. From a practical point of view, to investigate the innovation potential inherent in the use of smart contracts in insurance is clearly relevant. Smart contracts along with the underlying blockchain technology are viewed, in fact, as among the most important innovations since the Internet and they may have a significant impact on insurance by automating several processes, such as the underwriting of policies, claims handling and payouts. The paper, however, is also grounded on a theoretical and more systematic perspective. The very idea of smart contracts and the resulting prospect of automating the entire insurance contract need to be confronted with the theory of incomplete contract. As complete contracts, that specify the obligations of the parties in each possible state of the world, are not feasible, standards are generally needed to consider the specific circumstances of a case. Automation, however, typically hinges on rules, especially rules that can be expressed in a conditional logic, while standards for their inherent nature are flexible and can hardly be coded, thus being crucial to consider in the first place to what extent the insurance contract can be automated and the conditions for the possible automation of the entire contract. Moreover, to suggest another theoretical and systematic implication, it is worth noting that smart contracts bear on the essence of an insurance contract—the insurer's promise to pay. By automating processes and ensuring the payment of claims once the relevant conditions are triggered, smart contracts can reinforce the insuring agreement and transform the relationship between the insurer and the insured.

The paper proceeds as follows. After this introduction, Sect. 2 discusses the phenomenon of smart contracts by exploring their basic technical functioning, as any study of the legal implications of smart contracts needs to build on an understanding of their nature from a technical point of view. Section 3 addresses the role that smart contracts are likely to play in insurance in the near-term, also by discussing some of the projects that are currently being implemented in the industry. Section 4 expands on this, discussing the prospect of the extension of the role of smart contracts to potentially automate the entire insurance contract. Section 5 concludes.

2 The Technical Functioning of Smart Contracts

Computer scientist Nick Szabo was the first, in 1996, to refer to smart contracts as innovative contracts that are "smart"[6] since they are "far more functional than their inanimate paper-based ancestors." According to Szabo, a smart contract is "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[7] Although there is no settled definition of the term, a smart contract can be considered as a contract that can be automatically enforced in accordance with pre-defined conditions.[8] The typical and basic example is a vending machine: once a person has satisfied the conditions of the contract by inserting money into the machine, the machine automatically performs its obligation and delivers the product.[9]

Smart contracts have the potential to go beyond vending machines and apply to all sorts of contracts that are capable to be coded. In this perspective, a distinction can be drawn between smart contracts *stricto sensu* (a.k.a. "smart contract code")—in computer science, basically, computer code executed on a blockchain—and smart contracts in law (a.k.a. "smart legal contracts")—contract terms represented in programming code, capable of being self-executing.[10] This distinction is relevant to point out possible translation issues from the natural and legal language into the code operational semantic, and possible consequent limits on representing a legal contract in programming code. To the extent that all or part of a traditional legal contract can be expressed into code, the contract may become self-executing, i.e. a smart contract.

The growing attention that smart contracts have recently got follows the wake of the latest developments in blockchain, as smart contracts are built on top of this technology and their potential clearly depends on the blockchain infrastructure.[11] The computer code, in fact, is digitally recorded on a blockchain or other distributed ledgers and runs on the computers connected to the network through the Internet (the so-called blockchain nodes),[12] thus implementing the contract.[13] Although the type of code may vary depending on the blockchain protocol on which it has to be

[6]The Oxford English Dictionary defines the word "smart", in relation to a device, as "programmed so as to be capable of some independent action."

[7]Szabo (1996).

[8]*See* Clack et al. (2017), p. 2.

[9]Szabo (1996).

[10]*See* Clack et al. (2017), p. 2.

[11]*See generally* Gatteschi (2018), p. 1; Willis Towers Watson (2016).

[12]Each node keeps a complete history of the transactions executed on the blockchain. Transactions are grouped together in data structures called blocks, and each block incorporates a unique reference to the prior block, thereby making it exceptionally difficult to alter an entry in the blockchain. *See* Amuial et al. (2016), § 1.2.

[13]Once the smart contract code has been programmed, the execution of the smart contract cannot be prevented, unless provided for in the code: Wright and De Filippi (2015), p. 35.

executed, suffice it to say that there are protocols such as Ethereum that have turing-complete programming capabilities, thereby supporting programming languages that have no limitations in terms of the logic that can be implemented and that can serve virtually any smart contracts (so-called "general purpose programming languages").[14]

In principle, the functioning of smart contracts is straightforward and fits into the scheme "if A, then B", that is, if a certain predetermined event or condition occurs, a consequence automatically follows. Somehow simplifying, for example, in the case of automobile insurance, an insurance company may create a smart contract providing that the policyholder has to be indemnified whenever a damage covered under the policy occurs. If a claim is filed and the insurance company approves it, the smart contract automatically credits the policyholder's account with the amount due under the policy. Every single step outlined above might be automated so that the claim can also be both automatically filed through black boxes or other devices that are incorporated in the car, registering the accident and notifying the insurer, and potentially even automatically assessed. Recent news, for instance, is that Liberty Mutual is engaged in developing automotive apps that would allow to assess car damages in real-time using the camera of a smartphone. The app uses anonymised claims photos to make a comparative analysis of the user's damage and provide a specific repair cost estimate. In the longer term, this might result in a reduction of the costs of claim adjustments and possibly in more efficient claim processes.[15] Compared with existing reality, in this scenario all processes would be automated since if the pre-programmed conditions are met (e.g. the claim is approved and the damage quantified) the smart contract automatically performs the relevant action (i.e. the indemnification of the policyholder). Nuances might be added to this example and a more sophisticated smart contract might be structured, envisioning a future where, with the advent of driverless cars, the smart contract might even direct the car itself to an accredited garage for its repairment.

Obviously, the potentials of smart contracts can be maximised if they interact with external information provided by trusted third-party oracles or Internet of Things (IoT) devices that connect to the Internet through incorporated sensors, enabling information gathering.[16] The best known examples are data collected

[14]Amuial et al. (2016), §§ 2.3, 2.20 (explaining that often "object-oriented" languages are used, which follow a design pattern that is built with objects like, for example, a digital representation of a car or of a human being. Objects can store relevant attributes such as the car model, the manufacturer, the production year, etc.); Cuccuru (2017), p. 186. *See also* Wright and De Filippi (2015), p. 12 (noting that some open source projects aim at developing programming languages for ever more sophisticated smart contracts).

[15]Sennaar (2017).

[16]U.S. Federal Trade Commission (2015), p. 5 (noting that IoT devices can be defined as the connection of physical objects to the Internet and to each other through embedded sensors and wireless technologies, creating "an ecosystem of ubiquitous computing"); O'Brien (2016), p. 12 [noting that the key IoT areas are: wearables (e.g. smart wrist bands), connected cars, connected homes, connected cities, and industrial sectors such as transportation, oil and gas, and healthcare].

from devices embedded into motor vehicles (so-called "telematics insurance") or sensors placed in private homes or business premises.[17] The need, however, to ensure the reliability of the data gathered is clear as the smart contract automatically performs based on the inputs it receives and corrupted information would negatively affect the desired outcome.[18]

Increased functionality, however, generally requires more programming code to be executed on the blockchain, and this may result in a higher likelihood of code errors and possible incidents that may pose threats to the security and reliability of the smart contract innovation. The implosion of The DAO, one of the earliest decentralised autonomous organisations, provides a good example of this risk, as in that case a flaw in the smart contract code led to a multimillion-dollar loss.[19] As the analysis below will show, the automation inherent in smart contracts can bring several possible benefits to insurance in terms, for example, of higher efficiency, reduction in costs and human errors, fraud detection, but the need to continue developing adequate operational standards remains strong,[20] since any further advance in the smart contract innovation will necessarily come from enhancements to the security of the underlying technology and coding system. In this perspective, initiatives such as the B3i consortium that brings together (re)insurers and brokers from all over the world to develop common operational standards for the application of blockchain and smart contracts to the (re)insurance industry[21] are undoubtedly worthy of attention as they can enable further advances in the use of this technology and promote convergence in the insurance industry. Regulatory sandboxes can also play an important role, allowing innovators to test their products in a controlled environment under the supervision of the competent authorities.

3 Near-term Applications of Smart Contracts to Insurance

Traditionally the insurance industry has not been quickly responsive to recognising and exploiting the value of technological innovations, but that tendency seems now moving in the opposite direction and the increasing traction recently gained by smart contracts and the underlying blockchain technology raises the question of what applications smart contracts can actually have.

[17] OECD (2017), p. 27.

[18] *See* Amuial et al. (2016), § 2.5 (emphasising that oracles must be trusted entities that submit the information relevant to the smart contract through cryptographically signed messages).

[19] Coppola (2016); Amuial et al. (2016), § 2.3.

[20] *See generally* IAIS (2017), p. 7.

[21] The Blockchain Insurance Industry Initiative (B3i) was formed in 2016 by 15 global (re)insurance companies mainly to explore and test the potential of blockchain in insurance. In 2018, the founders of B3i incorporated B3i Services AG in Zurich, to commercialise blockchain solutions for the (re) insurance industry.

To begin with, the most typical and immediate application seems to lie in the automation of claims handling and payouts, as these processes rest on the same conditional logic that smart contracts use, and therefore they can be easily automated in line with the "if/then" scheme outlined above, so that *if* the risk covered under the policy occurs, *then* the smart contract automatically indemnifies the insured. Current pilot projects are mainly focused on property and casualty insurance, but the prospect of smart contracts in life insurance is also relevant as the insured event is capable of being represented into a binary data form. In general, the examples of possible use cases can be many, and virtually every insurance payout might be automated, although automation is truly appreciated where the insured event can be easily ascertained as the advantage is likely to be lower if more complex assessments are required and third parties need to be involved in the process. In addition to the insurance company and the insured, in fact, other parties, such as assessors, mechanics, technicians, may interact with the smart contract and add relevant transactions to the blockchain ledger, under the terms of the insurance contract. For example, it is possible to involve a certified mechanic to provide for automatic indemnity to the policyholder only if the vehicle is repaired at that mechanic, with the mechanic itself confirming this by sending a transaction to the smart contract.[22] Or, to make another example, the smart contract may be programmed to trigger different deductibles depending on whether the repairs are carried out by certain repair shops, with the repair shops that have to add the transaction to the blockchain ledger. Obviously, especially where the transactions have to be manually sent to the ledger, the more the transactions are the less instantaneous the execution of the smart contract is going to be, so that the result would be more what might be called a 'mechanised contract' based on manual inputs rather than a real automated contract.

When the payment is triggered by inputs deriving from trusted oracles or IoT devices, however, the results can be truly surprising. For instance, this is the case of the "smart" flight insurance products developed by the start-up InsurETH or by AXA that created smart contracts capable of automating claims and refunds for flight delays or cancellations, relying on flight status information provided by oracles. The impact of this innovation is significant as data shows that only a very minor percentage of policyholders actually file flight insurance claims, while by using parameters to trigger the performance of the contract, all policyholders would be automatically compensated as soon as a cancellation or a delay is reported.[23] The connection of smart contracts with the IoT is also interesting, even more so since in the near future virtually all physical objects in the world are expected to be connected to the Internet.[24] Devices placed in private homes, automobiles and other vehicles, or business premises can transmit real-time information about, for example, water or gas leaks, fires, thefts and other accidents triggering automating claim processing,

[22]Gatteschi (2018), p. 6.

[23]McKinsey&Company (2017), p. 4; AXA (2017).

[24]Amuial et al. (2016), § 2.17; Deloitte (2018) (also noting that 600 million smart home devices are expected to be in use by 2021).

but also allowing for immediate intervention and assistance,[25] thereby possibly reducing the loss and the repair costs.[26] An illustrative example is given by the UK startup Neos that provides a connected home insurance service, offering continuous assistance through smart sensors that can alert homeowners to problems via a smartphone app to prevent possible damages. Incidentally, it is worth noting that this can affect the insured's duty to mitigate the damage as traditionally understood since, to the extent that insurance companies will be responsible to provide the IoT devices to the insured and ensure their proper functioning and continuous monitoring, it is reasonable to conclude that the above-mentioned duty will become larger in scope as not only the insured but also the insurer would be in the position to take reasonable measures to avoid the loss and mitigate damages.[27]

Micro-insurance products that typically allow low-income people in developing countries to have access to insurance services are also likely going to benefit from the use of smart contracts, as these products, for their very nature, call for low transaction costs and simplicity in claim processing. Payouts triggered by publicly available weather data are already a reality in the case of crop-insurance or weather-based insurance more generally.[28] Moreover, index-based agricultural insurance permits to determine payouts using indexes that are correlated with losses caused by insured risks such as floods or pests, considering different variables such as precipitation, vegetation levels, woodland management, and it has emerged as a way to increase availability of coverage for smallholders. By relying on these indexes, in fact, insurers can issue compensation payments without having to assess the loss at the single farm level, and once the relevant data are transmitted to a smart contract, the entire process would be automated.[29] The advantages deriving from the use of smart contracts in these cases are self-evident, considering the benefits that automation would bring in terms of making claim processing faster and cheaper, and enhancing trust between the insurance providers and the micro-insurance clients. Moreover, the use of smart contracts on digital platforms may foster direct sales channels particularly for less complex coverages such as auto insurance and for mass insurance and micro-insurance products, with possible reduction in their costs.[30]

In addition, the potentials of smart contracts can also extend beyond claims handling and payouts to include the automation of underwriting. In particular,

[25]Some devices, in fact, may interact with the physical world by receiving inputs from Internet applications. For example, a sensor may monitor a motor's internal temperature and send the data to an application, so that if the temperature gets too high, the application would send a command to the motor to cool it down. *See* Amuial et al. (2016), § 2.17; OECD (2017), p. 15.

[26]Willis Towers Watson (2016), p. 3.

[27]The slogan on the website of Neos, the home insurance start-up mentioned above in the text, is quite telling on this point as it states "[n]o matter where you are in the world, you're connected to home, giving you the confidence and comfort that Neos is looking after the place that matters most.". *See* Neos (2018).

[28]Willis Towers Watson (2016), p. 2.

[29]Hernandez (2017).

[30]*See* Willis Towers Watson (2016), p. 3.

smart contracts can play an important role in setting rates, by relying on big data analytics and access, for example, to usage and demographic data. In the auto-insurance industry, GPS data might be used to collect premiums based on the kilometers driven. Devices placed in the vehicles might also gather information on how fast, or when a person drives, or about her braking patterns to determine and charge personalised, and possibly lower, premiums. Further, it is interesting to note that some dental insurance contracts might adjust premiums automatically depending on the brushing habits of the insured.[31] This is the case of the smart toothbrush developed by the dental insurer Beam, which tracks all the oral hygiene of a person and uses that information to charge rates for dental insurance plans.[32] In all these cases, a smart contract would read the data and automatically compute the premium or apply discounts or extra charges, by performing a risk assessment according to the programmed code.[33] The same might be true for smart wearable devices that may transmit data to the smart contract about, for example, health and fitness conditions. More accurate rates thus might be set and, in principle, there could be the possibility of real-time pricing that would clear the way for pay-as-you-go types of coverage.

It is also possible to assume that in a less-near future, insurance companies would be interconnected with several accredited third parties, institutions and authorities that would record relevant information on a blockchain ledger, so that premiums might be automatically calculated by smart contracts receiving inputs, for example, from hospitals and other medical centres that would transmit official records of treatments, other insurance companies that may send data about previous claims of the applicant, police departments sending information about criminal records.[34] Privacy concerns and data protection are clearly among the main obstacles to this scenario, other obstacles being the need to ensure the quality of the data and to systematically involve as many different actors as possible to gather enough data and make this scenario feasible.

Moreover, the very decision on whether to underwrite a certain risk might be automated. In the context of peer-to-peer insurance where typically insureds self-organise to pool funds and administer their own coverage, vote-based oracles connected to smart contracts can determine whether to assume a certain risk based on the majority decision of the group participants.[35] Even data from social networks might be used to this end, as in the case of Dynamis, a U.S. company that has implemented a smart contract for peer-to-peer insurance that provides supplementary unemployment insurance by using data from LinkedIn to verify a person's identity and employment status, and automate underwriting and claims handling.[36]

[31] Casey and Niblett (2017b), p. 102.

[32] Farr (2018).

[33] *See* Gatteschi (2018), p. 8.

[34] Gatteschi (2018), p. 8.

[35] Willis Towers Watson (2016), pp. 2 f.

[36] Huckstep (2016).

More generally, a major impact on the automation of both underwriting and claim processing is likely to result from the application of artificial intelligence to smart contracts. As it is well-known, "artificial intelligence" generally refers to the capacity for a machine to have human-like abilities such as reasoning, learning, decision-making, and the fact that today machines are able to perform ever more tasks that normally require human intelligence is undisputed.[37] This holds true in insurance as well, where artificial intelligence is applied more and more to predict premiums and claims and to permit fast settlements and targeted investigations, since it may allow to go through a large number of claims and select those that require further investigation before being paid or settled, thereby contributing to curb fraud[38]—which is notoriously a severe problem for insurance companies.[39] In this scenario, to the extent that artificially intelligent algorithmic systems can make underwriting and claims handling decisions, a smart contract would receive the relevant input and execute the decisions, thus automating these processes.

As the discussion above shows, in the near-term, most probably in the next 5 years or so, smart contracts will be mainly exploited to start automating underwriting, claims handling and payouts, and their impact on these processes can be significant, especially when they are used in conjunction with third-party oracles, IoT devices and artificial intelligence. In particular, automation will clearly lead to higher efficiency as the speed of claims handling would increase, while the costs and possible human errors associated with manual processing are likely to reduce. From a more theoretical and systematic perspective, it should be noted that smart contracts can reinforce the insuring agreement, as they act on the essence of an insurance contract—the insurer's promise to pay. By automating payouts and ensuring that claims are actually paid in accordance with the terms of the contract, smart contracts enhance the trust between the parties since, on the one hand, valid claims would be automatically processed and paid while, on the other hand, the technology interconnected with the smart contract can facilitate targeted investigation and this would permit to detect and deny fraudulent claims more easily. It is clear that the effect will be a reduction in transaction costs, namely in the costs of policing and monitoring the other party to make sure that her obligations are carried out as provided by the contract[40] and, more generally, the costs of ascertaining and proving the existence of relevant facts,[41] most notably the occurrence of the insured event.

To the extent that the use of smart contracts is limited to the automation of underwriting and claims management, the question whether a smart contract can be a

[37]The examples can be many: automatic translation services, face recognition systems to unlock smartphones or for criminal investigations, medical diagnosis, self-driving vehicles, machines playing games, machines that are able to create paintings or musical compositions. *See* Reillon (2018), pp. 2 ff.

[38]*See* Borselli (2018), p. 41.

[39]In 2016, for example, insurance companies in the U.S. lost more than $50 billion because of fraud: Sengupta (2017).

[40]*See* Coase (1937), pp. 386 ff.; Coase (1960), p. 15; Dahlman (1979), p. 148.

[41]*See* Scott and Triantis (2005), p. 190.

substitute for a traditional legal contract written in natural, human language seems not relevant. In this case, in fact, there would be no reason to assume that the parties would not execute a traditional contract as they still need to agree on the terms that will govern their relationship such as the scope of coverage, definitions, extensions, exclusions, conditions and general provisions. Irrespective of whether the contract is concluded in person, online or more generally at distance, a traditional legal contract will be in place, and the possible automation of underwriting and claims management would only represent a modality of execution of that contract. That is to say, the smart contract and its underlying programming code would provide a mechanism for the automatic execution of some aspects of a traditional legal contract—i.e. those aspects that are capable of being represented in conditional logic.

Considering that the programming code cannot serve as a regulatory instrument unless recognised as such, it follows that contracting parties have to assent to the adoption of a smart contract to automate underwriting and claims management, while no enabling laws seem needed as the consent of the parties to the contract would suffice to this end. Enabling laws, nonetheless, might prove valuable to foster the use of this technology, by removing any uncertainty about its legitimacy.[42] The legal contract does not need to incorporate the smart contract's code, as normally the policyholder cannot be supposed to understand the code and to assent to it. Anticipating arguments that will be developed in the following section, it is reasonable to expect that, especially in adhesion contracts—where the policyholder, typically a consumer, adheres to the contract with little or no choice about its terms—the policyholder would simply consent to a provision stating that certain contract clauses (e.g. those regulating rate setting or payouts) are automatically executed through a smart contract, while the insurance company would be responsible to use the appropriate computer code, so that the smart contract would function in accordance with the relevant terms set out in the legal contract.[43]

4 The Prospect of Truly Smart Contracts

Stanford University's scientist Roy Amara supposedly warned that "[w]e tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run."[44] Bearing in mind the "Amara's law", the discussion above clarified

[42] Consider, for example, the Delaware Blockchain Initiative promoted in 2016 by then-Governor Jack Markell to foster the use of the blockchain and smart contract technology in Delaware, and that resulted in the enactment of Senate Bill n. 69 in 2017 which provides an enabling regulatory framework for the use of this technology by corporations incorporated in that State. *See* Tinianow and Long (2017). *See also* Parker (2017) (reporting similar initiatives in other U.S. states).

[43] *But see* Levi and Lipton (2018) (arguing, with respect to smart contracts in general, that the text of the legal contract should include a representation by each party that they have examined the smart contract's code and that it matches the text of the legal contract).

[44] Ratcliffe (2016).

that the potentials of smart contracts in insurance in the near-term mainly lies in the automation of underwriting, claims handling and payouts, and this appears to be a quite realistic perspective as the projects that are currently being implemented in the industry demonstrate.[45] Not to underestimate, if not ignore, the effects of smart contracts in the long run, however, a fundamental question to be considered is whether their role can extend beyond the scenario discussed above to include in the future the automation of the entire insurance contract.

In addition to underwriting and claims management, several insurance contract clauses might be automated, since they meet the binary logic criterion, as in the case, for example, of the provisions regulating the maximum amount that can be paid under the indemnity principle, underinsurance and overinsurance, or also the aggravation or reduction of the risk.[46] In these instances, in fact, a smart contract can be programmed to trigger the relevant legal consequences, thereby ensuring that, according to the indemnity principle, the amount to be paid would not exceed the loss (or, as the case may be, the cost of repairing or replacing the insured property), or reducing the indemnity in proportion of the insured value in the case of underinsurance, and compensating up to the actual value of the insured property in the case of overinsurance. With regard to the aggravation or reduction of the risk, as this information would obviously be gathered after the execution of the contract, IoT devices may be able to detect changes in the risk and send inputs to the smart contract, automating the exercise of the insurer's right to withdraw from the contract if the aggravation of the risk exceeds a pre-programmed value, or proportionally reducing the premium in the case of a reduction of risk and also allowing the automatic exercise of the possible withdrawal right of the insurer[47] if the reduction in the premium is lower than a predetermined amount. In some instances, technology would also innovate insurance contract rules. For example, still with respect to the aggravation or reduction of risk, the duty of the insured to inform the insurer about changes in the risk will lose relevance since it is reasonable to assume that in most situations IoT devices and, more generally, monitoring technologies provided by the insurer will be responsible to detect and signal changes in the risk, so that the focus will very likely shift on the responsibility of the insurer to make sure that the devices function properly—similarly to what has been argued above regarding the possible remodeling of the insured's duty to mitigate the damage.[48]

It should be noted, however, that certain features of legal rules can hardly be captured in binary logic.[49] To make one example, take the case of overinsurance

[45] *See above* Sect. 3.

[46] For a comprehensive overview of these and other provisions under the laws of several European jurisdictions, *see e.g.* Basedow et al. (eds) (2009).

[47] *See* Article 1897 of the Italian Insurance Code (providing for the right of the insurer to withdraw from the contract within 2 months after receiving notice from the insured).

[48] *See above* Sect. 3.

[49] *See* Surden (2012), p. 636 (stating that "some—but not all—contractual terms or conditions can be meaningfully represented in terms of data and rules for the purpose of automated assessment"); Clack et al. (2017), pp. 5 ff. (distinguishing between operational and non-operational aspects of a

mentioned above, where the insurer typically has the right to avoid the contract if the policyholder acted with fraud to obtain insurance for an amount higher than the value of the insured property and, if in good faith, can also keep the premium.[50] The question arises as to whether concepts like fraud or good faith can be expressed in conditional logic. More generally, the very idea of automating the entire insurance contract, and not just selected clauses needs to be confronted with the theory of incomplete contracts. Although there is no widely accepted paradigm of incomplete contracting,[51] somehow simplifying for our purposes, this theory generally posits that complete contingent contracts—those that specify the obligations of the parties for each possible state of the world—are not feasible since, particularly where the future contingencies are complex and uncertain, the parties would incur transaction costs and difficulties in foreseeing all the possible contingencies and comprehensively regulating them in a contract. The contract, moreover, would be too costly to enforce, as courts or arbitral panels would have to distinguish among innumerable and complex contingencies.[52] It follows that standards are normally used to fill in gaps in the contract, as they are flexible, thereby allowing the parties to consider the specific circumstances of a case. Terms such as "good faith", "reasonableness", "best efforts", "diligence", "materiality" are thus common in virtually all contracts, the insurance contract included. Automation, however, rests on rules, especially rules that can be expressed in a conditional logic.[53] Thus, when it comes to the automation of the entire insurance contract, this can represent an important obstacle to making it a reality.[54]

It is nevertheless possible to predict a world where smart contracts, combined with future developments in artificial intelligence and machine learning, might challenge traditional views and change contracting practices, automating the entire contractual relationship of the parties. The algorithms behind artificial intelligence identify statistical correlation in the data they analyse, thereby enabling machines to perform tasks that would require human intelligence.[55] Because of the ever larger

legal contract, the latter being the parts of a contract that cannot be automated); De Filippi and Wright (2018), pp. 76 ff. (noting that some contract clauses and terms are not suitable for being represented into programming code).

[50] *See* Article 1909 of the Italian Civil Code, which is a rule common to several other European jurisdictions, as Articles 2:101 and 8:103 of the Principles of European Insurance Contract Law demonstrate.

[51] Maskin and Tirole (1999), p. 83.

[52] *See* Hart and Moore (1999), Maskin and Tirole (1999) and Scott and Triantis (2005).

[53] As no contract can incorporate rules for every single state of the world, drafting rules that are not tailored to specific contingencies is not a viable course of action as they can prove to be either too broad or narrow in scope, unlike standards. *See* Casey and Niblett (2017a), pp. 1402 f.; Casey and Niblett (2016), p. 430.

[54] *See e.g.* Cuccuru (2017), pp. 189 f. (stating that "code lines are not able to render 'grey areas', everything is either 1 or 0" and thus agreements that require a certain degree of flexibility cannot be converted to smart contracts).

[55] Reillon (2018), p. 1; Bambauer and Zarsky (2018), pp. 1 ff.

quantity of data available and improvements in algorithms,[56] the applications of artificial intelligence today have increased, and together with machine learning—that is, algorithms that allow machines to self-learn from data and make predictions—artificial intelligence has the potential to transform large sectors of the economy.[57]

Data-driven automation already plays a major role in legal practice and scholarship. E-discovery clearly demonstrates the potentials of data analytics in the law, as it changed how law firms execute discovery processes, replacing activities once performed by legal practitioners.[58] Further, algorithms have been developed to summarise and classify the law. In a recent law review article—to mention one notable example—Professors Eric Talley and Gabriel Rauterberg conducted an empirical research using machine learning techniques to develop a data set of "corporate opportunity waivers"—i.e. contractual modifications, permitted by some U.S. state statutes, of the duty of corporate fiduciaries not to usurp business opportunities that belong to the corporation, a subset of the general duty of loyalty—in U.S. public companies' filings with the Securities and Exchange Commission. While no systematic research was made before in this field because of the impossibility to manually collect the relevant data in an efficient way, the authors trained a machine learning algorithm to automatically classify the selected documents, thereby revealing important empirical findings.[59] The potentials of this approach can clearly extend to other areas of law.

Advances in cognitive computing and natural language processing will allow machines to process unstructured data such as contract clauses, statutes and rules or court opinions, and this will be instrumental in fully automating legal contracts. Several initiatives are in place to this end. An open source package, for instance, allows to turn real legal materials into structured data objects thus facilitating, among other things, the conversion of legal contracts into smart contracts.[60] Another project attempts to draft legal contracts with a domain-specific programming language designed to capture the features of law and its semantics and logic, its credo being "software is eating law."[61] Aside from the promotional teasers of these and similar

[56]Tällt (2017), p. 10.

[57]Talley (2018), p. 184 (emphasising that "astounding advances in data analytics [. . .] over the last two decades have virtually upended several brick-and-mortar industries"); Alarie et al. (2017), p. 7 (noting that machine learning technology already gives excellent results and will continue to develop); Coglianese and Lehr (2017), p. 1147.

[58]*See* Talley (2018), pp. 186 f.

[59]Rauterberg and Talley (2016, 2017).

[60]Reference is made in the text to the product LexNLP by LexPredict. *See* https://contraxsuite.com/lexnlp/; Bommarito et al. (2018).

[61]This is the case of the product called Legalese, provided by Legalese Pte. Ltd. *See* https://legalese.com. Similarly, other projects aim at developing coding platforms to create legal contracts in the form of code-based principles and permitting the integration of the contract code with the blockchain: *see e.g.* https://openlaw.io, or https://contractCode.io. *See also* Dewey (2017).

projects, it seems unquestionable that several efforts are tending toward the reduction of contracts and, more generally, legal documents to computer code.[62]

The turning point, however, will come when artificial intelligence and machine learning will be used to predict legal outcomes. Predictive technology is still in its infancy, but some advances have already been made and further improvements can be expected. Data may be collected from statutes and rules, case law, regulators' decisions, expert reports and other legal materials, and analysed through algorithms to determine the possible legal outcome of a specific case,[63] even potentially considering how possible ideologies of judges or arbitrators may influence their decision-making.[64] Several academic studies found that algorithms can actually be used to predict court decisions with a quite high degree of accuracy,[65] showing that they may do even better than legal experts.[66] Decision-making can become more accurate and consistent.[67] Thus, it should not be surprising that software exploiting artificial intelligence and machine learning to predict how courts will decide a case, considering the specific factual patterns, is already commercially available.[68] Obviously, the more legal data of good quality are available, the smarter artificially intelligent machines can become, and initiatives such as that launched by the Harvard Law School Library, the world's largest academic library, that aims to

[62]For a relevant example, *see* Flood and Goodenough (2017) (illustrating the computational representation of financial contracts by applying a standard computational formalism to a loan agreement).

[63]*See* Ashley and Brüninghaus (2006), pp. 309 ff.; Talley (2018), p. 28; Casey and Niblett (2017b), pp. 100 ff.

[64]*See* Fedderke and Ventoruzzo (2015), pp. 1211 ff. (examining the correlation between the ideology of U.S. Supreme Court justices and their decisions in the area of securities regulation, by collecting and coding data from selected cases).

[65]*See e.g.* Katz et al. (2017) (constructing a model to predict the decisions of the U.S. Supreme Court in a generalised, out-of-sample context and achieving, over nearly two centuries, 70.2% accuracy at the case outcome level and 71.9% at the Justices vote level); Aletras et al. (2016) (predicting decisions of the European Court of Human Rights using textual information extracted from sections of the Court's judicial opinions, and reporting strong predictive performances).

[66]*See* Ruger et al. (2004), pp. 1150 ff. (obtaining predictions of the U.S. Supreme Court decisions from legal specialists and through a statistical model, and noting that the model predicted 75% of the Court's decisions correctly, while the experts correctly forecasted results in 59.1% of cases).

[67]*See* Allen and Widdison (1996), p. 29.

[68]Tax Foresight, for example, is a product developed by the companies Blue J Legal and Thomson Reuters that allows to predict legal outcomes in tax cases. *See* http://www.bluejlegal.com/tax-foresight; Alarie et al. (2017) (reporting that in out-of-sample testing the software got more than 90% of predictions correct). For several other interesting examples *see* Rayo (2018). From a more general perspective, it is worth noting that algorithms have been used in criminal sentencing as a tool to predict recidivism risk. *See e.g. State v. Loomis*, 881 N.W.2d 749 (Wisc. 2016) (holding that proper consideration of risk assessment algorithms at sentencing does not violate a defendant's right to due process).

digitise its entire collection of U.S. case law and make it freely accessible online[69] certainly point in that direction.

In this scenario, parties to the contract would rely on artificial intelligence and machine learning technologies to interpret the contract terms and apply those terms to the facts and circumstances of a case.[70] From this perspective, "automation of the entire insurance contract" should be taken in its broadest sense to imply that the contract itself would self-interpret its own terms and be completely self-executing. To put it another way, both the interpretation and the enforcement of the contract terms would be automated—what can be called the *true smart contract*.

To make this discussion more concrete and appreciate the potential for full contract automation in insurance, it is worth considering some possible applications of predictive technology to the insurance contract. Take, for instance, the duty of disclosure, a subset of the general duty of good faith, which is ubiquitous in all insurance contracts. In virtually all jurisdictions, the prospective policyholder must disclose to the insurer material facts affecting the risk and, based on this information, the insurer determines whether to accept the risk and what premium to charge. In the event of material misrepresentations or nondisclosures, different remedies are available to the insurer, typically ranging from avoidance of the contract to the right of withdrawal, depending on whether the applicant acted with gross negligence or fraudulent intent, or simply with negligence.[71] Needless to say, this issue is highly litigated, as the policyholder may find herself in a situation where either coverage is denied or the amount to be paid under the policy is reduced, and it is clear that several legal standards are at stake to decide a possible dispute—materiality, negligence, gross negligence, good faith, just to mention some of them. An artificially intelligent algorithm might process all relevant data, such as applicable statutes and case law, and make an autonomous decision like avoidance of contract or not to pursue any remedy at all if the inaccuracy is considered not material. A smart contract, interconnected with the algorithm, would in turn enforce that decision, thereby terminating the contract with the possible corresponding right to keep the premium or, respectively, continuing the contractual relationship and compensating the insured if the risk occurred. All this would happen in real time, as soon as a

[69] *See* Harvard Law (2015) (stating that the Harvard Law School Library's collection comprises over 42,000 volumes accounting for a total of approximately 40 million pages of court decisions, and that this so-called "Caselaw Access Project" is carried out with the support of Ravel Law, a legal research and analytics company).

[70] *See* Casey and Niblett (2017b), pp. 101 ff. (arguing, however, that not only the interpretation but also the very creation of the contract terms can be automated since, with advances in predictive technology, so-called "self-driving contracts" will proliferate, where the parties agree to broad *ex ante* objectives and let automated analytics translate these objectives into specific terms at the time of performance, based on information gathered after the execution of the agreement).

[71] *See e.g.* Articles 1892 and 1893 of the Italian Civil Code. *See also* Basedow et al. (eds) (2009), pp. 80 ff. (providing a comprehensive overview of the relevant rules applying in other European jurisdictions).

possible misrepresentation or nondisclosure is detected as a result, for example, of data sent to the blockchain by an assessor or information deriving from IoT devices.

Another prominent example of the potential room for automated analytics in insurance concerns the duty to settle, typically regarded as a U.S. legal doctrine, but recognised also in some European jurisdictions,[72] which in the context of liability insurance requires the insurer to settle reasonable claims within the policy limits. Although the standard of review may vary depending on the relevant jurisdiction, for our purposes suffice it to say that an insurer who refuses a reasonable settlement proposal and takes unsound litigation decisions resulting in an excess judgment normally bears the full loss, that is it is liable for the entire judgment entered against the insured, including extra damages, in excess of the policy limits. It is no surprise that there has been a considerable amount of litigation over whether the insurer's decision not to settle in a particular case is reasonable or not, as this issue determines if the insurer or the insured bears the loss for the judgment in excess of the policy limits entered in favour of the third-party plaintiff. The focus becomes one of reasonableness, and the conduct of the insurer is also reviewed under the general duty of good faith and "based upon those principles of fair dealing which enter into every contract."[73] Several courts in the U.S. have held that the "test is whether a prudent insurer without policy limits would have accepted the settlement offer."[74] Predictive technology would collect and analyse data from the relevant statues and case law to understand how these standards operate in practice and, by applying the law to the peculiar elements of the case at issue, it would make the settlement decision. Once the smart contract receives the relevant input, the consequent action would follow, thus either accepting or denying the settlement proposal. There can obviously be other examples, but these two, also for the complexity of the laws involved, can be considered paradigmatic of the role that smart contracts, in combination with artificial intelligence and machine learning, may play in the future in automating the entire insurance contract.

Besides being capable of transforming contract performance and enforcement, this smart contracting model will be accompanied by a substantially new approach to contract formation. The growth of online insurance exchanges and robo-advisors that can provide automated investment services is already a reality.[75] Especially in contracts that include a consumer as a party, it is realistic to expect that friendly interfaces will interact even more effectively with the prospective policyholder to allow her to choose the appropriate coverage, even with the support of images and other graphic representations that would display differences in the scope of coverage—not to mention the possible assistance of robot advisors, that can automatically

[72] *See* Borselli (2016), pp. 156 ff.

[73] *See e.g. Hilker v. Western Automobile Ins. Co*., 231 N.W. 257, 258 (Wis. 1930), one of the first duty to settle cases decided in the U.S. *See also*, for Italy, Cass. 5 February 2004, n. 2195; Cass. 13 May 2008, n. 11908; Cass. 3 April 2014, n. 7768.

[74] *Crisci v. Sec. Ins. Co.*, 66 Cal. 2d 425, 431 (1967).

[75] Baker and Dellaert (2018), pp. 714 ff.

match prospective policyholders to insurance products on a personalised basis, understanding the client needs and proposing the appropriate coverage.[76] Similarly, the prospective policyholder will be able, in principle, to subscribe a larger or narrower policy by selecting exclusions and extensions from among predetermined lists, and possible inconsistencies between the coverage sought and the one selected as well as changes in the premium might be signaled in real time, not differently from what happens today when purchasing a railway or plane ticket, with computers signaling changes in the cost depending on the class of the ticket or on the seat that the passenger selects or proposing options on priority check-in or excess baggage. Pop-up windows and other dialogue boxes may also provide clear and basic explanations of the policy terms and send warning messages to improve the intelligibility of insurance contracts.[77] Customer engagement in insurance will thus markedly increase—a break with the past, as insurance, traditionally, has not been particularly sensitive to this issue. In a truly interconnected world the prospective policyholder may also find an application pre-completed with the relevant data received from accredited parties participating in the blockchain network, such as hospitals, police departments, regulatory agencies, or other insurance companies and, as long as the data are considered reliable, this is likely to deprive the duty to disclose of its meaning.

It is reasonable to assume that the natural language version of the insurance contract will continue to be available and coexist with the smart contract code and artificially intelligent algorithms. Although there is increasing awareness of the importance to master technology in today's society, and offerings of computer coding courses and the like in universities, law schools and other academic institutions are growing, a future where parties—consumers in particular—can be supposed to understand and consent to contracts written exclusively in computer code now seems unrealistic. The fact that consumers notoriously tend neither to read nor understand natural language contracts,[78] only to pull them out should a dispute arise, is a different and broader matter that should generally lead to a higher degree of simplification and clarity in standard form contracts,[79] but cannot be an argument for the idea of contracts written only in programming code. Smart contracts combined with artificial intelligence and machine learning will be able to self-interpret and self-enforce their terms but contracting parties will still have to agree on the terms

[76] *See* OECD (2017), p. 23.

[77] *See* Italian National Association of Insurance Companies (ANIA) (2018), pp. 1 f. (making similar proposals to improve contract clarity).

[78] *See* Ben-Shahar (2009), pp. 1 ff.; Bakos et al. (2014), pp. 1 ff.

[79] *See e.g.* the so-called "Letter to the Market" issued by the Italian Insurance Supervisory Authority on March 14, 2018, that urges insurers to simplify insurance contracts according to guidelines promoted by the Italian National Association of Insurance Companies (ANIA) in conjunction with major consumer and intermediary associations to make the contracts more intelligible to the policyholders: IVASS (2018), pp. 2 f.

themselves in the first place—not differently from what happens today.[80] Even when the contract is concluded entirely through the support of user-friendly interfaces as illustrated above, the computer programme will always generate the corresponding natural language version.[81]

As in the case of the automation of underwriting and claims management discussed above, also for the automation of the entire insurance contract no enabling legislation seems strictly needed since it should be within the power of the parties to consent to contracts that would perform automatically.[82] Contracting parties, and the insured in adhesion contracts, will have to give their explicit assent to the automation of the interpretation and enforcement of the contract terms, in line with the principle established by the European General Data Protection Regulation that grants individuals the right not to be subject to a decision based solely on automated processing, including profiling,[83] unless the data subject gave her explicit consent.[84] As the discussion below will clarify, a regulatory framework, however, will be necessary to address the issues that true smart contracts might pose.

An important point to emphasise is that, although the contract would self-interpret and self-enforce its terms, parties do retain their right to file suits in court or seek arbitration, should they disagree with the determinations executed by the smart contract—exactly as when contract performance is based on human judgment. Even if smart contracts, by definition, aim at avoiding the need for enforcement proceedings, automatic performance might still turn out to be wrongful and parties should be entitled to contest it.[85] The judicial or arbitrator review will clearly be on the merits of the automated decision and not on the underlying programming code and algorithms, as any automated decision will always be assessed against the relevant set of legal rules and doctrines. It might be the case, however, that contracting parties refer to the very decision of the algorithm to support their claims.

[80] *But see* Casey and Niblett (2017b), pp. 100 ff., envisioning a world where the contract itself will self-create its own terms, while the parties only set general *ex ante* objectives and let algorithms translate these objectives into *ex post* specific terms accounting for real-time contingencies—a future, this, which is truly fascinating but that appears too far-distant.

[81] *See* Clack et al. (2017), p. 11.

[82] As discussed in Sect. 3 above, enabling laws, however, might remove any possible uncertainty about the legitimacy of contract automation, thereby furthering the use of smart contracts.

[83] "Profiling" is broadly defined by Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L119) 1 [hereinafter European General Data Protection Regulation], and includes "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" to analyse or predict, among other things, aspects concerning that person's economic situation, health, personal preferences, reliability, behaviour.

[84] Article 22, European General Data Protection Regulation (providing also for other exceptions, such as when the decision is authorised by European Union or national laws that also lay down appropriate measures to protect the data subject's rights and freedoms and legitimate interests).

[85] *See* Werbach and Cornell (2017), p. 376 (arguing that there will be a shift in litigation from claimants seeking fulfillment of promissory obligations to claimants seeking to reverse transactions already completed).

For example, in the duty to settle context, where, as discussed above, it could be difficult to determine, in hindsight, if the insurer's decision not to settle was reasonable, the algorithm's determination, where properly documented, might turn out to be conclusive proof in cases that are on the borderline between a reasonable and a not-so-reasonable refusal to settle.

Over time, judicial and arbitrator review of automated decisions will align increasingly the algorithms with the law. The more the algorithms are accurate, the less likely their decisions will be overturned by courts or arbitral panels, and the higher the trust that contracting parties in turn will place in the algorithms. A virtuous circle will ensue, where the number of cases litigated or arbitrated will reduce, and the newly rendered judgments or arbitral awards will contribute to refine the algorithms even more.

Contracting patterns thus will evolve. Changes will be incremental, and this process will probably take decades to be completed. Smart contract codes and artificially intelligent algorithms will progress over time, as humans will continue improving them. To this end, there is no doubt that lawyers and legal scholars will be central to addressing and fostering the technology developments. Automation in law is not, and never can be, the exclusive realm of data scientists, computer engineers, mathematicians or statisticians. To make smart contracts and any other technological innovation a reality in the legal field, it should go without saying that technological knowledge and skills have to be complemented by a high degree of legal expertise to adequately recognise and navigate the complexity of legal systems.

As contracts will be able to make autonomous decisions and automatically execute them, the pressing issue is not whether computers can be granted legal personality since,[86] to the extent that parties give their assent to contract automation, it seems far more sensible to argue that the autonomous decision should be attributed to the relevant contracting party. Rather, law should focus on who the providers of smart contracts and artificially intelligent algorithm systems are and on how these technologies operate.[87]

Specialised private companies are likely to enter this market[88] and, considering the resource commitments and expertise needed to provide effective services, most probably a few firms will end up dominating it, as in the case of the proxy advisory industry where the global players are in the order of two or so.[89] For the large quantity of data that they collect, insurance companies are also well placed to stand out as providers,[90] although it can be expected that in the initial stage they will engage the services of third-party vendors, to then follow a trend similar to the one

[86]For a discussion of the idea of computer's personhood, *see* Solum (1992), pp. 1231 ff.; Allen and Widdison (1996), pp. 35 ff.; Teubner (2018), pp. 108 ss.

[87]Casey and Niblett (2017b), pp. 125 ff.

[88]*See* Casey and Niblett (2017b), p. 127.

[89]*See* Copland et al. (2018), p. 2 (noting that Institutional Shareholder Services and Glass Lewis are clearly the largest proxy advisory firms globally).

[90]*See* Casey and Niblett (2017b), pp. 127 ff.

that is developing in the market for e-discovery, where insourcing is increasingly common. For obvious reasons, these new technologies will be targeted first at the largest insurance markets, such as the United States, Europe and China. Providers will have to differentiate smart contract codes and algorithms by jurisdictions as products will have to be calibrated against the relevant legal and regulatory framework. Although the sources of insurance regulation generally can be traced more and more at the international level,[91] insurance contracts are still largely regulated at the state level, and this is true both for the U.S., where insurance regulation traditionally has been the responsibility of the individual states, and for the European Union, where harmonisation of insurance contract law among the Member States is overall limited.[92] It should be noted, nonetheless, that technology operational needs and reasons of economies of scale might lead to an increase in the standardisation of insurance products across companies and countries, and be also a factor in determining further convergence of national insurance laws and regulations in the future.

As true smart contracts will mature and their potentials will become manifest, regulation should be established to address the issues that this phenomenon might pose. It is sensible for regulators first to track the technological developments, also using regulatory sandboxes, to understand the functioning of the technology and identify the potential risks without undermining innovation, only then to consider possible adjustments to the regulatory framework.

As a threshold matter, there will clearly be the need to ensure the security and reliability of the underlying technology and coding system, as the risk of flaws in smart contract codes and artificially intelligent algorithms is high,[93] and any realistic prospect of implementing contract automation in insurance will be rooted in the operational adequacy of the technology used.

Moreover, there might be room for abuse to the extent that the smart contract code and algorithms do not faithfully reflect the terms actually consented to by the policyholder and the applicable laws or, to put it another way, to the extent that the actual functionality of the smart contract is not adequately disclosed.[94] Although policyholders would have the right to file suit in court or seek arbitration as discussed above, it seems far from uncommon that a number of them, especially where consumers are involved, will decide not to do so either because they may find it not convenient to pursue the claim or because they would simply rely on the smart contract. In this case, the need arises to protect the policyholder and promote transparency of automated decision-making.[95]

[91] *See* Marano (2017), pp. 5 ff. (discussing the increasing transnational dimension of the sources of insurance regulation today).

[92] *See* Cousy (2017), pp. 43 ff. (arguing for the harmonisation of insurance contract law in the EU).

[93] *See* above, Sect. 2.

[94] Cohney et al. (2019), pp. 591 ff. (finding mismatches between smart contracts and the relevant offering documents in the context of initial coin offerings).

[95] *See* European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

In principle, regulation should be more robust where the policyholder is a consumer, while it might be lighter for contracts concluded between the insurance company and another business party that might be capable to protect itself.[96] This distinction, however, might be blurred in practice since not all business parties are likely to be so sophisticated that can be expected to understand the programming code and the relevant algorithms. Probably a scenario where private third parties would provide the smart contract might give more assurance of the faithful match between the code and the legal terms than the case where the contract itself is coded by the insurance company. Nonetheless, considering that insurance companies, as "repeat players", would most probably be the sole buyers of the smart contracts sold by third-party providers, conflicts of interests might arise and need to be addressed. In this perspective, the imposition of independence requirements on third-party vendors appears to be the most realistic prophylactic measure. In addition, joint and several liability should be imposed on insurance companies and third-party providers for damages due to flaws and discrepancies in the smart contract code and algorithms. The system should be backed by adequate monetary sanctions to deter fraudulent practices, and regulators should be given the power to access the programming code and the relevant algorithms to investigate alleged malfunctions and anomalies of the smart contracts, thus fostering the safety and reliability of the relevant technology. Over time, the need for third-party vendors and, even more, for insurance companies to preserve their reputation in their respective markets is likely to play a role in aligning the computer code and algorithms with the legal terms and ensuring the proper functioning of smart contracts.

Considering the global nature of the smart contract phenomenon and of technological innovation more generally, there is clearly a need for uniform standards of regulation, oversight and enforcement, also to avoid possible risks of regulatory arbitrage. To this end, supranational authorities and organisations, especially the International Association of Insurance Supervisors, can play an important role in developing common regulatory standards, so that regulators across the world can share a clear set of principles and objectives, thereby promoting a harmonised approach to the regulation of smart contracts in insurance.

5 Conclusion

The potential for contract automation in insurance appears significant. In the near-term, smart contracts can have a substantial impact on underwriting, claims handling and payouts, while in the farther-distant future there are grounds to assume that the entire insurance contract will be automated. For this scenario to occur, however, technological advances alone will not suffice. The ability to navigate the complexity

[96] *See* Casey and Niblett (2017b), p. 127.

of the relevant legal framework and ultimately integrate technology and law will be crucial to make contract automation in insurance a reality.

One might wonder, however, why contracting parties, in particular insurance companies, should embrace this path-breaking innovation. The obvious answer is that the scenario examined above, overall, will be superior to the current one, and in fact, as discussed, smart contracts can provide substantial advantages in terms of operational efficiencies and streamlined underwriting and claims management processes, fraud detection, more accurate rate setting resulting in personalised and possibly lower premiums, enhancement of trust between the insurer and the insured, customer engagement. The truth, nevertheless, is that technology will become more and more pervasive in insurance and society at large. It will permeate law and transform existing contracting patterns and, more generally, traditional paradigms. Yet, as technological innovation never takes place in a legal vacuum, law will play a central role in marking out a line of equilibrium between the objective of fostering automation and innovation in insurance and the need to ensure policyholder and investor protection.

Acknowledgments The author wishes to thank the Association Internationale de Droit des Assurances (AIDA) Europe for awarding the AIDA Europe Academic Prize to this paper. He is also grateful for the invaluable comments by the participants at the VII AIDA Europe Conference held in Warsaw on April 12–13, 2018, and at the seminar "IOSCO and the new financial architecture" organised by the University of Luxembourg and the Max Planck Institute Luxembourg for Procedural Law, and held at the University of Luxembourg on October 4, 2018.

References

Alarie B et al (2017) Using machine learning to predict outcomes in tax law. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2855977

Aletras N et al (2016) Predicting judicial decisions of the European Court of Human Rights: a natural language processing perspective. PeerJ Comput Sci 2:e93. https://doi.org/10.7717/peerj-cs.93

Allen T, Widdison R (1996) Can computers make contracts? Harv J Law Technol 9:25–52

Amuial SS et al (2016) The Blockchain: a guide for legal & business professionals. Thomson Reuters

Ashley KD, Brüninghaus S (2006) Computer models for legal prediction. Jurimetrics 46:309–352

AXA (2017) AXA goes blockchain with fizzy. https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy

Baker T, Dellaert BGC (2018) Regulating Robo advice across the financial services industry. Iowa Law Rev 103:713–750

Bakos Y et al (2014) Does anyone read the fine print? Consumer attention to standard-form contracts. J Leg Stud 43:1–35

Bambauer J, Zarsky T (2018) The algorithm game. Notre Dame Law Rev 94:1–47

Basedow J et al (eds) (2009) Principles of European insurance contract law. Sellier European Law Publishers, Munich

Ben-Shahar O (2009) The Mity of the 'Opportunity to Read' in contract law. Eur Rev Contract Law 5:1–28

Bommarito MJ et al (2018) LexNLP: natural language processing and information extraction for legal and regulatory texts. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192101
Borselli A (2016) The insurer's duty to settle in the United States and in Europe. The pursuit of a proper standard of review. In: Jovanovic S et al (eds) Reforms and new challenges in insurance law. AIDA Serbia, Belgrade, pp 156–170
Borselli A (2018) Insurance by algorithm. Eur Insur Law Rev 2:40–44
Casey AJ, Niblett A (2016) Self-driving laws. Univ Toronto Law J 66:429–442
Casey AJ, Niblett A (2017a) The death of rules and standards. Indiana Law J 92:1401–1447
Casey AJ, Niblett A (2017b) Self-driving contracts. J Corp Law 43:100–132
Catlin T et al (2017) Insurtech – the threat that inspires. https://www.mckinsey.com/industries/financial-services/our-insights/insurtech-the-threat-that-inspires
Clack C et al (2017) Smart contract templates: foundations, design landscape and research directions. https://arxiv.org/pdf/1608.00771.pdf
Coase RH (1937) The nature of the firm. Economica 4:386–405
Coase RH (1960) The problem of social cost. J Law Econ 3:1–44
Coglianese C, Lehr D (2017) Regulating by robot. Administrative decision making in the machine-learning era. Geo Law J 105:1147–1223
Cohney S, Hoffman D et al (2019) Coin-operated capitalism. Columbia Law Rev 119:591–676
Copland JR et al (2018) The big thumb on the scale. An overview of the proxy advisory industry. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3188174
Coppola F (2016) Ethereum's DAO hacking shows that coders are not infallible. https://www.forbes.com/sites/francescoppola/2016/06/20/the-dao-hacking-shows-that-coders-are-not-infallible/#6292e17a3983
Cousy H (2017) Changing insurance contract law: an age-old, slow and unfinished story. In: Marano P, Siri M (eds) Insurance regulation in the European Union. Solvency II and beyond. Palgrave Macmillan, pp 31–57
Cuccuru P (2017) Beyond bitcoin: an early overview on smart contracts. Int J Law Technol 25:179–195
Dahlman CJ (1979) The problem of externality. J Law Econ 22:141–162
De Filippi P, Wright A (2018) Blockchain and the law. The rule of code. Harvard University Press, Cambridge
Deloitte (2018) 2018 Insurance Industry Outlook. https://www2.deloitte.com/it/it/pages/financial-services/articles/gx-insurance-industry-outlook.html
Dewey JN (2017) A code-based contract development application and process for the execution of code-based 'smart documents'. https://contractcode.io
Farr C (2018) This start-up made connected toothbrushes – now it aims to overthrow the 'primitive' dental insurance industry. https://www.cnbc.com/2018/05/15/beam-dental-raises-22-million-from-kleiner-to-change-dental-insurance.html
Fedderke JW, Ventoruzzo M (2015) Do conservative justices favor Wall Street: ideology and the Supreme Court's securities regulation decisions. Florida Law Rev 67:1211–1280
Flood MD, Goodenough OR (2017) Contract as Automaton: the computational representation of financial agreements. https://www.financialresearch.gov/working-papers/files/OFRwp-2015-04_Contract-as-Automaton-The-Computational-Representation-of-Financial-Agreements.pdf
Gatteschi V et al (2018) Blockchain and smart contracts for insurance: is the technology mature enough? Future Internet 10(2):1–16
Hart O, Moore J (1999) Foundations of incomplete contracts. Rev Econ Stud 66:115–138
Harvard Law (2015) Harvard Law School launches 'Caselaw Access' project. https://today.law.harvard.edu/harvard-law-school-launches-caselaw-access-project-ravel-law/
Hernandez E (2017) Digital innovations in smallholder agricultural insurance. http://www.cgap.org/blog/digital-innovations-smallholder-agricultural-insurance
Huckstep R (2016) Dynamis – if insurance, then blockchain. https://www.the-digital-insurer.com/blog/insurtech-dynamis-if-insurance-then-blockchain/
IAIS (2017) FinTech Developments in the Insurance Industry. https://www.iaisweb.org/page/news/other-papers-and-reports

Italian National Association of Insurance Companies (ANIA) (2018) Contratti Semplici e Chiari. https://www.ivass.it/normativa/nazionale/secondaria-ivass/lettere/2018/lm-14-03/Allegato_ANIA_Contratti_semplici_e_chiari.pdf

IVASS (2018) Simplification of insurance contracts. Guidelines of the Technical panel ANIA – Consumer Associations – Intermediary Associations for clear and simple contracts. Letter to the Market, 14 March 2018. https://www.ivass.it/normativa/nazionale/secondaria-ivass/lettere/2018/lm-14-03/Letter_to_the_market_of_14_3_2018.pdf?language_id=3

Jubraj R (2018) InsurTech: a catalyst for insurers' wider innovation journey. https://insuranceblog.accenture.com/insurtech-a-catalyst-for-insurers-wider-innovation-journey

Katz DM et al (2017) A general approach for predicting the behavior of the Supreme Court of the United States. https://doi.org/10.1371/journal.pone.0174698

Levi SD, Lipton AB (2018) An introduction to smart contracts and their potential and inherent limitations. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/

Marano P (2017) Sources and tools of the insurance regulation in the European Union. In: Marano P, Siri M (eds) Insurance regulation in the European Union. Solvency II and beyond. Palgrave Macmillan, pp 5–29

Maskin E, Tirole J (1999) Unforeseen contingencies and incomplete contracts. Rev Econ Stud 66:83–114

McKinsey&Company (2017) The promise of blockchain. https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/The%20promise%20of%20blockchain/The-promise-of-blockchain.ashx

NEOS (2018) Smarter home insurance. https://neos.co.uk/

O'Brien HM (2016) The Internet of Things. J Internet Law 19:12–20

OECD (2017) Technology and innovation in the insurance sector. https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf

Parker L (2017) US States working on blockchain legislation in 2017. https://bravenewcoin.com/news/us-states-working-on-blockchain-legislation-in-2017/

Ratcliffe S (ed) (2016) Oxford essential quotations. Oxford University Press. http://www.oxfordreference.com

Rauterberg G, Talley E (2016) A machine learning classifier for corporate opportunity waivers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2849491

Rauterberg G, Talley E (2017) Contracting out of the fiduciary duty of loyalty: an empirical analysis of corporate opportunity waivers. Columbia Law Rev 117:1075–1151

Rayo EA (2018) AI in law and legal practice – a comprehensive view of 35 current applications. https://www.techemergence.com/ai-in-law-legal-practice-current-applications/

Reillon V (2018) Understanding artificial intelligence, European Parliamentary Research Service, http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614654/EPRS_BRI(2018)614654_EN.pdf

Ruger TW et al (2004) The Supreme Court forecasting project: legal and political science approaches to predicting Supreme Court decisionmaking. Columbia Law Rev 104:1150–1209

Scott RE, Triantis GG (2005) Incomplete contracts and the theory of contract design. Case Western Law Rev 56:187–201

Sengupta S (2017) The power of machine learning in insurance. https://vision.cloudera.com/the-power-of-machine-learning-in-insurance/

Sennaar K (2017) How America's top 4 insurance companies are using machine learning. https://www.techemergence.com/machine-learning-at-insurance-companies/

Solum LB (1992) Legal personhood for artificial intelligences. N C Law Rev 70:1231–1287

Surden H (2012) Computable contracts. U.C. Davis Law Rev 46:629–700

Szabo N (1996) Smart contracts: building blocks for digital market. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Talley E (2018) Is the future of law a driverless car? Assessing how the data-analytics revolution will transform legal practice. J Inst Theor Econ 174:183–205
Tällt (2017) Insurtech Disruption Trends 2017. Artificial intelligence
Teubner G (2018) Digital personhood? The status of autonomous software agents in private law. Ancilla Iuris, 107–149
Tinianow A, Long C (2017) Delaware blockchain initiative: transforming the Foundational Infrastructure of Corporate Finance. https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/
U.S: Federal Trade Commission (2015) Internet of Things. Privacy & security in a connected world. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
Werbach K, Cornell N (2017) Contracts *Ex Machina*. Duke Law J 67:313–382
Willis Towers Watson (2016) Want to get an insurer's attention? Just say blockchain. https://www.willistowerswatson.com/en/insights/2016/06/want-to-get-an-insurers-attention-just-say-blockchain
Willis Towers Watson (2018) Quarterly InsurTech briefing. https://www.willistowerswatson.com/-/media/WTW/PDF/Insights/2018/05/quarterly-insurtech-briefing-q1-2018.pdf
Wright A, De Filippi P (2015) Decentralized blockchain technology and the rise of *Lex Cryptographia*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

Digitalisation of Insurance Contract Law: Preliminary Thoughts with Special Regard to Insurer's Duty to Advise

Piotr Tereszkiewicz

1 Introduction

For decades or even centuries, insurance industry has not changed significantly. Similarly, insurance contract law developed gradually, as it did not have to deal with unexpected challenges of abruptly changing reality. Since the beginning of the twenty-first century, insurance law and practice have witnessed two major developments, that is, the emergence of the Big Data technology and significant reforms of insurance contract law.

Recent technological advances have begun profoundly changing the business of insurance. All stages of the insurance value chain (product design, marketing and distribution, underwriting and pricing, post-sales services and contract governance and claims management) are influenced by technology-enabled innovation in insurance (InsurTech, EIOPA 2017a).[1] First, insurance products are increasingly purchased on-line. Following insurance industry data, over 40% of insurance products will soon be purchased online.[2] Specialist analysis of supervision bodies show that 44% of customers would prefer to buy insurance and investment products online in the UK, with only 21% preferring not to.[3] Most importantly, according to a Gallup poll, "millennials" are more than likely to purchase policies online instead of through

This contribution was written in the framework of the research project 2015/17/B/HS5/00495 funded by the National Science Centre in Poland.

[1] EIOPA (2017a).

[2] Capgemini (2017).

[3] EIOPA (2017b), p. 80.

P. Tereszkiewicz (✉)
Private Law Department, Jagiellonian University in Cracow, Kraków, Poland
e-mail: piotr.tereszkiewicz@uj.edu.pl

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_6

an agent.[4] This means that a significant class of insurance consumers will become a target for (almost exclusive) on-line distribution of insurance products. From the regulatory perspective, this implies that access to insurance should be ensured, in the long term, for digital customers who are financially literate and do not need to hold a physical meeting with a financial adviser to conclude an insurance contract.

Second, consumers benefit from the design of more personalised products and services adapted to their evolving needs. Several examples will be discussed below. Third, a greater availability of data and capacity for processing it open new possibilities for insurers. The processing of structured and unstructured information through Big Data enables more accurate prediction of risks and events, allowing more risk-based pricing, even on a personalised basis.[5] Clearly, new technologies will create risks for customers, as products and services of insurers will be delivered virtually.[6] Whereas these developments are not yet entirely predictable, it is clear that legal rules on insurance contracts will be increasingly confronted with challenges resulting from digitalisation in the near future.

2 Examples of New Insurance Products

Innovations associated with the phenomenon of Big Data have brought about a major transformation of insurance contracts and the rise of new products and business models. Many of the new approaches would not be possible without new technologies. Out of several new products, I wish to indicate Usage-Based Insurance, often applied in car insurance. Rather than relying on past driving records and statistics to determine premium costs, usage-based auto insurance incorporates present-day habits and the number of miles driven (e.g. blackboxes tracking the driving behaviour and environment).[7] Linking insurance premiums to driving behaviour can be attractive to certain consumers, particular those who engage in less-risky practices.[8] At the same time, insurers benefit from studying consumer behaviour and keep delivering advice aimed at helping consumers improve their driving records. Offering usage-based insurance requires the use of emerging technologies, such as connecting devices and advanced analytics. Some insurers track miles as well as driver habits: a plug-in device or mobile app monitors car-trip details. Discounts are awarded to drivers who drive less often, in less risky manners

[4]Results are based on a Gallup Panel Web and mail study completed by 18,039 national adults, aged 18 and older, conducted between 4 December 2013 and 14 January 2014.

[5]Helveston (2016).

[6]European Commission (2016).

[7]In Italy, blackbox tracking devices were integrated in approximately 15% of the motor insurance contracts underwritten in 2015, EIOPA (2017a), p. 8.

[8]Capgemini (2017), p. 31.

or when there is less traffic.[9] A possibility to constantly monitor customer conduct opens ways to highly personalised insurance products, e.g. a customer who consumed alcohol the night before might get a recommendation from his device to use public transportation instead of driving to work.

In a similar vein, new on-demand and just-in-time insurance products offer consumer a possibility of purchasing tailored insurance policies only for specific periods, without being obliged to subscribe to longer term plans, as has traditionally been the case.[10] Products indicated above are no more tailored insurance products in the traditional meaning, but actually innovative smart products that have not been subject to outright regulation, but will have to be dealt with by means of insurance contract law rules.

3 Reforms of Insurance Contract Law

The rise of new insurance products, as described above, comes not long after a sharp deregulation (liberalisation) of insurance law in the European Union. Most importantly, a requirement of prior approval of insurance standard terms by a public body was abolished. The deregulation of the European insurance market, which resulted from the European Union law in 1990s, was also one of the major reasons for the renaissance of national insurance contract codifications. The last decade has witnessed a wave of insurance contract law re-codifications, which wholly or partly replaced the codifications dating from the beginning of the twentieth century (e.g. the Marine Insurance Act 1906 in the UK, German Insurance Contract Act of 1908, the French Code des Assurances 1930). New insurance contract statutes have been enacted among others in Austria (on-going reforms since mid-1990s), the Czech Republic (2004), the Netherlands (2005) and Germany (2007), while important reforms began to take place in England in 2012, with the enactment of Consumer Insurance (Disclosure and Representations) Act 2012 and the Insurance Act 2015.[11] In parallel with these national developments, an academic expert group, the Restatement Group,[12] prepared a restatement of the European insurance contract law, the Principles of European Insurance Contract (PEICL).[13] While the PEICL set a Common Frame of Reference of Insurance Contract Law in the EU, they primarily serve as a model law for the European or national legislators on insurance contract.[14] Similarly, in the United States, since 2010, there have been works on, first the Principles, and subsequently, the Restatement of the Law of Liability Insurance

[9] Capgemini (2017), p. 31.

[10] Capgemini (2017), p. 31; EIOPA (2017a), p. 8.

[11] For an overview, see Basedow (2015), pp. 44 et seq.

[12] See under http://restatement.info/.

[13] Basedow et al. (2015).

[14] On possible functions of PEICL, Fontaine (2011), pp. 39 et seq.

under the auspices of the American Law Institute.[15] While this is a specific branch of insurance law, the Restatement covers general concepts relevant for the whole body of insurance contract law.[16]

The above-mentioned reforms or reform projects in both Europe and the U.S. have strengthened or aim at strengthening the position of policyholder as a consumer in her relation to the insurer. Most importantly, they have introduced or consolidated the philosophy of consumer protection, mostly by standard disclosure and control of standard contract terms, into the domain of insurance law.[17] This is a thoroughly valuable and significant development. Nonetheless, it seems that recent insurance reforms in Europe, innovative as they might be when judged against the benchmark of traditional (maritime inspired) insurance law, are locked in the pre-digital age. One could even claim that the transformation of insurance law happened a few years too yearly to fully embrace the specific challenge of digitalisation of insurance.

Until now, the issue of digitalisation of insurance has hardly been studied and it has only just begun to attract the attention of insurance regulators.[18] Furthermore, it would be premature to expect new regulatory approaches regarding InsurTech to date in individual legal systems or on a global standard setting. The regulatory paradigm is a standard insurance contract, either a consumer contract or a business insurance contract.[19] At first sight, insurance contract law acts do not consider Big Data enabling insurers to personalise insurance relationships to a high degree. Profound reflection is required to establish how contemporary insurance contract law rules deal with personalisation of insurance contract.

4 Major Instances of 'Personalisation' in Insurance Law

4.1 The Insurance Applicant's Duty to Disclose

A prominent feature of insurance contracts is that the characteristics of the buyer (policyholder) affect the costs of the seller. A high-risk customer will cost more than a low-cost customer. The traditional rule of insurance, both in common and continental European insurance law, has been the duty of an insurance applicant to disclose risk-relevant circumstances to the insurer.[20] The duty has been said to be necessary for the protection of insurers, who could refuse or adapt coverage given a

[15]On which, see Feinman (2015).

[16]Such as interpretation of insurance contract, misrepresentation or fraud by policyholder, see Feinman (2015).

[17]Heiss (2012).

[18]European Commission (2016).

[19]Heiss (2012).

[20]E.g. the celebrated English case Carter v. Boehm (1766) 3 Burr. 1906, 1909, per Lord Mansfield.

high risk in the case of an applicant. Nowadays, the duty of disclosure appears justified only in exceptional cases, e.g. unknown risks. As far as better know risks are concerned, the difficulty of investigating them is not comparable to the nineteenth century reality by which the duty of disclosure was determined. Already in the 1990s of the twentieth century, before the dawn of the Digital Age, it was claimed that the insurers nowadays are better equipped to investigate risks through inspectors and have technical expertise to assess the risk and to elicit material information.[21] Nowadays, there is no doubt that Big Data enables insurers to transform their function from 'reactive claims payers' to 'preventive risk advisors'. The rise of Big Data phenomenon makes it necessary to revisit the assumptions regarding the duties of disclosure. Given the multiple data available to an insurer in the future, it is throughout possible that the insurer already has the information about the insurance applicant. It is even likely that insurers may have more information on the insured than the insured could directly provide. Can an insured comply with his duty to disclose by simply being passive in the engagement process, given that the insurer possesses the knowledge already?

The Big Data phenomenon raises a number of questions regarding the information flow between consumer and insurer and its consequences. First, one may claim that the extended use of Big Data may risk de-personalising a policyholder in the face of broad statistical information. Second, the example of usage-based insurance raises fundamental questions from the perspective of insurance contract law. Tentatively, one can claim that personalisation of insurance assumes an entirely new dimension. The policy-holder's duty of disclosure (uberrima fides) related mostly to past events or her present condition affecting the insurer's risk and the insurance premium. Usage-based insurance focuses on the actual conduct of policyholder during the insurance relationship. The pre-contract disclosure does not appear to play an important role in that model of insurance where the insurer is an active information-searching agent. Finally, for the time being, it is open to inquiry whether the emergence of Big Data will expand market availability for some (classes of) insurance customers or on the contrary whether consumers with higher risk profiles would face a higher degree of exclusion.[22] In several EU Member States, bans on the use of certain information for underwriting, such as genetic data, have been introduced.

4.2 Personalised Duties to Warn and Advise

From the legal perspective, personalisation of insurance products has been facilitated by the emergence of 'personalised disclosure and advice' in insurance law. The last decade has seen the proliferation of insurer duties to warn or advice a prospective

[21] Clarke (1997), p. 90.

[22] EIOPA (2017a), p. 4.

policyholder as to the content of the insurance product in question. One could claim that this reflects the fact that a typical insured party views the insurance relationship to be one in which the company promises security and protection, rather than a detailed and obscure set of specifications and exclusions of cover.[23] At the European Union level, the Insurance Mediation Directive (IMD) of 2002[24] introduced a duty of insurance intermediaries to specify the demands and the needs of customers, as well as underlying reasons for any advice given to customers on a given insurance product. This obligation, which should cause insurers to "know their customers and their own products," is probably the first step in the process of personalising insurance law. Under several national insurance contract laws, in particular under German law, the duties of insurers to advise their clients have been developed to ensure a relatively high level of personalised pre-contract explanations offered to customers.[25] Following these developments, insurers have assumed a proactive role in collecting consumer data to offer tailored insurance coverage and avoid liability for wrong advice.

The emergence of Big Data allows insurers to gather even more information about potential customers. This could justify imposing on insurers a duty to provide highly personalised coverage taking specific characteristics and risks of a customer. Further, the Big Data allows offering increasingly personalised products.[26] Yet, at the same time, personalisation of insurance products inhibits comparison of such products. This is a major challenge for insurance law from the perspective of consumer protection, as it undermines the consumer law goal of ensuring product comparability. I recognise that the importance of data protection regime, in particular General Data Protection Regulation (GDPR)[27] is of paramount importance as far as questions under inquiry are concerned. While the questions regarding data protection may be occasionally referred to, they remain beyond the scope of this contribution.

The following parts of this contribution are devoted to analysing how a duty of an insurer to provide advice to an insurance applicant has evolved in the European Union, with particular regard to online contracting in the domain of insurance business.

[23]For a view of insurance as relational contract, see Feinman (2009), p. 553; Tereszkiewicz (2013), p. 235.

[24]Insurance Mediation Directive 2002/92/EC of 9 December 2002 (2003) OJ L9/3.

[25]Loacker (2015).

[26]Loacker (2015), p. 287.

[27]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), OJ L 119, 4.5.2016, pp. 1–88.

5 The Evolution to the Duty to Advise with Particular Regard to Online Distribution

5.1 Directive 2002/92/EC on Insurance Mediation

Directive 2002/92/EC on insurance mediation[28] (IMD) was a legal act of fundamental relevance for the process of creating the European insurance contract law. As a minimum harmonisation directive, the IMD aimed at contributing both to the completion of the single market for financial services and to the enhancement of customer protection in this field.[29] Applying only to insurance intermediaries, the IMD set forth a number of provisions addressing the intermediary/policy-holder relationship.[30] While the IMD dealt with a broad range of insurance intermediaries, it fell short of imposing parallel duties on insurers as such (Article 2(3) IMD).[31]

Arguably, one of important provisions for shaping the intermediary/policy-holder relationship was Article 12(3) IMD. It provided for a duty to explore the potential policy-holder's needs. The provision reads as follows:

> Prior to the conclusion of any specific contract, the insurance intermediary shall at least specify, in particular on the basis of information provided by the customer, the demands and the needs of that customer as well as underlying reasons for any advice given to the customer on a given insurance product. These details shall be modulated according to the complexity of the insurance contract being proposed.

This provision imposed on an insurance intermediary a duty, on the one hand, to specify the demands and the needs of a prospective policy-holder with a view to a specific contract, and, on the other hand, to specify underlying reasons for any advice the intermediary gives to a customer. This phrasing was rather broad and did not provide detailed guidance on the precise extent of the intermediary's duty. Nevertheless, the second sentence of Article 12(3) IMD, namely that details regarding the intermediary's duties 'shall be modulated according to the complexity of the insurance contract being proposed', could be regarded as guidance for national legislators as regards the criteria according to which the exact scope of intermediary's duties ought to be hammered out.

Furthermore, Article 12(3) IMD clearly obliged a prospective policy-holder to cooperate with an intermediary by providing information on his/her coverage needs.

While Article 12(3) IMD could not be taken to introduce a far-reaching duty to explore the needs of a prospective client, it certainly introduced a 'know your customer' rule into the European insurance law.[32] Compared to the far more

[28] Insurance Mediation Directive 2002/92/EC of 9 December 2002 (2003) OJ L9/3.

[29] IMD Preamble, Considerations 7 and 8.

[30] See Article 2(3) IMD. IMD fell short of imposing parallel duties on insurers as such. Cf. Langer and Rosenow (2006), p. 195.

[31] See the IMD Preamble, Consideration 9; Tereszkiewicz (2013), p.239.

[32] Moloney (2008), p. 254, calls this rule: "a quasi-know-your-client requirement"; see also Tereszkiewicz (2013), p. 239–240.

extensive MiFID[33] regime regarding investment products, the IMD focused more on product than on a client's status or qualities.[34] Nevertheless, given that the IMD was a measure of "minimum harmonisation," the manner in which Article 12(3) IMD was drafted ('shall at least specify') allowed Member States to extend the scope of such duties in the process of implementing this provision into national law. Despite its apparently modest regulatory reach, a 'know your customer rule', as laid down in Article 12(3) IMD, appears to have had great relevance not only for the law regarding intermediaries, but also for the general conduct of the insurance business.

5.2 IMD and Digitalisation of Insurance

Enacted in 2002, IMD reflected generally the pre-digital age and the pre-history of Internet. Most importantly, IMD provisions made no explicit reference to the provision of information via a website (cf. Art. 13 IMD). Still, IMD impact on personalising insurance relationships—in a manner favouring the InsurTech application—should be regarded as considerable.

Following the enactment of the IMD, it has been claimed that there is a strong case for a 'know your customer duty' to be applied to insurers as well.[35] On this interpretation, this rule should apply generally in the process of selling insurance. There are two major ways of extending this duty to insurers. First, it is arguable that provisions regarding intermediaries' duties could be applied per analogiam to direct insurers.[36] Nevertheless, it must be borne in mind that while intermediaries may provide advice about products accessible on a specific market, insurers as sellers generally advise on the scope of their products. This could definitely make analogous extensions of such duties to insurers debatable. Secondly, a less controversial manner of extending the 'know your customer' duty on insurers could consist of enacting specific provisions to this effect.[37]

The analysis of the recent German Insurance Contract Act provides a valuable illustration of the exact impact of the IMD-mandated 'know your customer' duty, on the general conduct in the insurance business. It also illustrates the long process of extending the provisions on the duty to advise to digital contracting.

[33]Directive 2004/39/EC OJ (2004) L145/1 ('MiFID') and Commission Directive 2006/73/EC OJ (2006) L241/26 ('MiFID Level 2 Directive).

[34]For a comprehensive study of MiFID regulatory techniques see: Moloney (2008), chapters 4, 5.

[35]Cousy (2008), p. 505.

[36]Cousy (2008), p. 505.

[37]In favour of extending this duty on to insurers, Cousy (2008), p. 505.

5.3 The Example of German Law

A new German Insurance Contract Act[38] was enacted on 23 November 2007 and entered into force on 1 January 2008, repealing the Insurance Contract Act of 1908. Designed as a comprehensive codification of the law relating to insurance contracts, the German Insurance Contract Act governs all types of insurance contract except for marine insurance and reinsurance (Section 209 VVG). As regards the German Insurance Contracts Act's legislative history, Insurance Mediation Directive profoundly influenced the legislative approach to pre-contractual duties in the marketing of insurance products. The rationale of the 'know your customer duty', as laid down in Article 12(3) IMD, has been applied beyond the IMD's ambit to selling insurance through different channels. In what is perceived as an instance of 'Europeanisation of German insurance law', the VVG imposes a virtually identical scope of pre-contractual duties to advise clients on both insurers and insurance intermediaries.[39]

The provision of fundamental importance is Section 6(1) VVG that specifies the requirements and the scope of the insurer's pre-contractual duty to give advice. It may be useful to recite Section 6(1) VVG in full:

> If the difficulty in assessing the insurance being offered or the policy-holder himself and his situation gives occasion thereto, the insurer must ask him about his wishes and needs and, also bearing in mind an appropriate relation between the time and effort spent in providing this advice and the insurance premiums to be paid by the policy-holder, the insurer shall advise the policy-holder and state reasons for each of the pieces of advice in respect of a particular insurance. He shall document this, taking into account the complexity of the contract of insurance being offered.[40]

Nevertheless, the prevailing view assumes that Section 6(1) VVG does not provide for an unconditional (general) duty incumbent upon an insurer to explore and specify needs regarding insurance cover resulting from an applicant's situation and his or her requirements in any case.[41] Instead, Section 6(1) VVG is interpreted as requiring a specific reason (discernible cause) triggering the duty to advise.[42] Essentially, the insurer retains their original position of insurance seller, and the

[38]Gesetz zur Reform des Versicherungsvertragsrechts vom 23. November 2007, BGBl. Teil I/2007, Nr. 59 vom 29.11.2007, 2634–2678.

[39]See legislative materials BT-Drucks. 16/3945, 58. Ebers (2008) regards this as an instance of 'Europeanisation of German insurance law'; I discussed the Europeanisation of German Insurane Contract Law in the context of the duty to advise in Tereszkiewicz (2013).

[40]The English translation of this provision comes slightly adjusted from the English translation of the entire German Insurance Contract Act, accessible at the homepage of the German Insurance Association (GDV): http://www.gdv.de/Downloads/English/German_Insurance_Contract_Act_2008.pdf.

[41]Wandt (2016), p. 130, supports his position with an excerpt of legislative materials to that effect, cf. BT-Drucks. 16/1935, 24; Bruns (2015), p. 77.

[42]A so-called 'Anlassbezogene Beratung', a concept developed by German courts and endorsed in German scholarship, see Ebers (2008), Remark 3, with further references; Loacker (2015), pp. 245–247; Wandt (2016), pp. 130 et seq.

provision of Section 6(1) VVG should not turn him into an insurance advisor, unless specific circumstances arise.

It follows that the insurer's duty to advise depends on whether, considering the circumstances of a given case, there is a need for advice to be provided to the applicant.[43] In this respect, Section 6(1) VVG specifies 'the difficulty in assessing the insurance being offered', 'the policy-holder himself or herself' or his or her 'situation' as the relevant criteria in evaluating whether a duty to advise should be triggered in a given case. While the wording of Section 6(1) VVG may imply that these are the only criteria to be considered, the prevailing view tends to regard them as only illustrative, major examples.[44] It is submitted that a broad interpretation of these criteria will enable virtually all circumstances that may give rise to a duty to advise to be embraced.

As a necessary requirement, an applicant's need for advice must be recognisable to the insurer, which means no more than an 'objective' recognisability in a particular case. It is by no means clear, however, in the light of Section 6(1) VVG, which of the parties to a future insurance contract should be charged with being pro-active at the pre-contractual stage and to what extent: should the insurer actively explore the applicant's situation or is the applicant obliged to draw the insurer's attention to any of her particular needs?

Under Section 6(6) VVG, the duty to advise does not apply if the contract is negotiated with the policyholder by an insurance broker or if it is a distance contract within the meaning of Section 312c of the German Civil Code.

While the duty to provide advice under German law was a major advance in general, the exclusion of pre-contractual advice in distance contracts (online concluded contracts) appeared surprising. Distance contracts are contracts entered into between a business and a consumer solely by the use of means of distance communication as regulated in Section 312b(1) and (2) German Civil Code. The legislative materials justified the exclusion claiming that a duty to advise could not be practically fulfilled in distance contracting.[45] Clients, who wished to conclude insurance contracts online, it was assumed, should realise that they would obtain the necessary information in any case, but advice only if they explicitly requested it from the insurer. The exclusion of distance contracts from the scope of the duty to advise was critiqued as inadequate already at the time the Act was passed.[46]

The questionable exclusion of pre-contractual advice in distance contracts remained in force until the implementation of the new IDD to German law, which

[43]Wandt (2016), p 130.

[44]Scholarship on VVG provides guidance as to factors triggering the duty to advise, see e.g. Pohlmann (2015), Remark 38 et seq; Ebers (2008), Remark 13 et seq. See also Wandt (2016), pp. 130–131.

[45]BT-Drucks. 16/1935, 58; Bruns (2015), p. 78; Wandt (2016), p. 129.

[46]Ebers (2008), Remark 54; Loacker (2015), p. 244.

entered into force on 23 February 2018.[47] The revised Section 6 (6) VVG no longer contains an exclusion of duty to provide advice in distance contracts.

5.4 *Principles of European Insurance Contract Law*

The PEICL purport to be a 'Restatement of European Insurance Contract Law', modelled on American Restatements of the Law, in a manner that had previously been adopted by the Lando Commission on European Contract Law in the course of drafting its Principles of European Contract Law (PECL).[48] While the PEICL set a Common Frame of Reference of Insurance Contract Law in the EU, they also serve as a model law for the European or national legislators on insurance contract.[49] Further, the PEICL has been drafted with a view to constituting an optional instrument on insurance contract law, which can be chosen by parties instead of national insurance contract law.[50] An EU-approved optional instrument would enable insurance companies to offer their services through the EU internal market using a single, standard set of rules. At the same time, EU citizens would have a possibility to purchase non-national insurance products, thus simplifying insuring risks spread over different EU Member States. The aim and nature of the PEICL must be emphasised here, as they will be highly relevant for the interpretation of its specific provisions.

Section Two of the PEICL is entitled 'Insurer's Pre-Contractual Duties' and contains provisions that confer on insurers duties to provide information and advice to insurance clients. Article 2:201 PEICL deals with the provision of pre-contractual documents by an insurer containing relevant information concerning the insurance contract. This rule, which is modelled on the Third Insurance Directives, appears to reflect a well-established duty under the EU law.[51] From the perspective of this contribution, we focus on an insurer's duty to provide warning under Article 2:202 PEICL. It may be useful to recite paragraph (1) of Article 2:202 in full:

> When concluding the contract, the insurer shall warn the applicant of any inconsistencies between the cover offered and the applicant's requirements of which the insurer is or ought to be aware, taking into consideration the circumstances and mode of contracting and, in particular, whether the applicant was assisted by an independent intermediary.

[47] Gesetz zur Umsetzung der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb und zur Änderung weiterer Gesetze, BGBl. I 2017 S. 2789.

[48] See Heiss (2015), p. liii. with further references.

[49] On possible functions of PEICL Fontaine (2011), pp. 39–41.

[50] Batallier Grau (2014), p. 154.

[51] See the Third Insurance Directives and the Directive on distance marketing of financial services (2002/65/EC), see Comment 1 to Article 2:201 PEICL.

In contrast with Article 2:201 PEICL, the provision of Article 2:202 PEICL is undoubtedly classified as an individualised duty.[52] At first sight, Article 2:202 PEICL appears to constitute a rather limited duty to warn the potential policyholder about inconsistencies between the applicant's requirements and the cover offered. As Loacker rightly emphasises, Article 2:202 PEICL stands in the tradition of a notably reluctant concept of assistance toward the applicant.[53] The first of the two alternatives, as mentioned in Article 2:202 PEICL, namely the case of the insurer having positive knowledge—without having made any specific enquiry—of an inconsistency between the applicant's requirements and the cover offered is rather straightforward. There is no doubt that an insurer is then under a duty to warn.

More complex is the second alternative set out in Article 2:202 PEICL, namely that an insurer ought to be aware of the inconsistency mentioned above. Providing that an insurer ought to be aware of the inconsistency implies that an insurer is under a duty to establish or specify the applicant's wishes and demands as regards the insurance cover. This first step corresponds to a 'know your client' duty, as introduced in the EU law under IMD and, as will be shown below, refined and extended by the most recent IDD. It has been claimed that the insurer's duty to explore the applicant's needs and wishes implies a duty to advise the latter about the insurer's products that may suit applicants' needs. On such a reading, one could claim that Article 2:202 PEICL, although formally labelled 'a duty to warn', actually provides for a 'duty to advise'.[54]

Furthermore, the use of 'the circumstances and mode of contracting' as a criterion to define the duty to warn very clearly emphasises the open-ended character of Article 2:202 PEICL. In this respect, the Drafters' Comments (Comments) on Article 2:202 PEICL provide an example of face to face pre-contractual negotiations between an applicant and an insurer as a typical situation where the duty to advise will be most extensive. In this respect, an explicit reference to Article 12(3) IMD is made.[55] By contrast, insurer's duties to warn (advise) will be less extensive if there are no face to face negotiations between the applicant and the insurer or an agent representing the insurer.[56] Under such circumstances, the insurer will only be able to give fairly routine assistance. A further Comment claims that the pre-contractual duties of the insurer may be limited if the mode of contracting does not entitle the applicant to expect assistance.[57] There is no explicit reference to distance contracting or possible smart applications that may collect data from customers on their

[52]Loacker (2015), p. 258.

[53]Loacker (2015), p. 260, claims that instead of requiring such a proactive identification of the applicant's most important needs, any activity of the insurer is conditioned and defined by the special circumstances of the individual case.

[54]Armbrüster (2008), p. 788, claims that Article 2:202 PEICL obliges an insurer to make an enquiry about an applicant's specific demands as to insurance cover as well as advising her hereabout; Tereszkiewicz (2013), 250–251.

[55]Comment 4 to Article 2:202 PEICL.

[56]Comment 4c to Article 2:202 PEICL.

[57]Comment 4d to Article 2:202 PEICL.

insurance needs. The PEICL, including the accompanying Comments, do not take a clear position on the extent of the duty to warn or advise with regard to distance contracts, the significance of which is nowadays rapidly growing. It must be emphasised that in line with the PEICL's aim and scope, Article 2:202 is drafted in a rather open manner, presumably to ensure its acceptability on the part of market actors and legislators across the EU.[58] On the one hand, if PEICL is taken as a model law for a national insurance contract law legislator, the provision on a duty to advice, developing the idea of the flexible framework of Article 2:202, may be drafted in a much more detailed manner, taking explicit account of advice provision in digital contracts or by means of smart applications. On the other hand, if PEICL were to applied in its current version as a self-standing act on insurance contract law, one can question whether PEICL provisions on pre-contractual advice are detailed enough to deal with online provision of advice.

Another crucial issue regarding the regime of the insurer's duty under Article 2:202 PEICL concerns its temporal scope. Under Article 2:202 PEICL, the duty to warn is restricted to the stage 'when concluding the contract'.[59] Clearly, cases of inconsistent cover may arise during the contract period as well. Further, there is a case for extending the insurer's duty to explore the clients' needs to the contractual state given that the relationship between the parties has been established. A contractual duty of an insurer to explore and advise the client would undoubtedly be in line with the idea of a continuous information exchange between the parties that is greatly facilitated by new technologies.

Concluding, the position of the PEICL on the duty to advise must be perceived in the context of its unique legal character. On a continuous scale, they constitute a further development of the concept adopted in IMD, yet have been drafted in a fairly cautious manner.

5.5 Insurance Distribution Directive

Under Insurance Distribution Directive, which was discussed above, national legislations in EU Member States differed as to the scope of the insurer's duty to provide advice, in particular in online transactions. Uncertainty regarding advice in online transactions was summed up in an EIOPA opinion of 2015:

> EIOPA found issues where advice is required to be provided by national law or when so promoted, and the way insurance intermediaries or undertakings comply with their consequent duties when sales are conducted online. In this respect, distributors sometimes do not provide sufficient advice when distributing their products, or the information displayed is not

[58]Cf. Cousy (2009), p. 253. Loacker (2015), p. 260, stresses the 'striking flexibility' of the PEICL's approach.

[59]This is rightly emphasised by Loacker (2015), p. 262, who suggests that to close the emerging protection gap, it is advisable to interpret the PEICL under Article 1:104 in a way that promotes good faith during the contractual relationship as well.

fair enough. This may lead consumers to buy products that insufficiently meet their needs and requirements.

The Regulatory Approach of Insurance Distribution Directive

Enacted in 2016, the new Insurance Distribution Directive builds upon almost 15 years long 'life' of Insurance Mediation Directive, which it repeals. Given the objective of this contribution, it is necessary to examine the Insurance Distribution Directive (hereafter referred to as: IDD)[60] in respect of its approach toward digitalisation of the insurance sector. The regulatory approach of IDD rests on the assumption that insurance is sold as a product.[61] IDD regulates conduct of business by all distributors of insurance products, including insurance companies and has clear implications for the normative view of insurance contract in the national laws of EU Member States.[62] Most importantly, IDD lays down the information requirements and imposes certain conduct of business and transparency rules for insurance products distributors, including intermediaries or ancillary insurance intermediaries (e.g. travel agents or car rental companies), insurance companies and their employees. It is worthwhile to emphasise that IDD does not provide any guidance as to which contracts shall be deemed insurance contracts for the purposes of applying the IDD. Rather, the IDD adopts the 'conduct' approach and lays down conduct obligations of insurance products distributors. My analysis of IDD focuses on its provisions regarding pre-contractual and contractual duties to provide advice, with particular regard to digital contracting.

By comparison with the above-mentioned national acts on insurance contract law and its predecessor, IDD provisions do consider the growing importance of digitalisation of insurance business. According to the approach toward client protection that underlies the IDD, consumers should benefit from the same level of protection despite the differences between distribution channels.[63] Most importantly, this is reflected in the key concept of the IDD, that of 'insurance distribution'. The notion of 'insurance distribution', contained in Article 2.1 (1) IDD, is very broad. It clearly addresses most important issues resulting from digitalisation of insurance distribution. It is worthwhile to quote it in full:

> 'insurance distribution' means the activities of advising on, proposing, or carrying out other work preparatory to the conclusion of contracts of insurance, of concluding such contracts, or of assisting in the administration and performance of such contracts, in particular in the event of a claim, including the provision of information concerning one or more insurance contracts in accordance with criteria selected by customers through a website or other media and the compilation of an insurance product ranking list, including price and product

[60]Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast), OJ L 26, 2.2.2016, pp. 19–59.

[61]In particular Considerations 44 and 45 Directive 2016/97/UE.

[62]Cf. Considerations 5–7 Directive 2016/97/UE.

[63]Cf. Recital 6 and 8 IDD.

> comparison, or a discount on the price of an insurance contract, when the customer is able to directly or indirectly conclude an insurance contract using a website or other media.

The concept of 'insurance distribution' under IDD comprises comparison website. This is clarified in Recital 12 of the IDD that refers to comparison shopping websites.

> This Directive should apply to persons whose activity consists of the provision of information on one or more contracts of insurance in response to criteria selected by the customer, whether via a website or other media, or the provision of a ranking of insurance products or a discount on the price of an insurance contract when the customer is able to directly or indirectly conclude an insurance contract at the end of the process.

This means that comparison shopping websites in the field of insurance law that directly or indirectly enable consumers to conclude insurance contracts are subject to IDD and, most importantly, its provisions on rules of conduct toward consumers. From the perspective of consumer protection, this should be regarded as a major development, which also reflects political expectations toward European regulator.[64] For several years now, in particular in car insurance, comparison shopping websites have had profound impact on national markets in Europe.[65] The legal character and the quality of their services varied a lot and gave rise to concerns of consumer protection bodies.[66] The existence of statutory cancellation rights (cooling-off periods) and short duration of certain insurance contracts (e.g. car insurance) will certainly further stimulate the strong market position of comparison sites.[67] Certain aspects regarding advice provision are discussed below.

Furthermore, in what is a crucial improvement of the IMD, IDD considers digital communication between parties in its provisions on pre-contract information. In principle, pre-contractual information under the IDD has to be communicated to client on paper (Art. 23. 1 (a)) or a durable medium other than paper.

Still, the IDD authorises providing pre-contractual information by means of a website if it is addressed personally to the customer or if the following conditions are met (Art. 23 (5)):

(a) the provision of that information by means of a website is appropriate in the context of the business conducted between the insurance distributor and the customer;
(b) the customer has consented to the provision of that information by means of a website;
(c) the customer has been notified electronically of the address of the website, and the place on the website where that information can be accessed;

[64] According to EIOPA (2014), p. 7, there was strong support among the EIOPA Members for comparison websites to be regulated in a harmonised manner across the EU under the Insurance Mediation Directive—Recast (IMD2).

[65] EIOPA (2015).

[66] See EIOPA (2014); see also the study of the Deutsches Institut für Service-Qualität (2015). Both studies draw attention to different risks faced by comparison site users.

[67] Loacker (2015), p. 288.

(d) it is ensured that that information remains accessible on the website for such period as the customer may reasonably need to consult it.

Further, the IDD clarifies that the provision of information using a durable medium other than paper or by means of a website shall be regarded as appropriate in the context of the business conducted between the insurance distributor and the customer if there is evidence that the customer has regular access to the internet. The provision by the customer of an e-mail address for the purposes of that business shall be regarded as such evidence (Art. 23 (6) IDD).

Pre-Contractual Exploration and Warning

Arguably, the most important development under IDD may consist of extending pre-contractual individualised duties of exploration on all insurance product distributors, including online distribution of insurance products. Under Article 20 IDD, insurance distributors are obliged to specify the demands and needs of the customer and shall provide the customer with objective information about the insurance product.

Generally, one could claim that IDD does not introduce a general obligation to provide advice when an insurance product is sold. It is up to national legislators, as was the case under IMD, to lay down requirements (triggers) of a duty to advise, if such a duty is foreseen in national law, as is the case in Germany. This interpretation could be derived from Article 20, Sentence 3, which reads:

> Where advice is provided prior to the conclusion of any specific contracts, the insurance distributor shall provide the customer with a personalised recommendation explaining why a particular product would best meet the customer's demands and needs.

Consequently, one can claim that IDD does not impose a duty to provide advice, but it deals with the manner in which pre-contractual advice has to be provided.

With respect to online insurance transactions, this means that exploration and recommendations will be undertaken by means of electronic applications. Particular attention should be devoted to the issue of how triggers for the insurer's obligations to provide advice are laid down. With respect to non-standard insurance products, the examples of which have been provided in the introductory part of the contribution, needs and demands of clients have to be carefully examined. The key issue may be the right design of pre-contractual advice, which would convince users of its value with respect to 'new' insurance products. While there is no doubt that advice can be provided online, many online customers are used to easy and fast solutions and might not be interested in, for instance, full suitability exploration, which is necessary in case of insurance-based investment products.[68] The reason these customers do not show interest in full advice is, however, the lack of understanding of the complex nature of certain products, in particular new emerging products,

[68]EIOPA (2017b), p. 79.

offered on digital markets. It follows that design of pre-contractual exploration of needs and demands of insurance clients should aim at alerting clients about their need for advice.

Advice Provision and Competing Business Models

The question as to the duty to provide advice and its requirements in online distribution of insurance products has clear implications for different competing business models in the insurance sector. This can be illustrated with a recent example from Germany. Against the background of emerging insurance comparisons websites, Bundesverband Deutscher Versicherungskaufleute e.v. (BDV), a professional association of insurance traders in Germany, has pleaded for introducing the duty to provide advice according to the maxim 'No digital distribution of insurance products without advice'.[69] Following a suit asserting unfair competition brought by BDV, a Court of Appeal in Munich found in 2017 that the biggest comparison website in Germany, Check24, was obliged to inform its users in a more transparent manner about kickback payments it receives from different insurers whose products it markets.[70] Further, the Court recognised that Check24 was obliged to explore customers' needs and demands in respect of insurance while marketing insurance products. If one puts aside the aspect of fierce competition between traditional insurance intermediaries and digital insurance distributors, such as comparison websites, there is an important conclusion to be drawn. The fact that the law may not provide for pre-contractual advice in online transaction may indeed give rise to a mistaken view among insurance clients, as BDV points out, that insurance customers may easily and cheaply obtain insurance protection from online distributors. The central assumption underlying IDD, as illustrated above, renders such a perception incorrect.

Preliminary Assessment of IDD with View to Digitalisation

Undoubtedly, IDD considers the growing significance of digital distribution of insurance products. Yet, it is far too early to conclude whether, and to what extent, IDD responds to the needs of both insurance product distributors, on the one hand, and insurance customers, on the other hand. Further, there is no clear answer to the question as to whether IDD provisions are technology neutral. Rather, one should ask the question as to what 'technological neutrality' means with respect to insurance

[69] See Bundesverband Deutscher Versicherungskaufleute (2016).

[70] Judgment by Oberlandesgericht Munich of 6 April 2017, Case 29 U 3139/16, available under: http://www.gesetze-bayern.de/.

contract law.[71] If one understands 'technological neutrality' as not addressing the issue of whether insurance products are or should be sold online, but rather focusing on the content of the duties that apply to a sale of an insurance products regardless of the form, then IDD does not meet this definition. There are valid reasons for this choice of the EU legislator, given that the balance between traditionally concluded contracts and digital distribution is changing. Whilst IDD contains specific rules as to digital exchanges between the parties, it still rests on the paradigm of 'face-to-face' exchange between insurance product distributor and a customer. Further, extensive formal requirements provided by IDD in connection with pre-contractual documents and information may give rise to practical difficulties with respect to online services. What IDD possibly lacks are provisions dealing with specific features of on-line contracting in insurance matters forming together a distinctly different transactional environment. As Nancy Kim emphasises, efforts by online traders to create a 'smooth website experience' for consumers militate against consumer reading terms, which is particularly relevant in the domain of insurance products.[72] The EU legislator assumes that general consumer protection law acts that are applicable to online transactions will also provide sufficient protection for the insurance sector. Given its relatively narrow scope and the residual application of general contract and consumer law, including its provisions on online transactions, it must be stressed that the way in which IDD interplays with contract and consumer law will be crucial to its success in promoting safe and just application of InsurTech developments.

6 Conclusion

This contribution purported to show how online contracting has been integrated in the domain of the duty to provide advice in the European Union and German law on insurance contracts. As a general observation, it must be stressed that, with few exceptions, insurance contract law regulatory projects do not attach major importance to provisions on electronic formation. It is possible that legislators consider this a matter of general contract and consumer protection law and do not want to enact provisions that might deviate from general law on digital marketplaces. Given the rapid development of new business models, there may be a need for a gradual re-orientation of this perception. At a more specific level, explicit provisions dealing with duty of pre-contractual advice (exploration and warning) are a preferable solution to be accepted by future legislators, following the example set by the IDD. The dependency of the insurer's duties to provide advice on specific

[71] On possible meanings of 'technology neutrality' in legal discourse, see Maxwell and Bourreau (2015).

[72] Kim (2014), p. 265. For a discussion of the EU law approach to unfair terms in on-line consumer contracts see Brownsword (2018).

circumstances of the case in question, as is the case in PEICL, does not constitute a solution suited for regulating mass-markets transactions. While the courts' discretion may be exercised to impose duties to advise in specific cases of distance contracting, insurers, intermediaries and clients cannot be reasonably expected to be subject to judge-made rules on such specific questions as exploration of insurance needs and demands, as well as providing advice on these matters.

References

Armbrüster C (2008) Das Versicherungsrecht im Common Frame of Reference. Zeitschrift für europäisches Privatrecht 16:775–812

Basedow J (2015) Entwicklungen des Versicherungsvertragsrechts in Europa. In: Schnyder AK (ed) Versicherungsvertragsgesetz: Rückblick und Zukunftsperspektiven. Helbing Lichtenhahn, Basel, pp 37–50

Basedow J, Birds J, Clarke M, Cousy H, Heiss H, Loacker LD (eds) (2015) Principles of European insurance contract law, 2nd edn. Otto Schmidt, Köln

Batallier Grau JB (2014) The harmonization of European contract law: the case of insurance contracts. Conn Insur Law J 21:149–172

Brownsword R (2018) The E-Commerce directive and digital single market. In: Grundmann S (ed) European contract law in the digital age. Intersentia, Cambridge, pp 165–203

Bruns A (2015) Privatversicherungsrecht. C.H. Beck, München

Bundesverband Deutscher Versicherungskaufleute e.v. (2016). https://www.bvk.de/themen/publikation/position/idd-gelebter-verbraucherschutz-durch-professionelle-beratung-und-betreuung.492/. Accessed 19 Nov 2018

Capgemini. World Insurance Report 2017. Available at https://www.worldinsurancereport.com/

Clarke M (1997) Policies and perceptions of insurance. Clarendon Press, Oxford

Cousy H (2008) Les règles de conduit et le droit des assurances. In: Synthèses de droit bancaire et financier. Liber amicorum André Bruyneel. Bruylant, Brussels, pp 495–508

Cousy H (2009) Le sectur des assurances sera-t-il "mifidise" ? Bulletin des Assurances:245–253

Deutsches Institute für Service-Qualität (2015) Studie Kfz-Versicherungsportale, January 2015. https://disq.de/2015/20150115-Kfz-Versicherungsportale.html. Accessed 19 Nov 2018

Ebers M (2008) Kommentar zu § 6. In: Schwintowski H-P, Brömmelmeyer C (eds) Praxiskommentar zum Versicherungsvertragsrecht. Lexis Nexis Deutschland, Münster

European Commission (2016) Study on the role of digitalisation and innovation in creating a true single market for retail financial services and insurance. http://ec.europa.eu/finance/finservices-retail/docs/policy/160701-study-digitalisation-executive-summary_en.pdf

European Insurance and Occupational Pensions Authority (EIOPA 2014) Report on Good Practices on Comparison Websites, EIOPA-CCPFI-13/100 of 30 January 2014

European Insurance and Occupational Pensions Authority (EIOPA 2015) Opinion on sales via the Internet of insurance and pension products, EIOPA-BoS-14/198 28 January 2015

European Insurance and Occupational Pensions Authority (EIOPA 2017a) EIOPA-BoS/17-165. Roundtable: How technology and data are reshaping the insurance landscape. https://eiopa.europa.eu/.../08.0_EIOPA-BoS17-165_EIOPA_InsurTech_Roundtable_. Accessed 19 Nov 2018

European Insurance and Occupational Pensions Authority (EIOPA 2017b) Final Report on Guidelines under the Insurance Distribution Directive on Insurance based investment products that incorporate a structure which makes it difficult for the customer to understand the risks involved, EIOPA_BoS_17/204 11 October 2017

Feinman JM (2009) The insurance relationship as relational contract and the "Fairly Debatable" rule for first-party bad faith. San Diego Law Rev 46:553–571
Feinman JM (2015) The restatement of the law of liability insurance as a restatement: an introduction to the issue. Rutgers Univ Law Rev 68:1–32
Fontaine M (2011) An academic view. In: Heiss H, Lakhan M (eds) Principles of European insurance contract law: a model optional instrument. Sellier, München, pp 29–44
Heiss H (ed) (2012) Insurance contract law between business law and consumer protection. Dikke, Zurich
Heiss H (2015) Introduction. In: Basedow J, Birds J, Clarke M, Cousy H, Heiss H, Loacker LD (eds) Principles of European insurance contract law, 2nd edn. Otto Schmidt, Köln
Helveston M (2016) Consumer protection in the age of big data. Wash Univ Law Rev 93:859–917
Kim NS (2014) Situational duress and the aberrance of electronic contracts. Chicago-Kent Law Rev 89:265–288
Langer D, Rosenow J (2006) Konsumentenschutz bei der Vermittlung von Versicherungsverträgen in der Schweiz und in Europa. In: Liber Amicorum Bernd Stauder. Schultess, Bern, pp 195–226
Loacker LD (2015) Informed insurance choice? The insurer's pre-contractual information duties in general consumer insurance. Edward Elgar, Cheltenham
Maxwell WJ, Bourreau M (2015) Technology neutrality in internet, telecoms and data protection regulation. Comp Telecommun Law Rev 1:1–4
Moloney N (2008) EC securities regulation. Oxford University Press, Oxford
Pohlmann P (2015) Kommentar zu § 6. In: Looschelders D, Pohlmann P (eds) VVG-Kommentar. Carl Heymann Verlag, Köln
Tereszkiewicz P (2013) The Europeanisation of insurance contract law: the insurer's duty to advise and its regulation in German and European law. In: Devenney J, Kenny M (eds) The transformation of European private law. Cambridge University Press, Cambridge, pp 235–255
Wandt M (2016) Versicherungsrecht, 6th edn. Vahlen, München

New Technologies and Issues with Insurance Contracts in Japan

Tadao Koezuka

Abbreviations

ASCAA	Act on Securing Compensation for Automobile Accidents [Jidôsha Songaibaishô Hoshô Hô]
AI	Artificial Intelligence
CALI	Compulsory Automobile Liability Insurance [Jidôsha Songaibaishô Sekininhoken]
CALMA	Compulsory Automobile Liability Mutual Aid [Jidôsha Sonbaibaishô Sekinin Kyôsai]
CTG	Cardiotocogram
GIROJ	The General Insurance Rating Organization of Japan [Songaihoken Ryôritsu Sanshutsu Kikô]
GPGCAA	Government's Program Guaranteeing Compensation for Automobile Accidents [Seifu Jidôsha Songaibaishô Hoshô Jigyô]
IoB	Internet of Bodies
IoT	Internet of Things
MLIT	The Ministry of Land, Infrastructure and Transport [Kokudo Kôtsu Shô]
PAYD	Pay as You Drive
PHYD	Pay How You Drive
PLA	Product Liability Act [Seizôbutsu Sekinin Hô]
VAI	Voluntary Automobile Insurance [Nini Jidôsha Hoken]

T. Koezuka (✉)
Faculty of Law, Kagawa University, Takamatsu, Kagawa, Japan

Kobayakawa Law Firm, Takamatsu, Kagawa, Japan

Graduate Schoo of Law, Keio University, Tokyo, Japan

School of Law, University of Connecticut, Hartford, CT, USA

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_7

1 Introduction

Due to the remarkable development of information and communication technology (ICT) in recent years, topics such as autonomous driving technology, artificial intelligence (AI), and robots using Big Data are featured in the news daily in Japan. The influence of these new technologies on insurance contracts is significant. This chapter discusses several related problems occurring in Japan. The first problem is the accidents caused by autonomous vehicles, for which on-board AI recognizes, judges, operates, predicts and runs the vehicle. In Japan, a study group within the MLIT examined who should be responsible for an autonomous vehicle accident. The same argument can be considered for other AIs. Another issue is dynamic risk, which can be measured by ICT. New kinds of insurance measure dynamic risk using telematics and wearable devices, reflecting the risk in insurance premiums in real time. Because new insurance products collect personal information and analyze it to promote risk segmentation, reverse selection, privacy protection, and privacy infringement are also discussed. Furthermore, insurance should be protected against new technologies that enable the fusion of things with the human body. Finally, the problem of cyber risk insurance is addressed.

2 AI, Robots, Drones, and Cryptocurrency

2.1 Background

AI cannot perform the same level of activities as the human brain, but it is similar to the brain of a human being. AI functions by deep learning. In terms of this function, AI exceeds a personal computer and is different from things other than people. Manufacturers now produce smart goods in which AI is installed. AI is also responsible for interviews of job-seekers and is used in diverse fields.

Traditionally, under civil law, people have managed and controlled things, except disasters that they cannot control. Historically, humans have tried to control disasters using science technology. However, just like a disaster, humans cannot manage and control AIs. AIs autonomously learn a lot by deep learning and do not work as programmed. In addition, robots and drones, which are equipped with such AI, have been developed to operate autonomously out of human control. Who is responsible for accidents caused by malfunction of AI in the current legal system? These issues occur with autonomous vehicle accidents and have been discussed in Japan.

In addition, many kinds of cryptocurrency based on block-chain technology have been issued. Cryptocurrency is not real currency. However, it is unclear whether policyholders are allowed to pay insurance premiums in cryptocurrency under the Japanese Insurance Act. Furthermore, it is unclear whether an insurance company can pay insurance money in cryptocurrency under it. Because it is fundamentally a question of whether the “insurance as an economic system,” which exists as a

premise of insurance contracts, allows the principle equivalent to the balance by cryptocurrency.

2.2 *Autonomous Vehicles*

The Structure of Automobile Liability Insurance for Bodily Injury and Death in Japan

In Japan, automobile liability insurance is composed of liability insurance for body injury and death. This liability insurance is something like a two-story building; its basic foundation is CALI and CALMA,[1] which are based on ASCAA,[2] whereas its second story is "Coverage for Bodily Injury Liability" ["Taijin Baishô Hoken"], which is VAI. Furthermore, victims receive compensation under GPGCAA[3] when a victim is killed or injured in an accident caused by an uninsured, unidentified (e.g., hit-and-run), or stolen automobile and therefore cannot be compensated by both CALI.

For VAI, there are several kinds of coverages, including the following: (1) Coverage for Third Party Liability, which consists of Coverage for Body Injury Liability and "Coverage for Property Damage Liability" ["Taibutsu Baishô Hoken"],[4] (2) "Coverage for Self-Incurred Personal Accident"[5] ["Jison Jiko Hoken"], (3) "Protection against Uninsured Automobile"[6] ["Muhokensha Shôgai

[1]This mutual aid is operated by a cooperative, or a federation of cooperatives, established under the Agricultural Cooperative Society Act, the Consumers' Livelihood Cooperative Society Act, and the Act on Cooperatives of Small and Medium Enterprises. GIROJ (2017) at Glossary.

[2]The Japanese Act, "Jidôsha Songaibaishô Hoshô Hô", is translated as "Act on Securing Compensation for Automobile Accidents" by the Ministry of Justice. GIROJ translates it as "Automobile Liability Security Law".

[3]"Seifu Jidôsha Songai Baishô Hoshô Jigyô", or "Seifu Hoshô Jigyô", is translated as GPGCAA by Ministry of Justice. GIROJ translates it as the "Government's Automobile Liability Compensation Business".

[4]Voluntary Coverage is available for any kind of legal liability for an accident arising from the ownership, maintenance, and use of an insured automobile. GIROJ (2017), p. 1.

[5]The benefit is paid based on Coverage for Self-Incurred Personal Accident when no one is accountable for damages under ASCAA. GIROJ (2017), p. 20.

[6]When the insured is killed or has sustained permanent disability arising from an accident caused by an uninsured automobile this protection is to ensure the insured. Namely, the insured receives insurance money under this protection only if the insured is died or sustains permanent disability arising out of ownership, maintenance, or use of the uninsured automobile. GIROJ (2017), p. 22.

Hoken"], (4) "Coverage for Passengers' Personal Accident"[7] ["Tôjôsha Shôgai Hoken"], (5) "Bodily Injury Indemnity Coverage"[8] ["Jinshin Shôgai Hoken"], and (6) "Coverage for Damage to Own Vehicle"[9] ["Sharyô Hoken"].

Japan's Effort to Develop a Legal System for Autonomous Vehicles

When humans drive cars, they can control and operate the cars on the road using their abilities to recognize or predict danger, make an appropriate judgment, and implement proper operation. Compared with the efficiency of 10 years ago, there has been great improvement in AI performance. Namely, AI can recognize road conditions by cameras and sensors, analyze Big Data collected from sensors, make an appropriate judgment about what to do, and implement the proper operation, such as wrenching the steering wheel to the right in order to avoid a collision. AI now has the same car-driving abilities as a human.

The major automobile manufacturers are competing to develop autonomous vehicles at the international level. Japanese automobile manufacturers are vying for the lead. Meanwhile, the governments of the various nations have discussed international standards for safety of the autonomous vehicles at the WP29 in UN-ECE. The treaty aims to make several local regulations universal. Needless to say, a car's structure is also universal, being equipped with a shifter, brake, and accelerator. However, traffic regulation, traffic laws, and traffic rules are not universal. Rather, they are local in nature, reflecting each country's culture, history, religion, and ideas.

On April 17, 2018, the IT Strategy Headquarters of the Japanese Cabinet created an "Outline for Drafting the Laws Relevant to Automatic Operation" [Jidô unten ni kakaru Seido-Seibi-Taikô],[10] which aims to design laws and regulations for future traffic rules and liabilities arising from traffic accidents related to autonomous vehicles. For 2020, the Japanese Government will (1) draft the relevant laws, examining the Geneva Treaty to see if it is compatible with domestic traffic laws; (2) determine how to quickly provide protection to victims from civil liabilities to achieve swift implementation of more autonomous vehicles; (3) examine criminal

[7]The insured under this coverage receives the benefit when all of the insured occupy the space within the insured automobile is operated as a driver or passengers. GIROJ (2017), pp. 23–24.

[8]The insured is paid a benefit under Bodily Injury Indemnity Coverage, regardless of who is responsible for the accident. GIROJ (2017), p. 25.

[9]Coverage for Damage to Own Vehicle is available for damage arising from a collision, contact, running off the road, upset, collision with a flying or falling object, fire, explosion, theft, typhoon, flood, high waves, or any other accident on an all-risk basis.

[10]The IT Strategy Headquarters [Kôdo Jôho Tsuushin Network Shakai Suishin Senryaku Honbu] and the Strategy Council to Promote Utilization Data in Public and Private Sector [Kanmin Data Katsuyô Suishin Senryaku Kaigi] (2018), pp. 16–21.

responsibility and clarify the roles and responsibilities of drivers, users, personnel for safety, remote supervisors and operators, and entrepreneurs in legal systems for traffic rules and business for transport.[11]

With regard to civil liabilities, Japan has the ASCAA,[12] which gives victims the most comprehensive relief in the world. However, it is still unclear whether the ASCAA is available to victims of autonomous vehicle accidents. The first question is whether an autonomous vehicle is an "automobile" under article 2(1).[13] The second question is whether the use of an autonomous vehicle, which no driver makes run, is defined as "operation" under article 2(2).[14] Thirdly, it is unclear who is the "person that puts an automobile into operational use for that person's own benefit",[15] as this person is liable for compensation from damage arising from the operation of an automobile under the ASCAA.

The first question is whether an autonomous vehicle is an "automobile". The second question is whether its use is "operation". The third question is that the "person" who is liable to compensation is generally a "person in possession". Then, the ASCAA is available to victims when an autonomous vehicle causes an accident.[16] Therefore, victims of an autonomous vehicle accident will receive compensation from CALI and CALMA. The Japanese Government does not recognize need for reform of the ASCAA until 2025. Currently, the Japanese Government focuses on subrogation to automobile manufacturers by insurance companies after the companies pay indemnities to the victims. Namely, it is a task to examine the

[11]The IT Strategy Headquarters [Kôdo Jôho Tsuushin Network Shakai Suishin Senryaku Honbu] and the Strategy Council to Promote Utilization Data in Public and Private Sector [Kanmin Data Katsuyô Suishin Senryaku Kaigi] (2018), pp. 16–21.

[12]Law number: Act No. 97 of 1955. The basis for CALI and CALMA is the ASCAA. The aim of the ASCAA is to protect traffic accident victims. CALI and CALMA were established as a means to achieve that purpose. Therefore, CALI and CALMA are a kind of public insurance. That is to say, owners are obligated to insure their cars.

[13]In Article 2(1), the term "automobile" as used in this Act means an automobile as prescribed in Article 2(2) of the Road Transport Vehicle Act (Act No. 185 of 1951) (other than a small-sized special purpose vehicle manufactured for use in farm work) or a motorized bicycle as prescribed in paragraph (3) of that Article.

[14]In Article 2(2), the term "operation" as used in this Act means the use of an automobile in keeping with the way that such a machine is used, regardless of whether people or things are being transported.

[15]In Article 3, a person who puts an automobile into operational use for that person's own benefit is liable for compensation from damage arising from the operation of the automobile if this results in the death or bodily injury of another person. However, this does not apply if the person and the driver prove that they have exercised due care in connection with the operation of the automobile, that the injured party or a third party other than the driver has acted intentionally or negligently, and that there was no defect in automotive structure or function.

[16]Koezuka (2017), pp. 196–200.

structure for easily asserting insurance companies' subrogation right to manufacturers.[17,18]

Another discussion point is how victims should be protected when an autonomous vehicle accident is caused by hacking or cyber-attacking.[19] In this case, victims would be protected by GPGCAA, which is stipulated in article 71 to article 82-2 of the ASCAA. GPGCAA is available for an accident caused by a third party who has hacked or cyber-attacked AI equipped in an autonomous vehicle. In this case, the third party has no CALI and no CALMA for victims.

Finally, we consider case in which a bug in the installed software causes an autonomous vehicle accident. As long as the bug is recognized as a "defect" in the delivered product under the PLA,[20] manufacturers may be responsible for product liability.[21] Developers are separately responsible for tort liability[22] under the Civil Code.[23]

[17]The IT Strategy Headquarters [Kôdo Jôho Tsuushin Network Shakai Suishin Senryaku Honbu] and the Strategy Council to Promote Utilization Data in Public and Private Sector [Kanmin Data Katsuyô Suishin Senryaku Kaigi] (2018), p. 18.

[18]Before the "Outline for Drafting the Laws Relevant to Automatic Operation" was determined by the IT Strategy Headquarters of the Japanese Cabinet, the Study Group on Indemnity in Automatic Operation in the MLIT announced a report on the responsibility for accidents related to automatic operation on March 20, 2018. The comments on civil liability in the "Outline for Drafting the Laws Relevant to Automatic Operation" are based on a report by the Study Group. The report suggested that the accident recorder, which is mounted on an automobile and records when an automobile accident occurs, should be equipped in a autonomous vehicle in order to analyze an accident's cause or investigate the causes of an accident. MLIT (2018), p. 8.

[19]The IT Strategy Headquarters [Kôdo Jôho Tsuushin Network Shakai Suishin Senryaku Honbu] and the Strategy Council to Promote Utilization Data in Public and Private Sector [Kanmin Data Katsuyô Suishin Senryaku Kaigi] (2018), p. 18.

[20]Law number: Act No. 85 of 1994. In Article 3, the manufacturer, etc., shall be liable for damages arising from the infringement of life, body, or property of others that is caused by a defect in the delivered product that was manufactured, processed, imported, or provided with the representation of name, etc. described in item 2 or item 3 of paragraph 3 of the preceding Article. However, the manufacturer, etc., shall not be liable when the damages occur only with respect to such product.

[21]The decision on whether the "defect" exists in an autonomous vehicle or not is made at the time when the product is delivered, as "the defect in the delivered product" is stipulated in Article 3 of the PLA.

[22]The IT Strategy Headquarters [Kôdo Jôho Tsuushin Network Shakai Suishin Senryaku Honbu] and the Strategy Council to Promote Utilization Data in Public and Private Sector [Kanmin Data Katsuyô Suishin Senryaku Kaigi] (2018), pp. 18–19.

[23]Law number: Act No. 89 of 1896, Amendment of Act No. 44 of 2015. In Article 709, a person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable for compensation for any damages resulting in consequence.

Electronic Persons and Autonomous Vehicles

Some Japanese scholars are interested in the definition of a Legal Person, as discussed in the European Union.[24] They assert that an autonomous vehicle with AI should be given a legal personality or right capacity.[25] An autonomous vehicle seems to "recognize", "judge," "predict" and "operate" by itself, like a human. However, it is difficult to legally think that a car obtains rights and bears duties based on its intention, that a car can claim money from a person, or that a car can pay money to a person at a drive-through shop. Therefore, the intent is to create something like insurance in order to provide protection to a victim, consisting of registration fees paid by owners when they register an autonomous vehicle.[26]

Subrogation

As discussed previously, the focus of discussions on the future of autonomous vehicles is to allow insurance companies to exercise the right to obtain indemnity from manufacturers after paying indemnities to victims.[27] It is unclear if equipment for recorder media should be installed in an autonomous vehicle to allow insurance companies to exercise their right to manufacturers. It may be easier to clarify who is to blame for an accident when an investigating committee conducts a thorough investigation to determine the cause using recorder media.

Why is it necessary to create a scheme for excising insurance companies' rights to manufacturers? In my opinion, a person in possession is just a passenger, not a driver, in an autonomous vehicle. The cause of an accident is sought to fault an autonomous vehicle. However, a person, who takes the risk of inflicting damage to body injury or by death, does not pay CALI premiums and CALMA premiums; the person in possession[28] and user of the vehicle pays CALI premiums and CALMA premiums. Accordingly, insurance companies need a claim for manufacturers to pay indemnity. Insurance companies have no rational way to find and establish the fault of an autonomous vehicle. Thus, the proposal requiring manufacturers to equip autonomous vehicles with recorder media was suggested in the Report.[29]

In the near future, an automobile with internet devices or telecommunication devices will become to be more "connected" with some things (e.g., other cars, traffic lights, satellite navigation) through IoT. Several companies have a "cyber-

[24]EU Parliament (2017), p. 18.

[25]Nakayama (2015), p. 45; Tsuruhara (2015), p. 269; Shinpo (2016), pp. 2–3; Sato (2017), p. 98.

[26]Koezuka (2018a), p. 60.

[27]MLIT (2018), pp. 8, 10, 23.

[28]In Article 2(3), the term "person in possession" as used in this Act means the owner of an automobile, or any other person with the right to use an automobile, who puts an automobile into operational use for that person's own benefit.

[29]MLIT (2018), p. 8.

physical system" to optimize real space through analyzed data. As a result, it is rarely identified when, where, and how autonomous vehicles are attacked by viruses and why an autonomous vehicle accident happens. The car would be connected to a cyber-physical system even though an autonomous vehicle is equipped with recorder media. Therefore, liability insurance does not seem to be suitable for autonomous vehicle accidents because it does not clarify who is responsible and does not identify who is a cyber-attacker.

New Insurance Products

No-fault insurance is the most suitable voluntary insurance in the era of autonomous vehicles. No-fault insurance[30,31] is substantial accident insurance for bodily injury and death and requires three steps. The first step is that manufacturers receive immunity from product liability for several years only if an autonomous vehicle meets strict standards for safety.[32] The second step is that manufacturers sell this insurance, as an insurance window sales, and the insureds are all victims inside or outside of a car during an autonomous vehicle accident. The third step is that manufacturers pass the premiums for no-fault insurance onto the cost of autonomous vehicle s.

Needless to say, CALI would not be abolished because a manual cars will still operate on the roads in Japan in the near future. Victims who suffer bodily injury or die should be given protection by voluntary no-fault insurance.

Other AI, Robots, Drones, and Cryptocurrency

Human beings may suffer damage from other AIs more than from autonomous vehicles in the near future. AI will be incorporated into various things around us so that we can live a rich life. These other AIs are starting to be used in various industries. For example, security companies have introduced AIs for efficient investments to receive advice, and marketing companies make profits by utilizing AIs for market research. Furthermore, it is conceivable to implement an Act on Securing Compensation for AI Accidents just as ASCAA is implemented for automobile accidents.

Because the concept of AI varies widely in form and is difficult to define in scope, it is virtually impossible to legally define AI.[33] Therefore, it is challenging to establish the Act on Securing Compensation for AI as a general law. However, I

[30]Koezuka (2018b), pp. 87–89.

[31]Regarding physical damage of an autonomous vehicle, "Coverage for Damage to Own Vehicle" should make up its damage, regardless of fault or not.

[32]Kobayashi (2017), pp. 246–247.

[33]As with AI, it is difficult to define a robot and a drone.

believe that there is no choice but to establish the Act on Securing Compensation for AI in each individual field, such as medicine, marketing, and the investment field. Even so, as with investigating the causes of autonomous vehicle accidents, it is not possible to deny a hacker's attack; thus, the AI's decision process is a "black box". Substantially, the decision of AI is only one part of the automated process. It is extremely difficult to determine the cause of an accident by the damage and to clarify who is responsible for the accident. As a result, victims of AI accidents are appropriately covered by no-fault insurance, no matter who was at fault.

Second, in the future, various kinds of robots will become popular in society. We will come into contact with robots at various places, such as factories, hospitals, public transportation, schools, and so on. Along with that, someone will be damaged by the robot. The robot may suddenly become uncontrollable and may violently attack the victim. Food manufacturing robots may malfunction and manufacture foods that cause health damage. In these cases, from whom should the victim demand damages—the robot owner or the robot?

The victim wishes to receive compensation for damages received from the robot, but it does not clearly know what to do. Generally, victims can claim compensation for damages to the parties to the contract if there is a contractual relationship. If there is no contractual relationship, it is conceivable for the victim to request damages from the owner of the robot as the person who is responsible for the management. However, in the absence of a contractual relationship, it is difficult to prove negligence of tort-feasors when the victim pursues tort liability pursuant to Article 709[34] of the Civil Code of Japan for damages caused by a robot equipped with AI. Even if the victim is trying to pursue the manufacturer's product liability by insisting that the robot has "defects" under PLA and thereby caused damage, it is difficult for the victim to prove "defects" under it. Thus, the manufacturer is liable to bear no responsibility.

It is conceivable that, in the future, an Act on Securing Compensation for Robot Accidents may be established in order to guarantee damages claims by victims and to relieve the victims, like the ASCAA. However, it is so difficult to establish it. It is difficult to legally define a robot because there are various kinds of robots. For example, if all the robots were classified by their purposes, it is possible to recognize robots with various purposes, from medical robots or care robots to homicide robots or weaponized robots. It is also possible to recognize robots of various shapes, from humanoid robots to simple mechanical robots. By classifying all robots by their size, you can recognize robots of various sizes, from big robots used at construction sites and factories to molecular robots that are the same size as human cells.

As already mentioned, when a robot is programmed to work based on the AI but the victim suffered damage due to a defect or malfunction of the factory robot, it is extremely difficult for the victim to prove the defect. Thus, even in a robot accident,

[34] *See* Article 709 in Civil Code. A person who has intentionally or negligently infringed any right of others, or legally protected interests of others, shall be liable for compensation for any damages resulting in consequence.

the same problem arises as when exercising warrant rights from manufacturers to insurance companies in autonomous vehicle accidents. If the drones are moving by AI, similar problems arise. Therefore, if a legal processing scheme for autonomous vehicle accidents is established, it can be applied to the processing of other AI accidents, robot accidents, and drone accidents.

Regarding cryptocurrency and insurance contracts, the following can be said. The existence of legal "insurance as an economic system" is a precondition that an insurance contract is effective. If the "insurance as an economic system" does not exist legally, insurance contracts cannot be effective. As for the "insurance as an economic system," from the macroscopic viewpoint, it is necessary that the principle equivalent to the balance is established. From a micro viewpoint, it is required that the principle of equal benefit obligation benefits be established between policyholders and insurers.

It is unclear whether the principle of balance of payment and the principle of equal benefit obligation benefit can be maintained, even if the policyholder pays the insurance premium in the cryptocurrency and the insurer pays the insurance money in the cryptocurrency at the time of payment of the future insurance payment. Cryptocurrency, which is not managed by a central bank, is based on the new technology of block chain, in which record information is released and cannot be altered. For example, a dollar-denominated life insurance contract, in which the policyholder pays US dollars and the insurer pays insurance money in US dollars at the time of insurance payment, has been sold in Japan.

I believe that a cryptocurrency insurance contract is valid as long as policyholders pay insurance premiums in cryptocurrency and insurers pay insurance money in cryptocurrency at the time of insurance payment. However, for example, if the policyholder pays insurance premiums in Japanese yen and the insurer pays insurance money in cryptocurrency at the time of insurance payment, or if the policyholder pays the insurance premiums in cryptocurrency and the insurer pays the insurance money in Japanese yen when paying insurance money, it is not possible to maintain the principle of balance of payments and the principle of equal benefit obligation benefit.

3 Measurement of Dynamic Risk

3.1 Background

Several types of telematics insurance have been sold by insurance companies. This insurance uses new technology and is characterized by measuring risk in real time. That is, risks are inherently changing naturally. Conventionally, insurance companies cannot measure risks technically in real time. However, telematics—communication devices worn by the insured in the case of medical insurance or attached to a vehicle in the case of automobile insurance—make it possible to measure risk in real time. In this chapter, insurance that applies telematics is called telematics insurance.

In Japan, insurance companies sell telematics insurance in the field of automobile insurance and medical insurance.

3.2 Impacts on Automobile Insurance from Telematics

As in other developed countries, insurance companies in Japan sell telematics insurance. Telematics insurance uses vehicle-mounted communication devices, such as GPS or event data recorders, on the body of an insured automobile to record, transmit, and analyze driving information, such as sudden braking, acceleration frequency, and mileage. These devices analyze the information and measure the danger to calculate insurance premiums. Because longer travel distances increase the risk of a traffic accident, insurance companies in Japan already sell PAYD type automobile insurance[35] in which insurance premiums vary according to the actual mileage. As the traveling speed increases, the degree of roughness of the cornering increases, or the frequency of acceleration, sudden braking, and lane changes increase, the risk of occurrence of a traffic accident increases. Therefore, insurance companies sell PHYD[36] type automobile insurance, which calculates insurance premiums according to a driver's degree of risk.

There are two points hidden in PHYD type automobile insurance.[37] The first point is whether the insurance company can cancel the insurance contract if the driver repeatedly carries out extremely high risk driving after the conclusion of the insurance contract. In the event that a serious event occurs that will destroy the relationship of trust between the policyholder or the insured and the insurance company and it becomes difficult to continue the insurance contract, could the insurance company cancel the insurance contract based on grounds of a significant increase in danger outside the scope of underwriting risk? In the automobile insurance policy, the insurance company stipulates that if policyholder or the insured causes or is about to cause a serious event like insurance payment fraud, the insurance company can exercise the right to cancel the insurance contract.[38] However, a serious event does not include reckless driving to raise the accident occurrence rate.

The second point is as follows. Under the Insurance Act, it is stipulated that if the danger decreases markedly, the insurance policyholder or insured can request the insurance company to reduce the insurance premiums for a non-life insurance policy.[39] In addition, under the Insurance Act, it is stipulated that in the event of

[35]Hechtm (2008), pp. 1559, 1599; Johnsgar (2012), pp. 233, 241; Glancy (2014), pp. 1617, 1647–1648.

[36]Glancy (2014), pp. 1617, 1647–1648.

[37]Remark of Yamashita, Shinichiro (2018), p. 28.

[38]A provision similar to this clause in this automobile insurance policy is stipulated at Article 30 in Insurance Act [Hoken-Hô] (Act No. 56/2008).

[39]Article 11 of the Insurance Act.

increased risk, an insurance company can cancel a non-life insurance contract if certain conditions are satisfied.[40] However, for telematics insurance which measures risk in real time, the device automatically notifies the insurance company of the change in risk. Automatic notification by telematics in the cases of reduced risk and increased risk is made qualitatively different from countermeasures for increasing or decreasing the risk defined by the Insurance Act.

Therefore, the above-mentioned points that increase or decrease danger are examples that the Insurance Act has not been supposed to be under new technology.

3.3 Impacts on Medical Insurance from Wearable Devices

An insurance company sells Health Age Linked Medical Insurance in Japan. This medical insurance measures dynamic risk and determines insurance premiums just like telematics insurance in the automobile insurance field. An insurance company lends the wearable device to the policyholder and analyzes the causal relationship between the result of activity data,[41] medical checkup, or comprehensive medical examination, and the disease based on the data collected from the wearable device.[42]

Both life insurance premiums and medical insurance premiums are determined according to the level premium method based on the age of the insured and never change. Insurance premiums for Health Age-Linked Medical Insurance are determined based on the health age of the insured. The Health Age of the insured is measured and determined based on the daily insurance activity data. However, because the health age fluctuates, the insurance premiums also change conjunction with it.

Personal information of the insured person is collected from the wearable terminal, so it is necessary to pay sufficient attention to the handling of personal information. Because privacy may be infringed, privacy protection is also required. The same is true for telematics insurance.

[40] Article 29(1) of the Insurance Act.

[41] Activity data is (1) biological information such as daily blood pressure and pulse rate, (2) living information such as daily number of steps/walking distance, burned calories, exercise time/exercise amount, sleeping time and quality, meal etc.

[42] Suzuki (2015), p. 33; Kametsu (2016), p. 18 et seq.

4 Fusion of Things and Bodies

4.1 Background

In 2045, the average life expectancy is expected to reach 100 years by elucidating the mechanism of aging by analysis of genetic information and advances in regenerative medicine. For example, artificial joints, artificial hands, and prosthetic limbs are transplanted to the human body, the objects are organically combined with the objects in the human body, genome editing is performed and the function and health of the body are maintained.

The influence of the fusion of things and the human body on insurance, as well as the relationship with accident insurance are examined in the following section, taking a prosthesis as an example.

4.2 Impacts from Prosthesis

In the case of non-life insurance contracts, the number of objects of insurance that are connected to the Internet (IoT) increases not only in automobiles but also in household electronics, such as buildings, televisions, refrigerators, and the like. However, the insured of a life insurance contract and accident and disease insurance contract for fixed benefit collect activity data from the wearable device connected via the internet. Moreover, in the future, human beings may replace smartphones with micro-chips or nano-chips in the human body. In this way, the human body in which the chip is transplanted and connected to the Internet is said to be the IoB.[43]

Can the policyholder insure its autonomous vehicle, its smart house and its nursing robot against damage with a non-life insurance company? Because they are equipped with AI to optimize a real space by deep learning, diffrent from a traditional vehicle, house and a machine.

When the human body is connected via the Internet, sophisticated artificial joints and artificial organs connected to the brain may be implanted in the human body. When a prosthesis (prosthetic limb, artificial limb or finger) is worn on the human body, it will be impossible to divide it into things. However, could it be regarded as a part of the human body? For example, a person wearing a myoelectric prosthetic hand will be able to freely move a prosthesis by transmitting the myoelectric signal generated from the command of the brain to the artificial hand. If such a prosthesis is damaged by a sudden, accidental, and eternal accident, it is better to treat the prosthesis as a part of the body and compensate it from insurance benefits based on accident insurance without simply handling this prosthetic hand as a thing, or

[43] A concept to connect a fetus via the Internet has been proposed to rationally manage the perinatal period of the fetus, with an aim to maintain or improve the health of the fetus. This is called "Internet of Fetuses" (or "IoF"). Hara (2017), p. 12.

property and compensating for damage based on property insurance. If the prosthesis is damaged, a general accident insurance policy does not stipulate whether accident insurance will be applied.[44] In the case of an automobile accident, an insurance company pays indemnity the reasonable and necessary actual expenses a prosthetic hand based on CALI or CALMA in the event that a person with a prosthetic hand is involved in a car accident and the prosthesis is damaged.[45]

4.3 Impacts from Fusion of Things and Bodies

Ear, nose, or artificial organs made from IPS cells or ES cells by regenerative medicine cannot be viewed as objects of insurance, referred to as property insurance. Could the insurance company pay accident insurance benefits to the insured or beneficiary if the insured put a ball in an ear made of IPS cells and the ear breaks? Moreover, would the insurance company pay insurance benefits under a disease insurance contract to the insured or beneficiary if an artificial joint or artificial organ transplanted into the body of the insured has failed or been out of order and the insured suffers from a disease?[46]

As new technologies continue to develop, the fusion of things with the human body progresses more and more. This will cause problems as to what type of insurance should be applied to the fused human body. Traditional criteria that distinguish between personal insurance and physical insurance will not be able to guide the answer.

[44]In order to be paid injury insurance benefits, it is necessary for the insured to obtain the result of outpatient travel, admission to the hospital, surgery, residual disabilities, or death from injury. If only the prosthesis is damaged and the insured is not transported to the hospital, admitted to the hospital, undergoing surgery, or suffering from disability or death arising from bodily injury, then the accident insurance benefit will not be paid. Therefore, if the prosthesis is damaged and no bodily injury occurs, the insurance company could not pay the benefit.

[45]Insurance company indemnifies a victim for expenses for limb prostheses and other assistive devices according to "Criteria for Payment of Insurance Proceeds and Damages through Automobile Liability Insurance and Payment of Mutual Insurance Proceeds and Damages through Mutual Automobile Liability Insurance (Law Number: Public Notice of the Financial Services Agency and the Ministry of Land, Infrastructure, Transport and Tourism No. 1 of 2001; Amendment: Public Notice of the Financial Services Agency and the Ministry of Land, Infrastructure, Transport and Tourism No. 1 of 2010)". That is, regarding expenses for limb prostheses and other assistive devices, insurance company compensates for the reasonable and necessary actual expenses to produce and fit limb prostheses, dental prosthetics, ocular prostheses, eyeglasses (or contact lenses), hearing aids, crutches and other devices.

[46]Professor Hideaki Otsuka, Waseda University, has researched this theme on accident insurance and artificial joints.

5 Threats from Cyber Risk

Cyber risk insurance protects against loss caused by cyber-attacks. Cyber risk insurance is also an insurance product as a single unit, automobile insurance, or a product incorporated in war insurance and terrorism insurance.

Based on what we have discussed so far, the more that a society is data-driven, the more important that data management becomes because there is an increased threat of cyber risk. If a cyber-physical system is established in a special area, such as autonomous vehicle or medical care, AI functions on the basis of the data. If the data are destroyed, the function of the society will spiral out of control. For example, when a cooperative-type autonomous vehicle is traveling and a server bidirectionally communicating with the in-vehicle AI of the automatically driven vehicle suffers a cyber-attack, a car accident will occur if the autonomous vehicle cannot be automatically controlled, and many people may suffer.

In a data-driven society, it is very important to thoroughly implement cyber security. If cyber security is broken and the data are destroyed, it causes various AIs to become uncontrollable. Thus, it is necessary to devise insurance to compensate for damage caused by it. Cyber risk insurance has already been sold in Japan.

However, the problem is whether a cyber-attack is simply a third-party attack, terrorism, or war when the data in a cyber-physical system is subjected to a cyber-attack and thereby the AI that is operating properly with that data becomes uncontrollable. Could the insurers really be immune from obligation for paying insurance money in the case of a cyber-attack that affects the extent to which many autonomous vehicles accidents occur at the same time and a part of social functions stops? The insurers would be exempted from this obligation under an exemption clause for war if the accidents were caused by cyber-attacks and the cause of the accidents is recognized war. When the cause of the accident falls under the category of war in an exclusion clause of automobile insurance, the insurance company escapes payment of insurance money. In contrast, in war insurance or terror insurance, insurance companies need to pay insurance claims. If so, the question must be how to classify a cyber-attack, terrorism, or war.

6 Conclusions

Insurance companies can now use ICT to measure dynamic risks in real time. When this trend is thoroughly enforced, a person known to be high risk may enter into an insurance contract, and reverse selection may occur.

Next, under the principle of modern law, persons and things are clearly distinguished in the world of the law, which consists of rights and obligations.[47] Persons can obtain the right that they want and bear duty based on the manifestation of

[47] Ôya (2018), pp. 59, 68, 72.

intention, but things cannot do so. An insurance system is a way of dealing with risk that affects rights and obligations—in other words, it economically brings about changes in property situations in the legal world.

Even in the world of insurance, persons and things should be and are distinguished. Because persons have instincts to preserve the integrity of their bodies, regardless of whether the body is themselves or other people, it is difficult to try to defraud the insurance company by hurting themselves or another person's body or life. However, persons have less instinct to try to maintain the integrity of things. Thus, a person may destroy objects to obtain insurance money rather than attempting to obtain insurance money by harming others or their own bodies or life.

However, with the fusion of persons and things, the distinction between persons and things in insurance becomes relative. An example is an autonomous vehicle. An autonomous vehicle with AI is not being human being at all and has no ability to recognize legal effect; it performs a series of actions of recognition→judgment→prediction→operation. Traditionally, in the world of the law, when things affect human rights and duties, they have been treated as disasters. Now, because things, which perform cognition→judgment→prediction→operation based on AI, influence the rights and duties of persons, it is unclear whether it is appropriate to treat the event that affect rights and obligations as a disaster.

Moreover, elaborate prosthetic hands, which do not have a brain (like AI) and do not judge, are different from simple things. That is, these things reinforce human capabilities or expand functions to become part of the body. Therefore, I think that things should be recognized as quasi-body.

Finally, in a data-driven society, the importance of cyber risk insurance is enhanced. It is necessary to clarify the range of defense of cyber risk insurance that is incorporated into ordinary insurance (automobile insurance), such as consumer insurance, terrorist insurance, or war insurance.

References

EU Parliament (2017) Report with recommendation to the Commission on Civil Law on Robotics. Available at <http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html>

GIROJ (2017) Automobile Insurance in Japan. Available at: <https://www.giroj.or.jp/english/pdf/Automobile.pdf>

Glancy DJ (2014) Sharing the road: smart transportation infrastructure. Fordham Urban Law J 41

Hara K (2017) Global development of perinatal care management system, mobile CTG developed in Kagawa Prefecture [Kagawa Ken de Kaihatsu sareta Shûsanki Kanri Sisutemu, Mobairu CTG no Gurô-baru Tenkai eno Michi]. 114th Economic Research Institute Survey Monthly Report [Hyakujûshi Keizai kennkyûsho Chôsa Geppô] No. 358

Hechtm SB (2008) Climate change and the transformation of risk: insurance matters. UCLA Law Rev 55

IT Strategy Headquarters [Kôdo Jôho Tsûshin Network Shakai Suishin Senryaku Honbu] and the Strategy Council to promote utilization Data in Public and Private Sector [Kanmin Data Katsuyô Suishin Senryaku Kaigi] (2018) The Outline for drafting the laws relevant to self-driving drive [Jidôunten ni kakaru Seido-Seibi-Taikô]

Johnsgar AC (2012) Agents of change: how collaboration among insurers and the public sector can manage risk and foster climate-neutral behavior. Harv Law Policy Rev 6

Kametsu A (2016) New service that popularization of wearable terminals opens [Uearaburu Tanmatsu no Fukyû ga hiraku Atarashii Sâbisu]. Mutual Aid and Insurance [Kyôsai to Hoken] No. 702

Kobayashi M (2017) Issues on legal system for realizing autonomous vehicle [Jidôuntensha no Jitsugen ni muketa Hôseido jô no Kadai]. J Inf Process Manag [Jôhô Kanri] 60(4)

Koezuka T (2017) Risk measurement by using ICT and its effect to the automobile insurance contract [Hokengaisha no ICT wo Tsukatta Kikensokutei to Jidôsha Hoken nado eno Eikyô]. J Insur Sci [Hokengaku Zasshi] No. 636

Koezuka T (2018a) New technology and the legal issues on insurance law [Atarashii Gijutsu to Hokenhô no Kadai]. Jurist [Jurisuto] No. 1522

Koezuka T (2018b) Legal issues on autonomous vehicle and insurance company's claim for compensation to auto manufacturer [Jidôunten Jiko no Minjisekinin to Hokengaisha nado no Maker nado ni taisuru Kyûshôken ni kakaru Hôteki Shomondai]. J Insur Sci [Hokengaku Zasshi] No. 641

MLIT (2018) Study group report on liability for damages in automatic operation [Jidônten niokeru Songaibaishôsekinin nikansuru Kenkyûkai Hôkokushô]

Nakayama K (2015) The legal issues on autonomous vehicle [Jidôunten wo meguru Hôteki Kadai]. J Soc Automot Eng Jpn [Jidôsha Gijutsu] 69(12)

Ôya T (2018) Individuals who self-decide, Robot · AI [Robotto·AI to Jikokettei suru Kojin]. In: Yanaga M, Shishido J (eds) The laws of robots and artificial intelligence [Robotto·AI to Hô]. Yûhikaku

Remark of Yamashita, Shinichiro (2018) Round-table talk; disputed points and issues on insurance act [Zadankai; Hokenhô no Ronten to Kadai]. Jurist [Juristo] No. 1522

Sato M (2017) The legal issues on automatic operation [Jidôunten ni matsuwaru Hôteki Kadai]. Traffic Law Res [Kôtsûhô Kenkyû] No. 45

Shinpo F (2016) The subject of future analysis on robot law from several legal area [Hôryôiki Betsu ni mita Robot Hô no Kentô Kadai]. Legal Imperatives at Present [Toki no Hôrei] No. 2013

Suzuki H (2015) Current status and efforts of digitalization of the insurance industry — medical insurance linked to behavioral characteristics data— [Hokengyôkai no Dejitaruka no Genjô to Torikumi—Kôdôtokusei Data ni Rinkusuru Iryôhoken—]. Sompo Japan Nipponkôa Report No. 67

Tsuruhara Y (ed) (2015) The future of automatic operation 2016–2020 [Jidôunten no Mirai 2016–2020] (Nakayama, Koji writing). Nikkei BP

Part III
Cyber Insurance, Robots

Room for Compulsory Product Liability Insurance in the European Union for Smart Robots? Reflections on the Compelling Challenges

Aysegul Bugra

1 Background of the EU Initiative on Civil Law Rules on Robotics

The Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL))[1] was prepared by the European Parliament Committee of Legal Affairs Rapporteur Mady Delvaux and was publicised in 2016. Amongst several issues raised in the Report such as the impact of the rise of robotics on education and employment forecast,[2] intellectual property rights, flow of data[3] and ethical principles,[4] the main proposals made were in respect of civil liability rules that shall govern robotics with increased autonomous and cognitive features. Acknowledging the pace of the technological developments, the Report called upon the Commission to submit a proposal for a legislative instrument addressing the matters potentially to arise in the next 10–15 years in respect of robotics and

An earlier version of this chapter was awarded the Best Paper Prize by AIDA Europe in 2017 and was presented at the AIDA Europe Conference 2018 held in Warsaw, Poland in April 2018. The author is grateful to Ms. Helin Akbulut, Ms. Pinar Demiralp and Mr. Mucteba Faruk Ozdem for their research assistance on this chapter.

[1] Hereinafter referred to in the text as 'the Report'.

[2] The Report, paras 20–23.

[3] The Report, paras 10–12.

[4] The Report, paras 5–7.

A. Bugra (✉)
Dr. Nüsret - Semahat Arsel International Business Law Implementation and Research Center (NASAMER), Istanbul, Turkey

Transport and Insurance Law, Koç University, Istanbul, Turkey
e-mail: abugra@ku.edu.tr

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_8

artificial intelligence, which could be subject to an update later on.[5] In particular, the Report considered the below-mentioned issues which shall further be elaborated in this chapter with a focus on the challenges they may generate:

- The adoption of *strict liability* as a rule for all the parties involved in the liability chain,[6] including the manufacturers, owners, and users of robotics,[7]
- The introduction of a *compulsory insurance scheme* akin to the one existing in respect of liability arising from the harms caused by the use of motor vehicles, whereby the potentially liable parties would be required to take out insurance cover,[8]
- The compulsory insurance scheme being supplemented by a *compensation fund* where the latter would serve the twin purposes of guaranteeing compensation to victims where no insurance cover is in place for the acts of robots, as well as collecting investments and donations made in respect of smart autonomous robots.[9]

Based on the Report, the European Parliament issued a Resolution in February 2017 with Recommendations to the Commission[10] reiterating that the product liability rules currently applicable in the European Union under the Product Liability Directive[11] could merely cover damage caused by the harmful acts or omissions of robots provided that the victim proves the damage, the defect in the product and the causal link between the defect and the damage.[12] It was also further stated that once the parties who bear the ultimate responsibility are identified, their liability should be proportional to the actual level of instructions given to the robot. The Commission, in turn, agreed with the Parliament that an insurance system on robotics had to be well thought through, and also pronounced[13] that they would assess whether legislative action is necessary following the conclusion of stakeholder consultation on product liability challenges in the context of the Internet of Things & Autonomous Systems.[14] Following the Resolution and the Commission Response, the European

[5]The Report, para 25.

[6]The Report, para 27.

[7]This proposal will be considered under Sect. 3.2 below on product liability.

[8]The Report, para 31(a).

[9]The Report, para 31(b).

[10]European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL)), hereinafter referred to as 'the Resolution'.

[11]Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States concerning Liability for Defective Products.

[12]The Resolution, para AH.

[13]Follow up to the European Parliament Resolution of 16 February on Civil Law Rules on Robotics http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2017/11-20/A8-0005-2017_EN.pdf (last accessed, 2 November 2018).

[14]Follow up to the European Parliament Resolution of 16 February on Civil Law Rules on Robotics http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2017/11-20/A8-0005-2017_EN.pdf, at p. 3.

Parliament published a European Added Value Assessment in respect of connected and autonomous vehicles in February 2018.[15] In April 2018, a Commission Staff Working Document on liability for emerging digital technologies,[16] and in May 2018, the stakeholder and public consultation on the Product Liability Directive were completed and made public.[17]

The European Commission, following the Parliament's Added Value Assessment, opened a public consultation[18] and is currently working towards another Added Value Assessment on robotics and artificial intelligence, which is due in 2018–2019.[19] As in the case of autonomous and connected vehicles, the analysis of possible policy options for robots are presumably to be conducted in the light of the criteria of legal certainty, potential litigation burden, impact on consumer protection and innovation, degree of dependence on soft law, political acceptance and degree of regulatory intervention required.[20]

The initiative of the Parliament appears to be timely as some legislative steps have already been undertaken in some Member and non-Member States covering insurance of autonomous and intelligent systems.[21] A cautious yet determined approach to the regulation of civil liability rules and insurance would also need to be adopted in the European Union with a view to allow the sustainability of product innovation without compromising on the protection of the rights of product users. Careful steps would accordingly need to be made towards the implementation of a system adjustable to the changing needs, without overenthusiastically seeking to introduce

[15]A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles European Added Value Assessment, February 2018 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf (last accessed, 2 November 2018). Hereinafter referred to as "The Added Value Assessment on Autonomous Vehicles".

[16]Commission Staff Working Document - Liability for Emerging Digital Technologies- Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe SWD (2018) 137 final COM (2018) 237 final.

[17]Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products – Final Report, January 2018, p. 23. This Report is hereinafter referred to as "The Final Report on the Evaluation of Council Directive 85/374/EEC".

[18]European Commission Public Consultation on Recommendation on Connected and Automated Mobility (CAM) available at https://ec.europa.eu/info/consultations/public-consultation-recommendation-connected-and-automated-mobility-cam_en (last accessed, 2 November 2018).

[19]A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles European Added Value Assessment, February 2018 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf (last accessed, 2 November 2018), p. 14, fn 43.

[20]The Added Value Assessment on Autonomous Vehicles, p. 6.

[21]Automated and Electric Vehicles Act 2018 of the United Kingdom which received Royal Assent on 19 July 2018; Intelligent Robots Development and Distribution Act 2008 of South Korea, whereby certain insurance businesses are granted the right to operate a business for the purpose of providing cover for third party damages caused by intelligent robots.

future-proof rules that would hamper the speed of innovation. As the re-evaluation of product liability rules in the light of new technologies was carried out in the European Union as a priority, and because it was also proposed in the Resolution that product liability insurance should be made compulsory for the producers of robotics,[22] this chapter seeks to provide an assessment of the potential risks that may emerge from adopting a compulsory product liability insurance scheme.[23] Regard will accordingly be had on the challenges pertaining to the definition of smart robots and their classification as 'product' and 'service' (Sect. 2); on whether the functions of compulsory insurance would justify its introduction in the product liability sphere and how this may impinge on the moral hazard of producers (Sect. 3); and on what problems may the victims face in the claims process should such scheme be adopted (Sect. 4).

2 Challenges on Definition and Demarcation

The term 'robotics' used in the Report and the Resolution is seemingly meant to cover a wide range of devices. Given the numerous features they exhibit, clarity would be needed as to whether the same civil liability regime and insurance scheme shall be applicable in respect of the entirety thereof. Neither the Report nor the Resolution provide a common understanding as to the meaning of 'robotics'. This task is left to the Commission as regards cyber physical systems, autonomous systems, smart autonomous robots and their subcategories,[24] together with the assessment as to the very necessity of such definition. The European Parliament, although not having proposed a definition, agreed on several characteristics of 'smart robots' which were expressed as "the acquisition of autonomy through sensors and/or by exchanging data with its environment (inter-connectivity) and the trading and analysing of those data; self-learning from experience and by interaction (optional criterion); at least a minor physical support; the adaptation of its behaviour and actions to the environment; [and] absence of life in the biological sense".[25] Some assistance can also be offered by the approach to robots adopted in the Final Report on the Evaluation of Council Directive 85/374/EEC, which seeks to define it by reference to the Oxford Dictionary definition[26]: A robot is "a machine capable of

[22]The Resolution, p. 18.

[23]It is noteworthy that because the issues analysed in this chapter centre on robotics as 'products', the discussions on robots as artefacts classified as 'subjects' in law rather than 'objects' will not be considered. On that point, see the Resolution, para 59(f); see also Teubner (2018) on electronic personality of autonomous software agents.

[24]See the Resolution, para 1.

[25]The Resolution, para 1.

[26]See the Final Report on the Evaluation of Council Directive 85/374/EEC, p. 174.

carrying out a complex series of actions automatically, especially one programmable by a computer".[27] The avoidance of restrictive definitions was also clear in other contexts where it was provided that the term 'robot' could have differing meanings for everyone, and that it was increasingly difficult to explain their differences from other objects and systems given the pace in technology.[28]

Despite the underlying challenges on definition and demarcation, an almost evident category of smart robots is automated vehicles (AVs) which have already been considered by the Parliament as urgently requiring efficient rules applicable to the automotive sector.[29] Some assistance as to what may be covered under the regime proposed by the Parliament other than autonomous vehicles can be found by reference to the Final Report on the Evaluation of Council Directive 85/374/EEC. New technological developments considered therein are software embedded products; apps and other non-embedded software; Internet of Things; products shared with other users through collaborative platforms; devices for 3D printing; advanced robots and autonomous systems with artificial intelligence,[30] and software-based systems empowered with artificial intelligence.[31] Most of these systems are classified as 'product' within the meaning of the Product Liability Directive as they are 'movable' objects[32]—and tangible—with perhaps the exception of 'software' which can both be regarded as 'information' that is intangible by definition, and also having a physical aspect given that it can be embedded in devices.[33]

As per the proposals in the Resolution, the classification of a smart robot as 'product' would require its producer to purchase compulsory insurance for damages arising from defects in it. Where a smart device is not qualified as such, liability will be channelled to the providers of the service which would trigger a civil liability regime that is different than the one under the Product Liability Directive.

[27] https://en.oxforddictionaries.com/definition/robot.

[28] Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics, D6.2 Guidelines on Robotics http://www.robolaw.eu/RoboLaw_files/documents/robolaw_d6.2_guidelinesregulatingrobotics_20140922.pdf, at p. 15 (last accessed, 2 November 2018); Leenes et al. (2017), pp. 3–4. See also Palmerini et al. (2016), p. 79 for the view that autonomy, ability to work in physical environments and human-likeness may not constitute sufficient criteria for categorising 'things' as robots, on the ground that surgery robots are non-autonomous, softbots are non-physical and industrial robots are not human-like.

[29] Mapping the Cost of Non-Europe 2014–2019, p. 150. An insurance model proposed to be applicable in this regard was a special no-fault insurance scheme that supplements the injured party's entitlement to social security benefits, and that replaces civil liability claims for damages (The Added Value Assessment on Autonomous Vehicles, p. 115).

[30] This was explained as "physical machines perceiving their environment processing this information correctly and then carrying out a complex and adequate actions autonomously, e.g. advanced driver assistance systems or completely self-driving cars, these systems can also learn from their actions" in the Final Report on the Evaluation of Council Directive 85/374/EEC, p. 166.

[31] The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 166.

[32] Within the meaning of the Product Liability Directive Art. 2.

[33] The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 174.

The below section will therefore seek to shed light on the demarcation problem surrounding robots as 'product' with a view to assess whether the proposal on compulsory product liability insurance is realistically necessary and attainable in this respect.

2.1 Smart Robots as 'Product'

As much as the perception of robots being commercially available may seem sufficient in other disciplines to regard them as 'product',[34] the definition of 'product' in the Product Liability Directive is confined to movables as tangible objects,[35] leaving out intangibles or services.[36] The latter can nevertheless give rise to the liability of their manufacturers where domestic laws of the Members States contain adequate provisions applicable thereto. Moreover, certain technologies such as cloud computing systems could give rise to debates as to whether they shall be regarded as 'service' rather than as 'product'.[37]

The assessment of what artefacts could qualify as 'product' is a pertinent query for the purposes of insurance, particularly given that one of the proposals in the Resolution is the adoption of rules requiring producers to take out insurance, which has not been a common practice for this insurance line. The systems not qualifying as such yet are put into circulation as 'services' will not trigger the requirement for compulsory product liability insurance. They will nevertheless pose the risk of damage to third parties either in the form of death/bodily injury or property loss. The query that may accordingly ensue is whether third party protection through an efficient mechanism of compensation will be sought to be implemented through the requirement of compulsory commercial liability insurance in respect of robots that are considered as 'service'. Given that robots as 'product', i.e. as tangible objects, are more likely to cause both personal injury and property damages to third parties compared to robots qualified as 'service', a policy decision to require compulsory insurance (if at all) may be relatively more justified in the previous case than in the latter.[38]

[34]Engineering and Physical Sciences Research Council (EPSRC) Principles of Robotics, Principle 3. For a critique of the Principles, see Boddington (2017), pp. 170–176; Müller (2017), pp. 137–141.

[35]The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 175.

[36]The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 69.

[37]The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 27.

[38]Whether or not the introduction of compulsory product liability insurance is necessary and adequate has separately been elaborated below in Sect. 3.

A further grey area may appear with respect to smart robots which have not yet been put into circulation by their manufacturers. A product would need to be in circulation for attracting the application of the Product Liability Directive and any smart robot that is tangible and movable, although not yet in circulation, would therefore be subject to the national liability regimes covering damage caused to third parties.[39] A policy decision requiring compulsory insurance at the EU level would accordingly not extend to this circumstance. Provided the robot constitutes a 'final machinery' in the sense ascribed in Art. 2(g) of the Machinery Directive,[40] it would be subject to the health and safety requirements that would have to be complied with. It is also noteworthy that for this Directive to apply, the robot would need to be a "stand and function alone robot", and not a robot that would have to be incorporated into another system to operate.[41] Because smart robots as products not yet put into circulation—and not subject to the rules under the Product Liability Directive—would not pose the same level of risk that products put into circulation would do, requiring insurance cover for these circumstances would be hardly justified.

[39]Currently product liability rules applicable specifically to smart robots do not exist in any of the Member States, see also on this point the Final Report on the Evaluation of Council Directive 85/374/EEC, p. 37. Therefore, in theory, this eventuality would be subject to the national liability rules.

[40]Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast). The Machinery Directive aiming at harmonising the health and safety requirements applicable to machinery for consumer and industrial use as well as ensuring the free circulation of machinery within the EU has recently been evaluated as to its applicability to autonomous robots and artificial intelligence, see the European Commission Staff Working Document – Evaluation of the Machinery Directive – SWD (2018) 160 final. It was enunciated in this document that the definition of 'machinery' covered a wide range of devices spanning "from personal care robots or collaborative robots to complete automated industrial production lines", para 2.1.

[41]See the example of an industrial 'stand and function-alone robot' that constitutes a complete machinery under the Machinery Directive, as opposed to the example of an industrial robot designed without a specific application until incorporated into the final machinery that does not qualify as such, European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs Industrial Transformation and Advanced Value Chains Advanced Engineering and Manufacturing Systems, Guide to Application of the Machinery Directive 2006/42/EC Edition 2.1 – July 2017 (Update of 2nd Edition), p. 48.

3 Checks and Balances of the Scheme Proposed: Control of 'Moral Hazard'

The European Parliament proposed in their Resolution that "An obligatory insurance scheme, which could be based on the obligation of the producer to take out insurance for the autonomous robots it produces, should be established."[42] Currently, in the European Union, the duty to take out insurance exists in a number of instruments. To name but few, these are the Motor Insurance Directive,[43] the Regulation on Insurance Requirements for Air Carriers and Aircraft Operators,[44] and the Directive on the Insurance of Shipowners for Maritime Claims.[45] The proposals in the Resolution and the Report drew an analogy between the compulsory insurance system in place in respect of motor third party liability under the Motor Insurance Directive, and the one that is sought to be implemented in respect of smart robots.[46] The below sub sections seek to address whether this analogy is well-founded by reference to the functions of compulsory insurance and the nature of motor and product liabilities. They also provide an overview of circumstances which may impinge on the moral hazard of smart robot producers and how measures taken to control the moral hazard may affect third parties.

3.1 Functions of Compulsory Insurance and the Analogy Between Compulsory Motor Liability and Compulsory Product Liability Insurance

Compulsory insurance is one of the effective mechanisms in dealing with the compensation of third party losses effectively. Albeit it may be difficult to enumerate all the circumstances which would justify the adoption of a compulsory insurance scheme, certain common parameters can be noticed in analysing the areas where the duty to take out insurance was imposed. One of these parameters would be the protection of the potential wrongdoer who may not necessarily be in a position to effectively assess the likely advantages of having insurance[47] for whom the

[42]The Resolution, Annex to the Resolution: Recommendation as to the Content of the Proposal Requested, p. 18.

[43]Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability, Art. 3.

[44]Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators, Art. 4.

[45]Directive 2009/20/EC of the European Parliament and of the Council of 23 April 2009 on the insurance of shipowners for maritime claims, Art. 4.

[46]The Resolution, para 59(a); the Report, para 31(a).

[47]Faure (2016), p. 320.

insolvency risk may increase. This may be one of the reasons why motorists, who may often underestimate the potential consequences of driving both for themselves and others, are required to take out insurance. Similarly, insurance was also imposed in the European Union in respect of the operations of air carriers and aircraft operators, the operations of which have notably been regarded by the EU as carrying a great potential of insolvency risk.[48] The analysis of such potential was studied following the impact assessments conducted before the adoption of the relevant regulations,[49] and the operation of the insurance scheme adopted was assessed through minutely prepared reports.[50]

A second, and perhaps more obvious justification for compulsory insurance is the efficient protection of third parties affected by the actions of the wrongdoer. Compulsory liability insurance would in this sense serve the tort liability norm of compensatory justice. Third parties would particularly benefit from compulsory insurance where the tort liability judgment exceeds the wealth of the wrongdoer/insured: Instead of being under-compensated by the insured, they would recourse to insurance, provided they have a right of direct action against the liability insurers. The risk of the victim in failing to be fully compensated is accordingly sought to be avoided by the introduction of compulsory insurance, as is the case in the European Union under the Motor Insurance Directive.

The scheme proposed by the European Parliament begs the question of whether insurance for product liability shall indeed be made compulsory for the manufacturers of smart robots. It is noteworthy that this suggestion was also formerly raised by the UK Department for Transport (DfT) in their Consultation on Automated Vehicles. It was initially proposed by the DfT that compulsory motor insurance should be extended to cover product liability in circumstances where the motorists were not in charge of the vehicle (i.e. where the vehicle was on autonomous mode).[51] This had required the owner of the vehicle to take out insurance that covered both the manufacturer's and other entities' product liability which would have responded to

[48]The EU has specific legislation applicable to the measures that are required to be taken by insurance businesses for avoiding the insolvency risk, however compulsory insurance may be an effective mechanism as it has a dual effect of both protecting the policyholder ('wrongdoer' under a liability insurance policy) and the third parties affected by the acts of the policyholder.

[49]E.g. Communication from the Commission to the European Parliament and the Council - Insurance Requirements for Aircraft Operators in the EU - A Report on the Operation of Regulation 785/2004 COM (2008) 216 final.

[50]E.g. Commission Staff Working Document Impact Assessment - Accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability.

[51]Para 1.3 at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/536365/driverless-cars-proposals-for-adas-and_avts.pdf (last accessed, 10 November 2018).

the claims by the 'not-at-fault vehicle driver' while the vehicle was on autonomous mode, as well as the ones by the passengers and third parties.[52] This approach was later on abandoned in favour of another policy requiring less radical changes based on the response received from the automotive and insurance industries. The relevant policy advocated a single insurer model (covering both the driver's use of the vehicle and the AV technology) where the third party victim would have a right of direct action against the motor insurer, who would in turn have a right of recourse against the responsible party, where for instance the loss is caused by product failure.[53] This solution was advanced in the anticipation that product liability and motor insurers would in the future develop instruments so as to deal with the recourse stage as efficiently as possible, and that the government should have left the market dynamics play an active role without adopting an over-regulatory approach.

The obvious concern with respect to the analogy drawn in the Resolution and Report would lie in that in the case of product liability insurance, the insured will be a commercial entity (producer) and in the case of motor liability insurance, mostly a consumer with a rather limited wealth. Imposing a duty to take out insurance would therefore arguably be more justified in the latter case than in the former as there would be a greater risk that the damages would exceed the wealth of the insured and the third parties may accordingly be protected against this risk through compulsory insurance. One other remark could perhaps be expressed as regards robot producers having financial assets that are greater compared to the sources that the insurance companies can offer. In these types of cases self-insurance may arguably appear as a more convenient option as regards the level of protection guaranteed.[54]

A further reason why the abovementioned analogy may be regarded as rather unfit rests upon the distinction between the markets for motor vehicles and robotics: As much as the former is predictable in terms of insurable risks, the same is yet to be achieved with respect to the latter. Furthermore, there needs to be a sufficiently large number of insureds bearing risk exposure profiles that are alike for the insurer to refer to past risk profiling experience to accurately predict and accordingly quantify

[52]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/536365/driverless-cars-proposals-for-adas-and_avts.pdf, para 2.9.

[53]Pathway to driverless cars: Consultation on proposals to support Advanced Driver Assistance Systems and Automated Vehicles, Government Response available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581577/pathway-to-driverless-cars-consultation-response.pdf (last accessed, 22 September 2018), para 1.10.

[54]Faure (2016), p. 324 refers to the example of the Carbon Capture and Storage (CCS) Directive 2009/31/EC on the geological storage and carbon dioxide, where Art. 7(10) requires that applications for storage permits must be accompanied by proof of financial security; yet is flexible as to the form thereof which could include self-insurance. Multifarious alternatives to third-party liability insurance have also been advanced such as robot-related liability stocks (Huttunen et al. 2010, p. 8), and first-party insurance where the victims instead of manufacturers take out insurance (Calo 2011, p. 611, this suggestion is confined to the manufacturers of open robotic platforms for the actions and improvements of third parties. Calo also adds "The immunity could eventually sunset and be supplemented by a market for consumer robot insurance" at 611).

the risk.[55] Probabilities of accidents by robotics may not always be easily estimated given the scientific uncertainty surrounding them, which will in turn cause difficulties for insurers in setting fairly charged premiums. Particularly with respect to 'emergent behaviours' of robotics, i.e. "modes of behaviour which were not predicted by the designer but which arise as a result of unexpected interactions among the components of the system or with the operating environment",[56] the fundamental query for the insurers is how they will be placed to charge fair premiums where robots act in ways not even predictable for their programmers and trainers. This type of concern about smart robots which does not arise in the motor liability context would beg the question of whether other tools such as risk-sharing between operators[57] that is adopted particularly in respect of risks where knowledge of probabilities is limited, would be a more suitable option.[58] In the light of the foregoing, even if a preference is expressed in favour of a mandatory protection scheme, this should perhaps not be confined to compulsory liability insurance,[59] given that 'emergent behaviours' that may gradually become an area of concern in respect of predictability of robot actions would substantially make it difficult for insurance markets to offer affordable premiums.

Compulsory insurance is usually implemented as a solution to risks that would pose great danger to third parties, and it can therefore be argued that as the level of risks posed by different types of robots will not be identical, compulsory insurance may only be required and necessary for those robots that present a high level of risk of damage.[60] For instance, care robots would be more likely to pose a greater risk of bodily injury or death to third parties compared to robot toys, and whether the latter category should be subject to a compulsory insurance regime needs to be carefully thought through. In carrying out an impact assessment as to whether imposing compulsory insurance is necessary and justified in the context of robotics, circumstances such as the level of autonomy and predictability of the robot's behaviour, human presence in the environment where the robot operates, robot's physical capabilities and its connection with the environment may be taken into consideration.[61] However reason would dictate that due regard should also be had to whether

[55]Richardson (2002), p. 296.

[56]A term used in Arkin (1998), as mentioned in D6.2 Guidelines on Robotics, p. 23.

[57]Such as in the case of Protection & Indemnity Clubs whereby the shipowners contribute into a pool with the payment of 'calls' (premiums) and thereby form a risk-sharing tool to cover their liabilities against third parties.

[58]Skogh (1998), pp. 253–256.

[59]Summary of the public consultation on the future of robotics and artificial intelligence (AI) with an emphasis on civil law rules, available at http://www.europarl.europa.eu/cmsdata/130181/public-consultation-robotics-summary-report.pdf (last accessed, 2 November 2018) where a survey among stakeholders resulted in the finding that a majority thereof were not in favour of establishing an obligatory insurance scheme for damages caused by autonomous robots, nor of establishing a compensation fund.

[60]A similar view was expressed in Huttunen et al. (2010), p. 5.

[61]Huttunen et al. (2010), pp. 5–7.

insurance markets will easily accommodate a policy decision in favour of compulsory insurance. Oftentimes, developed and sufficiently large markets that are well equipped are required to cope with the demands of policyholders and third parties, and it would appear that the uncertainties surrounding robotics as well as different market characteristics in the EU are far from being reassuring in this regard.

3.2 Connection Between Strict Liability and Compulsory Insurance

The Product Liability Directive which would be likely to apply in establishing the smart robot producers' liability for third party damages[62] establishes a strict liability regime.[63] There may be strong correlations between strict liability and the requirement of compulsory insurance which has also been showcased in several jurisdictions through the introduction of compulsory insurance for liabilities occurring without fault.[64] From the 'insolvency' perspective, the injurer under a fault-based liability scheme would face such a risk once the *costs of care* would exceed its wealth, whereas a problem of underdeterrence would arise under strict liability as soon as the *damage* exceeds the injurer's wealth.[65] This latter situation would constitute one of the grounds for requiring compulsory insurance against the risk of underdeterrence by the injurer and accordingly that of the externalisation of costs.[66] A further justification for introducing compulsory liability insurance where strict liability applies may lie in that this could enhance incentives to reduce risk[67] which, in the context of producers of smart robots, could translate into incentivising the increase of safety levels of the products. Therefore, an analysis of whether the strict liability of producers under the Product Liability Directive should be complemented by a compulsory insurance scheme would need to be carried out to identify the advantages and drawbacks of such a policy decision.[68]

Product liability is an area where although strict liability is established, no general duty to take out insurance is imposed—the Product Liability Directive does not

[62]Unless a policy decision is made to the effect of drafting another instrument particularly aimed at covering the liability of producers of smart robots.

[63]For the view that setting the standard of liability as strict liability before a level of sophistication is reached in respect of products can have counter effects on product innovation in the European Union, see Palmerini et al. (2016), p. 83.

[64]Rubin (2016), p. 44; Cousy (2016), pp. 80–81.

[65]Faure (2006), p. 156.

[66]Faure (2006), p. 156.

[67]Shavell (2000), p. 178.

[68]Not all liability regimes applicable in the instruments requiring a duty to take out financial security currently in force in the European Union are based on strict liability. The view that favours that strict liability should be complemented by a compulsory insurance system would evidently not connote that fault-based liability may not be.

compel manufacturers putting their products into circulation within the European Union to take out insurance cover against potential third party claims. There is a large number of producers operating in the EU which are covered against strict liability arising from the Product Liability Directive under general insurance contracts (product liability insurance can be provided as a sub-section or endorsement of a combined public liability policy) with a considerable number of producers not even being insured against this risk.[69] The foregoing being the case, sectoral legislation applicable to the producers of certain products may impose a duty to provide financial security, a recent example of which appears in the Medical Devices Regulation.[70]

There may be several policy reasons for establishing strict liability, such as encouraging necessary incentives for investing in product safety; however to what extent this suggestion would prove right is controversial on the ground that it might rather persuade producers in purchasing insurance for matters outside their control.[71] Moreover, even where compulsory insurance is introduced, liability insurers will provide compensation to third party victims only where the victims are successful in proving that the product causing their loss was defective, and that there was a causal connection between the defect and the loss. It has already been acknowledged that these two instances constitute 53% of the cases where a third party claim was rejected due to their failure in discharging the burden of proof.[72] It would not be a fallacy to anticipate that this burdensome process would likely to be worsened in disputes involving robotics. Achieving the aim of protecting the victims may therefore lie in addressing this problem first, before a policy decision favouring the introduction of compulsory insurance can be made.[73] One should also not lose sight

[69]Only 22% of the enterprises are covered against strict liability arising from the Product Liability Directive under a product liability insurance contract, with 57% of the enterprises having a general insurance contract covering, inter alia, the product liability risks; and 21% of the enterprises are not covered against these risks under any insurance contract, see The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 16 fn 60.

[70]Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. Art. 10 para 16 provides "Manufacturers shall, in a manner that is proportionate to the risk class, type of device and the size of the enterprise, have measures in place to provide sufficient financial coverage in respect of their potential liability under Directive 85/374/EEC, without prejudice to more protective measures under national law."

[71]Posner R (2007) Economic Analysis of Law. Walters Kluwer cited in Leenes et al. (2017), fn 54 where it is also suggested that loss of reputation stands as a better incentive towards investing in safety.

[72]The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 23.

[73]Possibly by way of introducing a rebuttable presumption that the damage results from the defect, see Cauffman (2018), p. 5.

of the potential effect of introducing compulsory insurance on producers that may accordingly be incentivised to pass the cost of the compulsory insurance premiums onto the consumers in the form of an increase in product prices.

Product liability is mentioned as merely part of the network of liability that the Resolution proposed where the owners and users of robotics as well as programmers were mentioned as potentially liable parties. The list provided is possibly only of illustrative nature and could also cover whomever is involved in the chain having either given instructions to the robots or trained them. As much as the standard of liability of producers is relatively clear given the Product Liability Directive, whether the liability of the foregoing parties will be strict or fault-based is yet to be identified. In either case, the standard of liability established will be required to be adequate in addressing also robots' 'emergent behaviours'.[74] Determining the standard of liability is likely to require an analysis of the rules governing liability under the respondeat superior principle,[75] liability for the acts of children[76] and of animals,[77] as liability for the acts of smart robots is regarded to be analogous to the foregoing. One substantial challenge of this initiative would however lie in the lack of harmonisation of the tort law rules applicable in the EU jurisdictions.[78]

3.3 The 'Development Risk' Defence

Under the Product Liability Directive, manufacturers are not liable if they prove "that the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the existence of the defect to be discovered".[79] It has been argued in several instances whether unintended behaviour of smart robots resulting in a damage to third parties may constitute a 'defect' within the meaning of the Directive, and whether the development risk defence could relieve manufacturers of smart robots in a great number of cases on the ground that robotics technology is constantly evolving.[80] Before assessing the potentials for this suggestion, a general overview of the defence will be provided with a focus on

[74] D6.2 Guidelines on Robotics, p. 23.

[75] Hubbard (2014), pp. 1803–1872.

[76] Chopra and White (2011), pp. 128–130.

[77] Kelley et al. (2010), pp. 1861–1871.

[78] A comparative research project was conducted by a group of experts ('European Group on Tort Law') with a view to achieve a certain level of harmonisation among the tort law rules applicable in European Union countries. This initiative gave rise to the 'Principles of European Tort Law' (see European Group on Tort Law 2005) which may constitute a primary source of inspiration for approximating the EU Member States' tort laws.

[79] Art. 7(e). This defence is known as the 'development risk defence'.

[80] Courtois (2016), p. 289; Machnikowski (2016), pp. 17–110.

the judicial approach to the defence, the branches of industry that most rely thereon, as well as the frequency of such reliance thus far.

The defence aims at striking a fair balance between fostering innovation within Europe and the protection of consumers,[81] yet the Member States were given the option not to adopt the defence in their national instruments implementing the Directive.[82] The practice on derogation accordingly differed among the Members States: Luxembourg and Finland transposed the Directive by adopting the derogation without limitations whereby the derogation was made applicable to all categories of products and producers.[83] Hungary, in turn, adopted the Directive together with the development risk defence, which however does not apply in respect of medical products.[84] In Spain, manufacturers cannot invoke this exemption in respect of medical products and food products where the latter are produced for human consumption.[85] Moreover in France, the defence may not be relied upon where the damage is caused by an element of the human body or by products derived therefrom.[86] These national restrictions are accompanied by a strict interpretation of the defence by the Court of Justice of the European Union (CJEU) which confirmed that the defence would apply where the producer could prove that the objective state of knowledge that is at 'the most advanced level and not restricted to the relevant industrial sector' at the time the product was put into circulation was not such as to allow the discovery of defect in the product.[87] The defence is also not based on the unavoidability of the defect, but on the accessibility of knowledge by the producer.[88] It may be relatively clear that a confidential study that has not yet been published may not satisfy the accessibility test, however a more elaborate question may be whether a study published in a single country only in the local language could do so.[89] The defence is notably the most recurring liability exemption which has been triggered in 4% of the cases;[90] the foregoing hurdles in invoking the defence nevertheless ended up in a minimal number of cases where the producers were successful.

[81]The Final Report on the Evaluation of Council Directive 85/374/EEC provides that the removal of the development risk clause would not be beneficial for innovation in the EU according to the desk research conducted, see p. xvii.

[82]Art. 15 of the Product Liability Directive.

[83]The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 16.

[84]The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 16.

[85]The Final Report on the Evaluation of Council Directive 85/374/EEC, p. 16.

[86]Code Civil Français Art 1245-11: "Le producteur ne peut invoquer la cause d'exonération prévue au 4° de l'article 1245-10 lorsque le dommage a été causé par un élément du corps humain ou par les produits issus de celui-ci."

[87]ECJ C-300/95, *Commission v UK* [1997] ECR I-2649, paras. 26–27.

[88]*A v National Blood Authority* [2001] 3 All ER 289.

[89]Wuytz (2014), p. 31.

[90]According to the Final Report on the Evaluation of Council Directive 85/374/EEC the development risk clause was invoked more often in Italy, France, Hungary and Belgium, p. 24.

On the one hand, the proponents of this defence could argue that removing it would endanger innovation,[91] however the successful reliance thereon could risk that consumers are left without compensation. This would accordingly result in a protection gap for consumers and a potential consequent recourse to social security systems established in Member States; hence a plausible risk-sharing scheme as regards the scientifically unknown risks is necessary and unavoidable.[92] It is noteworthy that the problem of no compensation in the event where the development risk clause is successfully invoked will arise particularly in schemes where insurance is taken out for products other than automated vehicles, where a system is implemented whereby motor insurers will be the ultimate payers of claims where the manufacturers or their insurers rely upon the development risk clause so as to exonerate from liability.[93] Where no such scheme is in place and the clause is successfully triggered, third party victims will not be able to be compensated by insurers. Consistent successful reliance on the development risk defence by producers could also disincentivize a risk-averse producer to take out liability insurance, as its purchase decision would be made based on its assets in relation to potential liabilities, the likelihood of these liabilities and the degree of risk aversion.[94]

Whereas an option available is to remove the application of the clause in respect of AI and robotics amid concerns that third parties may be left uncompensated, chances are that this could raise product liability insurance premiums which may accordingly be passed onto consumers through price increases. This could also have a domino effect on R&D expenses whereby companies could possibly economise thereon and ultimately increase safety risks. Where, contrary to the proposal of the Resolution, product liability insurance is not compulsory and in theory no reliance is permitted for producers of robotics on the clause, it is submitted that it would be fairly difficult for producers to find a market to insure their development risks, given that they are rare and often result

[91]European Commission, Report from The Commission to the European Parliament, the Council and the European Economic and Social Committee, Fourth Report on The Application of Product Liability Directive, COM (547), 2011, p. 9. The Final Report on the Evaluation of Council Directive 85/374/EEC, pp. 82–83 also provides ". . .contrasting positions are held by businesses responding to the CATI survey with regard to removing the development risk clause: this possibility is viewed favourably by 43% of large firms, while the largest share of medium-sized firms (38%) thinks this removal would be disadvantageous. Small firms tend to think that this removal would be neutral (33%) or even disadvantageous (31%)."

[92]This view was expressed regarding connected and automated vehicles in Mapping the Cost of Non-Europe 2014–2019 available at http://www.europarl.europa.eu/EPRS/EPRS_STUD_603239_Mapping_fourth-edition-FINAL.pdf (last accessed, 10 November 2018), at p. 149.

[93]The UK Automated and Electric Vehicles Act 2018 which received the Royal Assent on 19 July 2018 adopted this approach, see 'Pathway to driverless cars: Consultation on proposals to support Advanced Driver Assistance Systems and Automated Vehicles, Government Response' available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581577/pathway-to-driverless-cars-consultation-response.pdf (last accessed, 2 November 2018), para 3.15.

[94]Shavell (2000), p. 174.

in severe damages.[95] On the other hand, a system where the producers can rely on the development risk defence and are required to take out product liability insurance would be likely to increase the moral hazard of producers who would be less incentivised to observe safety standards. In such a system, there would be a risk that third party victims may not be compensated unless the specific provisions making the insurance compulsory prohibit insurers to rely on the producers' defences.

3.4 Deductibles

A tool adopted for controlling the behaviour of insureds is, among others, to agree deductibles in insurance policies. In first-party insurance, deductibles serve the function of eliminating some claims altogether where they do not reach the figure stated in the deductible clause; however in liability insurance they prevent third party victims from claiming losses not reaching the deductible limits from insurers,[96] who are then left with the option of seeking them from the liable parties themselves. In theory, insurers may impose a high deductible in a product liability insurance policy to evade claims not reaching the stated limits and incentivise producers to adopt safety measures given that the risk of those claims would have been allocated to them. This could however create an unnecessary hurdle for third parties particularly where the type of loss suffered is death or personal injury that exceeds the deductible. In such a case, third parties would have to claim both against the producer and the insurer (should they have a right of direct action against insurers) for full compensation.

Further complications in addition to the above may also arise due to the differences in the wording used in deductible clauses for aggregating losses. In product liability policies, deductibles are often written either on per-occurrence or per-annum basis. Where the latter may be relatively straightforward in providing for the maximum amount to be borne by the claimant within a single policy year, the former would give rise to considerable controversy because of the multifarious meanings that can be attached to 'occurrence'.[97] For the purposes of damages arising from the acts of defective robots, the fundamental query would lie in whether (a) the defect that results in several harmful acts causing separate damages; or (b) each harmful act of the robot arising from the same defect causing separate damages; or (c) each separate damage, would qualify as 'occurrence'. The interpretation of the term 'occurrence' would accordingly dictate whether the deductible would apply to the entirety of damages arising from the same defect, or whether a different deductible would apply for each act

[95]Fondazione Rosselli, Analysis of the Economic Impact of the Development Risk Clause as provided by Directive 85/374/EEC on Liability for Defective Products - Final Report, p. 71.

[96]Schwartz (1990), pp. 316–317.

[97]In *Caudle v Sharp* [1995] C.L.C. 642, 648 it was enunciated by Evans LJ that for the purposes of a reinsurance contract "the occurrence out of which a claim arises, for loss suffered by the original insured, such as storm damage, flood damage or the like, *or in the case of professional indemnity losses, the negligent act or omission of the insured*" (emphasis added).

of the robot that results in damages. Due to the risk that varying meanings can be allocated to this wording in different European Union jurisdictions, unintended consequences in the treatment of third party victims may arise.[98]

However, where insurance is mandatory, deductibles may not be relied upon by insurers. The Motor Insurance Directive, for instance, dealt with this particular issue by providing that insurers are not allowed to require an injured party[99] to bear an excess.[100] A similar provision may also be adopted in the context of product liability policies for personal injury damages arising from a defect in the robotics manufactured to the effect that the insurers would not have the right to rely on contractual provisions—such as deductibles—to deny third party claims.

Property damages suffered by third parties would however be subject to a different system than personal injuries'. The Product Liability Directive states that producers are not liable for property losses suffered by product users which do not exceed €500, provided that the item causing third party loss is ordinarily intended for private use and was mainly used by the third party as such.[101] This figure was either interpreted as a threshold whereby losses not exceeding the figure would not be claimed, or as an excess that would have to be deducted from the indemnity.[102] In both cases, unless the property loss exceeds the figure of €500, no liability of the producer—and accordingly of the insurer—will arise. Accordingly, no compensation will be available for the third party. This situation will further be accentuated where the limit is increased in respect of property losses arising from the use of new technologies[103] which will potentially leave out a great number of small claims arising from the acts of robotics that will have to be borne by the victims. It is also noteworthy that where the property damage exceeds both €500 and the policy deductible, third parties would have to claim both against the producer (for the difference between €500 and the policy deductible) and against the insurer (for the excess of the policy deductible).

[98] An initiative to deal with the inconsistencies of different jurisdictions' approaches to aggregation wordings in the reinsurance context is undertaken by the drafting committee of the Principles of Reinsurance Contract Law (PRICL). Inspired by the work of the Project group 'Restatement of European Insurance Contract Law' that had resulted in the publication of the Principles of European Insurance Contract Law (PEICL) in 2009 (which was later on revised and was made public again in 2015), the aim of the committee is to provide a restatement of global reinsurance contract law principles.

[99] Defined as "any person entitled to compensation in respect of any *loss* or *injury* caused by vehicles" (emphasis added) and in theory, would also apply to third parties suffering property damages. However, see below the discussion on the role of deductibles in insurance policies covering the liability of producers for property damage where the Product Liability Directive would govern the liability of the producer.

[100] Art. 17.

[101] Product Liability Directive Art 9(b)(i) and (ii).

[102] The Final Report on the Evaluation of Council Directive 85/374/EEC, pp. 16–17. It is also noteworthy that in respect of property damage suffered by victims that is caused by vehicles stolen or obtained by violence, the Motor Insurance Directive grants an option to Member States to fix an excess of not more than €250 to be borne by the victim.

[103] See The Final Report on the Evaluation of Council Directive 85/374/EEC, p. xiii.

3.5 *Precautionary Measures*

Another option available to insurers for controlling the moral hazard of producers is to monitor their behaviour through policy clauses such as precautionary measures.[104] The rationale behind monitoring such behaviour rests upon the fact that the liability of the producer would trigger the insurers' own liability and any action taken towards decreasing the likelihood of this trigger would alleviate the insurers' risk. In the general context of product liability, however, it may be difficult for insurers to achieve this aim due to several reasons. Firstly, given that for the insurer's liability to arise the product would need to be defective within the meaning of the Product Liability Directive, the insurers' monitoring would have to aim to reduce the occurrence of defects. How this can be ensured is, though, far from being an easy task: defects are often developed during the production stage, however product liability insurance would often be purchased before the product is put into circulation, i.e. after the product has been developed. Accordingly, any steps towards monitoring the behaviour of the producer would merely have *ex-post* effect. Secondly, a clause seeking to monitor the behaviour of the producer by reference to compliance with the General Product Safety Directive[105] (GPSD—which operates *ex-ante*) may ensure a certain level of control; yet would arguably not grant sufficient protection for insurers: Non-compliance with safety requirements enshrined in the Directive would not necessarily result in the defectiveness of the product, or, from the insurers' perspective, compliance therewith would not in all circumstances prevent defect. Moreover, it is available to producers to allocate their risk of liability as well as expenses arising from recalling their defective products from the market onto liability insurers under 'product recall insurance'.[106] This could further disincentivise a producer having this type of cover from adopting a higher level of care in complying with the GPSD.

The above suggests that insurers would frequently stipulate precautionary measures to have an *ex-post* control, yet this arguably would not prove entirely useful for increasing product safety incentives that would have mostly occurred at the product development stage. An exception to this may however occur where a potential liability can be avoided if the producer is made aware that the safety of the product is called into question and acts to remedy the product deficiencies by for instance issuing additional user instructions. This latter possibility exists in the Medical

[104]These are also known as 'warranties' in certain jurisdictions such as the United Kingdom.

[105]Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety.

[106]This type of insurance is usually purchased separately than product liability insurance. The latter cover is sometimes offered as part of companies' commercial general liability insurance whereas the former is often not.

Devices Regulation[107] which imposes a duty to provide financial security for manufacturers of devices within the scope of the Regulation.[108]

Another problem that precautionary measures may pose is that the rules applicable thereto depends on the law governing the insurance contract. Accordingly, the control of moral hazard by insurers will depend on what consequences are attached to the breach of the precautionary measures as per the wording of the relevant policy, and any legislative rules that would be applicable to the clauses. The lack of harmonisation of the rules applicable to precautionary measures therefore stands as a hurdle which could obstruct the very aim of precautionary measures, i.e. to achieve deterrence: in jurisdictions where such clauses are strictly regulated and can be invalidated relatively easily, insurers would have to carefully draft their clauses so as not to lose the protection sought by their inclusion in the policies. Otherwise this would lead to the provisions not being applicable and lifting off the pressure on producers for observing safety standards. The diverse regulation of rules applicable to precautionary measures may further endanger the proportionate distribution of demands for product liability insurance among the insurance markets. This would notably beg the question of whether initiatives towards the harmonisation of insurance contract law principles such as the Principles of European Insurance Contract Law (PEICL)[109] could be an appropriate solution to this problem.[110]

Another issue is to what extent precautionary measures would disturb victims' rights against insurers where a right of direct action is granted to them for losses suffered from defective products. The obvious legal problem would lie in whether or not the outcome of any breach of precautionary measure by the producer (e.g. termination of the contract by the insurer, non-payment of any subsequent loss etc.) could be raised as a defence against the third party victim. As mentioned in the previous paragraph, the answer to this query would also depend on national law rules unless it is regulated at the EU level to avoid the risk of no compensation of third parties.[111] Such regulation would naturally be in the favour of victim protection, yet it could also be the subject of criticism by economists who would stress that

[107]Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[108]Art. 10.16 provides "Manufacturers shall, in a manner that is proportionate to the risk class, type of device and the size of the enterprise, have measures in place to provide sufficient financial coverage in respect of their potential liability under Directive 85/374/EEC, without prejudice to more protective measures under national law."

[109]The Principles of European Insurance Contract Law (PEICL) are a set of model rules which aims at establishing a common insurance contract law sphere across the European Union.

[110]Articles 4:101-4:103 contain provisions applicable to precautionary measures.

[111]PEICL Art. 15:101(2) provides "As against the victim, the insurer may raise defences available under the insurance contract unless prohibited by specific provision making the insurance compulsory. However, the insurer is not entitled to raise any defence based upon the conduct of the policyholder and/or the insured after the loss." This would connote that any breach of precautionary measure by the producer before any loss or damage to the victim has occurred may be relied on by the insurers as a defence against the victim.

the main aim of insurance is to cure the risk of underdeterrence and to remove risk from the injurer,[112] as opposed to principally protecting the victims.

4 Potential Limits to the Protection of Third Parties in the Insurance Framework

One of the policies behind the proposal of a compulsory insurance scheme for producers of smart robots was to ensure a higher level of protection for third party victims. This aim could be achieved to a greater extent through the introduction of a direct right of action against insurers. The below sections elaborate how the absence of a right of direct action against insurers or the Fund, along with how claims-made policies may operate in the insurance framework against this aim.

4.1 Lack of a Right of Direct Action Against Insurers

The right of direct action means that a party suffering injuries or damage for which another party is liable may bring an action against the liable party's insurer directly without having to sue that party. This right is usually granted to the victims in cases where there is a duty to take out insurance; yet where this is not required at the EU level, recourse would have to be made to the national law governing the insurance contract which may or may not grant it. Within the EU, third party victims have a right of direct action under the Motor Insurance Directive,[113] however this is not expressly provided for under the Regulation on Insurance Requirements for Air Carriers and Aircraft Operators.[114] At the international level, passengers may also bring a direct action against the insurers of carriers undertaking the carriage of passengers by sea under the Athens Convention as amended by the 2002 Protocol.[115]

[112] Faure (2006), p. 158.

[113] Art. 18.

[114] Regulation (EC) No 785/2004 of 21 April 2004 on insurance requirements for air carriers and aircraft operators, see also Directive 2009/20/EC of the European Parliament and of the Council of 23 April 2009 on the insurance of shipowners for maritime claims.

[115] Athens Convention relating to the Carriage of Passengers and their Luggage by Sea, 1974 as amended by the Protocol of 2002 to the Convention has been made applicable within the European Union through the Regulation (EC) No 392/2009 of the European Parliament and of the Council of 23 April 2009 on the liability of carriers of passengers by sea in the event of accidents. Art. 3(1) of the Regulation provides that the rules on insurance will be governed, inter alia, by 3 to 16 of the Convention as amended by the 2002 Protocol. Art. 4bis(10) of the Convention provides the right of direct action against insurers which will be applicable within the EU provided that the passenger claim is within the scope of application of the Regulation that is provided under Art. 2 of the Regulation.

The fact that recourse would have to be made to national laws where the EU legislative instruments are silent in this regard, risks of giving rise to inconsistencies in third party protection where some jurisdictions allow such direct actions in all cases[116] whereas others do it to a more restricted basis.[117] For a harmonised regime in the EU that is sought to be protective of third party victims, whether the right of direct action must be established in respect of both product liability and civil liability claims would need to be elaborated before the instruments regulating the insurance of robotics are implemented. Where the PEICL govern the insurance contract however, third parties would automatically benefit from the option of claiming directly against the liability insurers where the relevant criteria under Art. 15:101 are fulfilled.

PEICL would apply "where parties, notwithstanding any limitations of choice of law rules under private international law, have agreed that their contract shall be governed by it".[118] Where such agreement is made in favour of the application of PEICL, the provisions take effect in their entirety and the parties are not allowed to exclude the application of particular provisions.[119] It is also noteworthy that where contracts are governed by PEICL, no recourse to national law to restrict or to supplement the provisions of the PEICL is allowed with respect to the branches of insurance covered by PEICL,[120] i.e. liability insurance, among others. Their scope of application also cover insurance contracts which are concluded in accordance with a duty to take out insurance.[121] The aim of the PEICL was not to unify compulsory insurance law, yet to offer a uniform model law for insurance contracts.[122] An insurance contract governed by PEICL would therefore be subject to the provisions of PEICL on compulsory insurance, and would only be deemed to have satisfied the requirements pertaining to the duty to take out insurance if it complied with the specific provisions imposing the obligation[123] under the Community law or the law of the Member States. The latter laws will therefore prevail in case of any potential dispute between PEICL and the latter,[124] and so long as the PEICL comply with the

[116]E.g. French Code des Assurances Art. L124-3 provides "Le tiers lésé dispose d'un droit d'action directe à l'encontre de l'assureur garantissant la responsabilité civile de la personne responsable."

[117]For a list of the relevant rules adopted in the European Union Member States limiting the right of direct action to certain circumstances, see Basedow et al. (2016), p. 302 fn 42.

[118]Art. 1:102.

[119]Art. 1:102. This provision is subject to Art. 1:103 which provides a list of the mandatory articles which may not be derogated from; derogation from all other provisions may be allowed merely where such derogation would not prejudice the interests of the policyholder, insured or beneficiary.

[120]Art. 1:105.

[121]Art. 16:101 provides that the PEICL may be chosen by the parties of an insurance contract whereby an obligation to insure derives from the Community Law, the law of a Member State or the law of a Non-Member State to the extent allowed by the law of that State.

[122]Heiss (2016), pp. 309–310.

[123]Art. 16:101(2).

[124]Heiss (2016), p. 311.

relevant Community laws or national law rules on compulsory insurance, there would be no need of recourse to these laws.[125]

Given that the rules enshrined in the PEICL governing liability insurance seek to offer a high level of victim and policyholder protection,[126] it is expected that the provisions of the PEICL will oftentimes comply with the Community laws or Member States laws on compulsory insurance. In view of the foregoing, PEICL would be a fairly relevant model law particularly in respect of their rules on direct action of the victim against the insurer which is granted provided that either (a) the insurance is compulsory,[127] or (b) the policyholder or insured is insolvent,[128] or (c) the policyholder or insured has been liquidated or wound up,[129] or (d) the victim has suffered personal injury,[130] or (e) the law governing the liability provides a direct claim.[131] The valid incorporation of the PEICL into the insurance contract would be sufficient for this right to be applicable in respect of third party claimants against insurers if it is not already found in a legislative instrument that will govern the liability insurance for the acts of smart robots.

In addition to this right, further protection of third parties may also be achieved where the law governing the insurance contract contains rules requiring businesses providing insurance services to make payment within a given period of time or compensate losses arising from late payment.[132] Third parties having a right of direct action could accordingly sue the insurer and be compensated in reasonable time.

4.2 Lack of a Right of Direct Action Against the Compensation Fund

The suggestions made in the Resolution and Report were to the effect that the Commission should consider supplementing the compulsory insurance by a fund where the latter would serve the twin purposes of guaranteeing compensation to third parties where no insurance cover is in place for the acts of robots,[133] as well as to collect investments and donations made in respect of smart autonomous robots.[134]

[125]Heiss (2016), p. 312.

[126]See for instance Art. 15:101 on direct action against insurers and Art. 14:106 on bonus-malus systems respectively.

[127]Art. 15:101(1)(a).

[128]Art. 15:101(1)(b).

[129]Art. 15:101(1)(c).

[130]Art. 15:101(1)(d).

[131]Art. 15:101(1)(e).

[132]PEICL Art. 6:104 and 6:105. As provisions applicable to all contracts included in PEICL, they would also be relevant for liability insurance contracts.

[133]The Report, para 31(b); the Resolution, para 59(b).

[134]The Report, para 31(b).

Exploring the feasibility of establishing a compensation fund that would operate as complementary to a private insurance scheme would require an assessment of, including but not limited to, the below points:

- Whether the fund should cover all categories of smart robots or be category-specific (this part of the study would require an analysis of the key categories of smart robots that are more prompt to cause a major loss),[135]
- Whether it should operate at the EU level or be country-specific,
- Whether it should respond where no insurance is in place, where the insurance is not adequate to cover the third party claim, or where the insurer is insolvent,
- Who should contribute to the fund and in what proportions (whether a percentage of the annual net sales revenue would be adequate),
- Whether the contributors to the fund should enjoy limited liability because of having made such contribution,[136]
- Whether the right to operate in the robotics sector should be made subject to the granting of a license whereby the licensing bodies would assess the financial capability of the applicant according to the financial security provided,[137]
- Whether the unspent surplus of contributions, if any, should be redistributed to the contributors to be allocated to reinforce safety measures.

Compensation or guarantee funds are found in several sectors as the addressee of third party claims other than the insurers of the liable parties, or the liable parties themselves. Funds established to compensate third party claims arising out of the adverse effects of pharmaceutical treatment, oil pollution, or motor accidents currently operate at national, regional or international level.[138] Their exact function is usually determined by reference to the level of protection sought for the third party victims: supplementing the liability of the responsible party where the loss exceeds the party's limits of liability; and offering compensation where the responsible party succeeds to rely on an exclusion of liability, or where it fails to respond to the claim due to financial constraints such as insolvency, or where no insurance is in place for the liability in question. As much as compensation funds may operate as an 'insurer of last resort', they are separate entities than insurance undertakings, and provisions whereby the right of direct action is granted against insurers may not necessarily

[135]The Resolution, para 59(d).

[136]The Resolution, para 59(c).

[137]As in the Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC ('Offshore Safety Directive') Art. 4(2)(c).

[138]For examples, see the Swedish Pharmaceutical Insurer that is financed, inter alia, by pharmaceutical and R&D companies that respond to medication-related injuries of third party claimants; the Oil Pollution Compensation Fund (IOPC) established under the International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage 1992 (the 'Fund Convention' 1992) and which supplements the regime introduced by the International Convention on Civil Liability for Oil Pollution Damage 1992; uninsured and untraceable drivers' funds established as per the Motor Insurance Directive.

allow the exercise of such right against the funds. This has been pointed out[139] in respect of the Motor Insurance Directive Art. 18 which establishes such right against the insurance undertaking, yet neither this article nor any other one under the Directive covers the right of direct action against the guarantee funds. In addition to whether third parties will be allowed to have a right of direct action against the insurers, whether they will be permitted to directly claim against the fund would also need to be carefully thought through.

4.3 Claims-Made and Claims-Occurring Policies

Imposing a duty to take out insurance on producers with the aim of granting maximum protection for third parties may not always work in the favour of the latter where the contractual dynamics between the policyholder and insurer are such that they rule out some third party claims altogether. One of the ensuing queries would therefore lie in what types of defences would be available to the insurers when faced with a direct action by the victims. Under the PEICL, the insurers can raise all the defences available to them under the policy that they could have otherwise raised against the policyholder unless this is prohibited by the laws imposing the duty to take out insurance.[140] This being the case, no defence may be available to the insurers in respect of post-loss conduct of the policyholder[141] on the ground that the right of direct action arises with the occurrence of loss, and may not be affected by any subsequent conduct of the policyholder. Among these possible defences, precautionary measures were covered above.[142] The below is an overview of the impact of a policy written on claims-made or claims-occurring basis on third party protection.

As long as contractual flexibility permits and the relevant instruments imposing compulsory insurance do not regulate whether the relevant liability insurance policies should be made on loss occurring or claims-made basis, it may be argued that the intended level of safeguard may be difficult to achieve where a policy is written on claims-made basis. Such policies would entail a greater risk that the third party may not be compensated where, for instance, the claim was made at a time where there was no policy in place, or depending on the rules applicable to the contract, the cover was suspended. To the contrary, liability insurance policies on claims-occurring basis will be more in favour of third party victims as they will respond

[139]Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability, p. 128.

[140]Art. 15:101(2).

[141]Art. 15:101(2).

[142]See Sect. 3.5 above.

even after the policy is cancelled or elapses, provided that the event giving rise to the claim occurs during the policy period regardless of when the claim is made. Claims-made policies have been preferred particularly in respect of 'longtail' losses, i.e. where an injury or loss might not become manifest as soon as the act giving rise to it occurs.[143] For instance in the context of robots, exercising under the instructions administered by a malfunctioning care robot[144] could gradually result in an injury over time. Considering that the use of care robots will exponentially arise in the upcoming years, this type of gradual damages may not be rare and the choice of claims-made policies in such circumstances may operate to the detriment of third party claimants.

Product liability insurance contracts can in theory be concluded on either basis and the domestic insurance markets' established practice in this regard will play a role.[145] This may give rise to circumstances where third party claimants in some jurisdictions may have to bear the risks entailed with claims-made policies while claimants in other jurisdictions enjoy the relatively favourable claims-occurring based policies. Whether this danger of disparity should be averted through strict regulatory action by policy makers[146] or whether insurers should merely be encouraged to write occurrence coverage might become a subject of debate in the near future. For consumer liability insurance contracts, the definition of 'insured event' in the PEICL is made by reference to the event which gives rise to the liability of the insured/policyholder whereby the insurers would be required to respond even if the victim suffered a loss subsequent to the end of the policy period.[147] This rule is mandatory.[148] For commercial and professional liability insurance contracts, however, the rule only operates by default and parties are otherwise free to contract on claims-made basis provided that the

[143]The problems suffered by insurers facing asbestos claims in the United Kingdom rested upon the issuance of policies on claims-occurring basis whereby the insurers had to respond to claims even decades after the policies had elapsed. This subsequently paved the way for the abandonment of 'claims-occurring' policies for 'claims-made' policies, see on this point Mildred (2001), p. 244.

[144]It was submitted in Robinson et al. (2014), p. 581 citing "Mann JA, MacDonald BA, Kuo I, Li X, Broadbent E (2014) People respond better to robots than computer tablets delivering healthcare instructions (in submission)": "Research has found that an advantage of robotic technologies over other technologies is that people are more motivated to follow instructions. One study found that people were more likely to perform relaxation exercises if the instructions were administered by a robot in comparison to a computer tablet [65]".

[145]For instance, although in the United Kingdom there may be a tendency towards insuring product liability on a claims occurring basis, insurers may prefer offering claims-made policies for high risk products to limit their exposure.

[146]See Abraham (1986), p. 59 for the view that as long as there is ignorance of the claims future, imposing on insurers the writing of claims occurrence coverage may result in that they act as speculators whereas they are actually risk spreaders.

[147]Art. 14:107(1) provides "The insured event shall be the fact giving rise to the insured's liability that occurred during the liability period of the insurance contract unless the parties to an insurance contract for commercial or professional purposes define the insured event with reference to other criteria such as the claim made by the victim."

[148]Basedow et al. (2016), p. 297.

insurers are required to respond to claims not only occurring during the policy period, but also during an additional period of no less than five years.[149] The application of the latter rule to product liability insurance policies would appear to be protective of third parties without disproportionately disturbing the freedom of contract, and may therefore be regarded as an optimum middle course.

5 Conclusion

As much as the policy reasons behind the introduction of compulsory insurance may be the protection of third parties and the objective of achieving a higher level of product safety, it is submitted that a rushed and premature initiative towards this goal would constitute a caveat for product innovation. The role accorded to insurance in this setting would therefore need to be minutely elaborated. This chapter sought to demonstrate that compulsory insurance may be a remedy rather than an obstruction in cases where no fundamental uncertainties surrounding the definition of risks exist; the insurance markets are sufficiently large and developed to cope with the demands of insureds; and the costs of compulsory insurance premiums are not unnecessarily high to the point that producers would prefer externalising this cost by increasing the product prices. In addition to the foregoing, regulatory initiatives should consider the issue of direct action against insurers and assess whether a harmonised regime exists in respect of what circumstances would give rise to such right, as well as whether a balance is struck between contractual freedoms and necessary interventions in the insurance sphere.

A scheme not observant of the above may have an unintended effect of channelling producers to distribute their products outside of the European Union where no compulsory insurance would be required, which may in turn disturb the variety of robotics available in the EU market. This may significantly undermine the initial policy-making objective behind the introduction of compulsory insurance, i.e. ensuring the protection of third parties and product safety without hampering innovation of robotics within the EU.

References

Books

Abraham KS (1986) Distributing risk: insurance, legal theory, and public policy. Yale University Press

Arkin RC (1998) Behavior-based robotics. MIT Press, Cambridge

[149] Art. 14:107(2).

Basedow J, Birds J, Clarke M, Cousy H, Heiss H, Loacker L (2016) Principles of European Insurance Contract Law, 2nd exp. edn. Ottoschmidt
Chopra S, White LF (2011) A legal theory for autonomous artificial agents. The University of Michigan Press
European Group on Tort Law (2005) Principles of European Tort Law. Text and commentary. Springer, Wien, New York
Mildred M (2001) Product liability: law and insurance. Informa Law from Routledge

Book Chapters

Cousy H (2016) Compulsory liability insurance in Belgium. In: Fenyves A, Kissling C, Perner S, Rubin D (eds) Compulsory liability insurance from a European perspective. De Gruyter, pp 45–81
Faure MG (2016) Compulsory liability insurance: economic perspectives. In: Fenyves A, Kissling C, Perner S, Rubin D (eds) Compulsory liability insurance from a European perspective. De Gruyter, pp 319–341
Heiss H (2016) Compulsory liability insurance in the Principles of European Insurance Contract Law (PEICL). In: Fenyves A, Kissling C, Perner S, Rubin D (eds) Compulsory liability insurance from a European perspective. De Gruyter, pp 301–317
Machnikowski P (2016) An analysis of the state of the art in the era of new technologies. In: Machnikowski P (ed) European product liability. Intersentia, pp 17–110
Rubin D (2016) Compulsory liability insurance in Austria. In: Fenyves A, Kissling C, Perner S, Rubin D (eds) Compulsory liability insurance from a European perspective. De Gruyter, pp 17–44

Articles

Boddington P (2017) EPSRC principles of robotics: commentary on safety, robots as products, and responsibility. Connect Sci 29(2):170–176
Calo MR (2011) Open robotics. Maryland Law Rev 70:571–613
Cauffman C (2018) Robo-liability: the European Union in search of the best way to deal with liability for damage caused by artificial intelligence. Maastricht J Eur Comp Law:1–6. https://doi.org/10.1177/1023263X18812333
Courtois G (2016) Robot Intelligents et Responsabilité: quels Régimes, quelles Perspectives? Dalloz IP/IT 6:287–290
Faure MG (2006) Economic criteria for compulsory insurance. Geneva Pap Risk Insur Issues Pract 31:149–168
Hubbard FP (2014) "Sophisticated Robots": balancing liability, regulation, and innovation. Fla Law Rev 66(5):1803–1872
Huttunen A, Kulovesi J, Brace W et al (2010) Liberating intelligent machines with financial instruments. Nordic J Commer Law (2):1–14
Kelley R, Schaerer E, Gomez M et al (2010) Liability in robotics: an international perspective on robots as animals. Adv Robot 24:1861–1871
Leenes R, Palmerini E, Koops BJ et al (2017) Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues. Law Innov Technol 9(1):1–44
Müller VC (2017) Legal vs. ethical obligations – a comment on the EPSRC's principles for robotics. Connect Sci 29(2):137–141

Palmerini E, Bertolini A, Battaglia F et al (2016) Robolaw: towards a European Framework for robotics regulation. Robot Auton Syst 86:78–85
Richardson BJ (2002) Mandating environmental liability insurance. Duke Environ Law Policy Forum 12:293–329
Robinson H, MacDonald B, Broadbent E (2014) The role of healthcare robots for older people at home: a review. Int J Soc Robot 6:575–591. https://doi.org/10.1007/s12369-014-0242-2
Schwartz GT (1990) The ethics and the economics of tort liability insurance. Cornell Law Rev 75:313–365
Shavell S (2000) On the social function and the regulation of liability insurance. Geneva Pap Risk Insur Issues Pract 25(2):166–179
Skogh G (1998) Development risks, strict liability, and the insurability of industrial hazards. Geneva Pap Risk Insur Issues Pract 23:247–264
Wuytz D (2014) The Product Liability Directive – more than two decades of defective products in Europe. J Eur Tort Law 5(1):1–34

Working Papers

Teubner G (2018) Digital Personhood? The Status of Autonomous Software Agents in Private Law. Available at https://ssrn.com/abstract=3177096 or https://doi.org/10.2139/ssrn.3177096

Reports

A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles European Added Value Assessment, February 2018 available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf
Commission Staff Working Document Impact Assessment - Accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2009/103/EC of the European Parliament and the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability SWD/2018/248 final - 2018/0168 (COD)
Commission Staff Working Document - Liability for Emerging Digital Technologies- Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe SWD (2018) 137 final COM (2018) 237 final
Communication from the Commission to the European Parliament and the Council - Insurance Requirements for Aircraft Operators in the EU - A Report on the Operation of Regulation 785/2004 COM (2008) 216 final
European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs Industrial Transformation and Advanced Value Chains Advanced Engineering and Manufacturing Systems, Guide to Application of the Machinery Directive 2006/42/EC Edition 2.1 – July 2017 (Update of 2nd Edition)
European Commission Public Consultation on Recommendation on Connected and Automated Mobility (CAM), available at https://ec.europa.eu/info/consultations/public-consultation-recommendation-connected-and-automated-mobility-cam_en

European Commission, Report from The Commission to the European Parliament, the Council and the European Economic and Social Committee, Fourth Report on The Application of Product Liability Directive, COM (547), 2011
European Commission Staff Working Document – Evaluation of the Machinery Directive – SWD (2018) 160 final
European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL))
Evaluation of Council Directive 85/374/EEC on the approximation of laws, regulations and administrative provisions of the Member States concerning liability for defective products – Final Report, January 2018
Follow up to the European Parliament Resolution of 16 February on Civil Law Rules on Robotics. http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2017/11-20/A8-0005-2017_EN.pdf
Fondazione Rosselli, Analysis of the Economic Impact of the Development Risk Clause as provided by Directive 85/374/EEC on Liability for Defective Products - Final Report
Mapping the Cost of Non-Europe 2014–2019
Pathway to Driverless Cars: Consultation on proposals to support Advanced Driver Assistance Systems and Automated Vehicles, Government Response 2017 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581577/pathway-to-driverless-cars-consultation-response.pdf
Pathway to Driverless Cars: Proposals to Support Advanced Driver Assistance Systems and Automated Vehicle Technologies 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/536365/driverless-cars-proposals-for-adas-and_avts.pdf
Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics, D6.2 Guidelines on Robotics http://www.robolaw.eu/RoboLaw_files/documents/robolaw_d6.2_guidelinesregulatingrobotics_20140922.pdf
Report with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL))
Summary of the Public Consultation on the Future of Robotics and Artificial Intelligence (AI) with an Emphasis on Civil Law Rules. http://www.europarl.europa.eu/cmsdata/130181/public-consultation-robotics-summary-report.pdf

Legislative Instruments & Soft Law Materials

Automated and Electric Vehicles Act 2018 (UK)
Code Civil Français (France, consolidated version of 1 October 2018)
Code des Assurances (France, consolidated version of 22 November 2018)
Council Directive 85/374/EEC of 25 July 1985 on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States concerning Liability for Defective Products
Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety
Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)
Directive 2009/103/EC of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability
Directive 2009/20/EC of the European Parliament and of the Council of 23 April 2009 on the insurance of shipowners for maritime claims

Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC ('Offshore Safety Directive')
Intelligent Robots Development and Distribution Act 2008 (South Korea)
Principles of European Insurance Contract Law (PEICL)
Principles of Reinsurance Contract Law (PRICL)
Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
Regulation (EC) No 392/2009 of the European Parliament and of the Council of 23 April 2009 on the liability of carriers of passengers by sea in the event of accidents
Regulation (EC) No 785/2004 of the European Parliament and of the Council of 21 April 2004 on insurance requirements for air carriers and aircraft operators

The Idea of Robotic Insurance Mediation in the Light of the European Union Law

Marta Ostrowska and Maciej Balcerowski

1 Introduction: Insurance Intermediation in the Approaching Realm of Digitalization

New technologies are rapidly changing the nature of the financial infrastructure around the globe bringing innovation and digitalization to every aspect of the market. Because of the consequences of this revolutionary change, it is vitally important for the legislature to consider the legal implications and effects of such digitalization, without stifling its potential. Undoubtedly, the insurance industry is one of the businesses that are mostly affected by the new technologies. To keep up with the changing reality, the actors of the insurance market are also constantly innovating and trying to better meet the emerging needs and demands of the clients.

Nowadays, most digital innovation in insurance relates to the sales process, improvement of the internal processes, or claims settlement. Clearly, the variety of benefits stemming from the implementation of new technologies encourages (re) insurers and (re)insurance intermediaries to take the advantage of new technological developments to provide both innovative products and services and, consequently, become more competitive. For instance, such approach is reflected in establishing

M. Ostrowska (✉)
Insurance Law Institute, Faculty of Law and Administration, Warsaw University, Warsaw, Poland
e-mail: m.ostrowska@wpia.uw.edu.pl

M. Balcerowski
U-Solutions Underwriting, Warsaw, Poland

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_9

collaboration between the insurers and InsurTech startups to offer improved services to their consumers and to facilitate access to suitable insurance cover.[1]

Nevertheless, the benefits of new technologies cannot overshadow the sizable risks related to every change. From the regulatory point of view, the supervisors have a crucial role in ensuring that consumers and industry reap the benefits of digitalization. In short, it is important to find the right balance between maintaining high standards in consumer protection and fair competition on the one hand, and removing regulatory obstacles to stimulate innovation on the other. The European regulators have already taken the first steps to achieve these goals, e.g. innovation in the financial market has been declared priority for the UK Financial Conduct Authority (FCA).[2] In 2016, the FCA set up the "advice unit" to provide bespoke regulatory feedback to businesses planning to offer automated advice to the mass market (robo-advice). Now, it continues to research the potential flaws of robo-advisors and publish its resources to help improve already existing robo-advice services.[3]

Apart from the beyond legislative initiatives taken by the regulators, it is crucial to review the currently binding insurance law in terms of its adaptation to "absorb" new technologies. In this essay, the authors try to find the answer whether the Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution[4] (hereinafter referred to as the "IDD") ensures the compatibility with the digitalization of the insurance distribution and whether the robo-advisors fit its regulatory framework. Further, the goal of this essay is to open a discussion and encourage reviewing the insurance legislation as to its flexibility in terms of the new technologies.

[1]For further information of collaboration between the insurers and InsurTech startups, see Accenture's report *The rise of insurtech*, 28 April 2017, available at: https://www.accenture.com/us-en/insight-rise-insurtech.

[2]See e.g. drafted version of the speech by Bob Ferguson, Head of Department, Strategy & Competition Division, FCA delivered on 11 October 2017 during 2017 Annual Conference on Robo Advice and Investing: From Niche to Mainstream, available at: https://www.fca.org.uk/news/speeches/robo-advice-fca-perspective.

[3]FCA's Business Plan 2017/2018, available at: https://www.fca.org.uk/publications/corporate-documents/our-business-plan-2017-18.

[4]Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast) Text with EEA relevance (OJ L 26, 2.2.2016, p. 19–59).

2 The Idea of Robo-Advisor

2.1 Notion of Robo-Advisor

Although a variety of definitions of "robo-advisor" can be found in the popular press, on-line information services,[5] and legal literature,[6] to date there is no legal definition that could constitute a kind of "legislative benchmark". The European Union indeed sees the need for creating such definition which on the one hand would facilitate forming a legal regulation of the robo-advisory and on the other—would be flexible and not hindering innovation. This intention was expressed by the Committee on Legal Affairs in the Report of 27 January 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). According to the Report *a common European definition for smart autonomous robots should be established, where appropriate including definitions of its subcategories, taking into consideration the following characteristics: (i) the capacity to acquire autonomy through sensors and/or by exchanging data with its environment (interconnectivity) and the analysis of those data; (ii) the capacity to learn through experience and interaction; (iii) the form of the robot's physical support; (iv) the capacity to adapt its behaviour and actions to the environment.*[7] Here, it seems though that an attempt to create such definition might reveal pointless and simply fail because the concept to be defined is continually developing and might have countless manifestations that are difficult to predict.

With the above, for this essay we will use the term "robo-advisor" broadly—understood as any automated service used within the insurance distribution process that ranks, or matches clients to the insurance products on a personalized basis and that provides a personal advice or recommendation. Interestingly, the Polish supervision authority provides on its website an even wider and more general illustrative explanation of the term "robo-advisor" by referring to the form of automated financial advice which is based on the advanced algorithms using artificial intelligence and tools for the analysis of large data sets (Big Data).[8]

---

[5]See definition proposed by Forbes: https://www.forbes.com/sites/falgunidesai/2016/07/31/the-great-fintech-robo-adviser-race/#4524e79e4a6f; Lexology: https://www.lexology.com/library/detail.aspx?g=6962cb4f-f82a-4452-860c-fb0096dcd356; Business Insider: https://www.businessinsider.de/what-are-robo-advisors-robo-advice-2016-3?r=UK&IR=T.

[6]E.g. a definition of a robo-advisor proposed by P. Schueffel in the context of investment services, which is as follows: *A Robo-Advisor is a self-guided online wealth management service that provides automated investment advice at low costs and low account minimums, employing portfolio management algorithms.* See Schueffel (2017), p. 26; For further information on the problem of defining robo-advisors, see: Iannarone Nicole (2018), p. 149.

[7]Report of 27 January 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), p. 20, 3.

[8]Please note that the given definition of robo-advisor available at the Polish Financial Supervisory Authority website cannot be treated as its binding position or as a legal provision. See https://www.knf.gov.pl/dla_rynku/fin_tech/robodoradztwo.

2.2 The Benefits To Be Reaped of Robo-Advisors

Improved accuracy, minimization of human error or bias, and possibility to lower the costs of the insurance distribution are just a few of the many benefits associated with the expansion of robo-advisory in the insurance market.[9] Automation makes possible for the insurance services to have the potential to provide higher quality and more transparent advice to more people at a fraction of the cost of traditional human advisors.[10] This is because of the concept of machine learning that gives the computers the ability to learn without being explicitly programmed. Consequently, it offers an enormous improvement of the ability to analyze data, while also raises challenges to ensure non-discrimination, due process, transparency, and understandability in decision-making processes.[11]

2.3 Risks Related to Robo-Advisors

Originally, launching robo-advisors in the insurance industry was supposed to increase the efficiency of the distribution process, as well as its profitability, and to increase customer's safety. Moreover, the application of robo-advisors should mitigate or even eliminate the risk of causing damage to the client as no fallible "human factor" interferes. In theory, such risk is eliminated because robo-advisors "consists of" the algorithms which are to identify and reject cases of faulty adjustment of the insurance product, incorrect pricing, or a situation in which, because of the distributor's failure, the insurance coverage is suspended. Achieving the aforementioned goals would be theoretically possible if it is assumed that the underlying algorithms are not only flawless but are also able to predict all possible consequences.[12] Additionally, it should be assumed that robo-advisors (algorithms) would recommend the appropriate insurance product based on fully objective evidence. However, the observation of the IT systems already functioning within the insurance market neither accepts the above assumptions nor considers them correct. Hence, it seems that apparently the flawless concept of robo-advisory may at the same time be one of the basic threats for the clients using robo-advisors.

As to the risks related to the insurance distribution performed by robo-advisors, it is worth considering a relationship between the way in which the robo-advisor is programmed and the potential behaviors of the clients. To illustrate the possible

[9]Report of the Joint Committee of the three European Supervisory Authorities (ESAs) – EBA, EIOPA and ESMA on automation in financial advice, available at: https://esas-joint-committee.europa.eu/Pages/News/European-Supervisory-Authorities-publish-conclusions-on-automation-in-financial-advice.aspx.

[10]See Baker and Dellaert (2018), p. 714.

[11]Lech (2018), p. 22.

[12]See Baker and Dellaert (2018), p. 724.

dilemma, a problem faced recently by the constructors of the so-called autonomous vehicles will now be shortly discussed. On 19 March 2018, the first fatal accident "caused by" an autonomous vehicle occurred. From the investigation, it was established that the vehicle did not stop because a pedestrian was passing the street in a prohibited place. This case clearly reveals that the software did not consider the possibility that the human may act contrary to the applicable rules. A similar problem may affect the constructors of the robo-advisors' software. Although in this case, apart from the risk of the client breaching the applicable rules, the major risk would be related to the lack of knowledge and, subsequently, incomprehension of the information asked or provided by the robo-advisors.

3 The IDD Directive: Digital-Friendly or Technologically Negative?

The IDD Hardly Refers to Robo-Advisors or Automatization Within the Insurance Distribution Process However, it does not prohibit application of the new technologies. Therefore, as the insurance industry is leading the way in developing digitalization within the provision of financial services, it is worth asking whether the EU legislator considered this while creating insurance legislation, among which the IDD.

Clearly, it could be argued that the answer is already known. The new technologies have been used by (re)insurers and intermediaries for some time, even before the IDD has been adopted and therefore, it seems obvious that no legal obstacles are in the path of their application. Nevertheless, as the digital development continuously unleash more sophisticated robots, bots, androids, and other manifestations of artificial intelligence, still new doubts arise both on whether the new technologies still fit the regulation, which does not change so fast, and on the possibility of creating a legislation that would efficiently cover application of the new technologies. The urgent need of such legislative approach has been already noticed by the Insurance Europe federation that published a series of papers and reports on FinTech and InsurTech calling to ensure the so-called "future-proof rules".[13] The same opinion is shared by the Committee on Economic and Monetary Affairs which claims that *all new EU-legislation should be guided by the 'innovation principle'. This means that the potential effect of legislation on innovation should be investigated during the impact assessment phase of the legislative process. Technology neutrality in every level of legislation should be a core element of this.*[14] From the

[13]See *Insight briefing: Supporting innovation in insurance in a digital age*, Insurance Europe aisbl, February 2017, available at: https://www.insuranceeurope.eu/insight-briefing-supporting-innovation-insurance-digital-age.

[14]Report of 28 April 2017 on FinTech: the influence of technology on the future of the financial sector (2016/2243(INI)) issued by the Committee on Economic and Monetary Affairs, available at:

above, an in-depth analysis of the insurance legislation in terms of its flexibility and adaptation to the new technologies seems to be thoroughly justified and needed. Further in this essay, the focus will be put in particular on the permissibility of performing the insurance distribution by robo-advisors under the IDD.

As mentioned, the IDD hardly mentions the technical measures used within the insurance distribution process. Nevertheless, a general reference to digitalization is made within the definition of the insurance distribution (Article 2 sec. 1 point 1 of the IDD) where it is explicitly allowed to perform the insurance distribution activities *through a website or other media*. Interestingly, the term "other media" has not been further explained by the legislature. This may lead to the conclusion that the IDD—intentionally or otherwise—provides for the non-exhaustive list of the technical and organizational measures by means of which distribution services can be rendered. Undoubtedly, this can be recognized as a digital-friendly approach. In addition, at this point, it is worth to underline that the IDD is the first insurance distribution directive that directly includes the possibility of using the electronic means within the distribution process. Accordingly, the IDD considers a website and durable media as a permissible measure by means of which the obligatory information may be provided to the customer (Article 23 sec. 2 of the IDD).

Furthermore, the fact that the European legislator considered the development of digitization is also demonstrated within the Commission Delegated Regulation (EU) 2017/2359 of 21 September 2017 supplementing the IDD with regard to information requirements and conduct of business rules applicable to the distribution of insurance-based investment products[15] (hereinafter referred to as the "Regulation"). Under Article 12 of the Regulation ***the insurance intermediary's or insurance undertaking's responsibility*** *to perform the suitability assessment in accordance with Article 30(1) of Directive (EU) 2016/97* ***shall not be reduced due to the fact that advice on insurance-based investment products is provided in whole or in part through an automated or semi-automated system.*** This restriction recognizes the liability for actions taken by automated or semi-automated systems, including robo-advisors, which is currently lively discussed at both the business and legislative levels. However, as this problem is far more complex and broad, it should be analyzed separately. Although, for this analysis, the overall assessment of this provision should be considered rather positive. Nevertheless, it is hard to find a plausible explanation for limiting the application of such provision only to the distribution of insurance-based investment products. The authors therefore contend that the same rule should likewise be applicable to the traditional insurance products.

---

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0176+0+DOC+XML+V0//EN, p. 17.

[15]Commission Delegated Regulation (EU) 2017/2359 of 21 September 2017 supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to information requirements and conduct of business rules applicable to the distribution of insurance-based investment products (Text with EEA relevance) (OJ L 341, 20.12.2017, p. 8–18).

4 Concerns and Regulatory Challenges

Having analyzed the IDD in terms of its positive approach to the performance of the insurance distribution by robo-advisors, in this paragraph, the authors present the potential doubts that may arise over selected IDD provisions as to their suitability in the context of new technologies.

4.1 Professional Requirements and Conduct of Business Rules

Given the fact that robo-advisors are neither natural nor legal person, it is obvious that under the currently binding definition of the insurance intermediary they cannot be recognized as such. Thus, it seems that under the IDD, robo-advisors should be rather considered an instrument by means of which the insurance intermediary distributes the insurance products. Based on this assumption, it is clear that the IDD provisions regarding professional requirements (Article 10 of the IDD) and conduct of business rules (Article 17 of the IDD) should apply to the natural or legal person being an insurance intermediary and not to the robo-advisor. This apparently simple reasoning turns confusing when imagining a situation in which the distribution process is fully automated (i.e., the robo-advisor exercises the first insurance distribution activity and accompanies the client during the whole process of the execution of the insurance agreement) and the insurance intermediary owns and controls the enterprise only.[16] Who should be subject to the abovementioned regulation when the insurance distribution activities are fully automated? Assuming that the answer is robo-advisors, next concern arises on how to assess whether the robo-advisor acts *honestly, fairly and professionally in accordance with the best interests of* its *customers*. This seems to be one of the regulatory challenges to address.[17]

4.2 Automated Advice and Assessment of Suitability and Appropriateness

Other doubts may arise over the obligation to provide an advice and offer an insurance contract that is consistent with the customer's insurance demands and needs. Under Article 20 sec. 1 of the IDD, ***the insurance distributor shall specify****, on*

[16]This concern is also shared by other authors. See Baker and Dellaert (2018), p. 724.

[17]The available research often questions the ability of the robo-advisors to be honest. For further details, see e.g. Iannarone Nicole (2018), pp. 156 and 157; and Strzelczyk (2017), pp. 63 and 64.

the basis of information obtained from the customer, ***the demands and the needs of that customer*** *and shall provide the customer with objective information about the insurance product in a comprehensible form to allow that customer to make an informed decision.* ***Any contract proposed shall be consistent with the customer's insurance demands and needs.*** The first aim of this and the following IDD provisions is to provide the client with the offer of an insurance product that best suits his demands and needs. Secondly, the regulation reflects the advisory role of the insurance distributor.

Although it is claimed that robo-advisors have the potential to outperform humans in matching the clients to the insurance product, and therefore would perfectly manage to comply with the above provisions, it is hard to foresee whether the same regards compliance with more detailed provisions of the Regulation with this respect. For instance, Article 10 of the Regulation stipulates **the obligation to** ***ensure that the information collected about customers*** *and potential customers for the purposes of the assessment of suitability* ***is reliable.*** To do so, the insurance distributor should, i.a., ***ensure that customers are aware of the importance of providing accurate and up-to-date information,*** *(. . .) ensure that questions used in the process are likely to be understood by the customers and* ***to capture an accurate reflection of the customer's objectives and needs and the information necessary to undertake the suitability assessment***. Besides the ambiguity of these instructions and possible difficulties in designing the process that would comply with all of these requirements, it is worth to note that some recent studies' results explicitly indicate the difficulties that the robo-advisors may face while assessing whether the information provided by the customer is reliable.[18] Assuming these results are true, it should be decided whether lack of the ability to assess reliability of the information should exclude robo-advisors from the distribution of insurance-based investment products or whether the said provision should be amended accordingly.

4.3 The Liability for the Insurance Distribution Performed by Robo-Advisor

The problem of the liability for the actions and decisions taken by robo-advisors has already been mentioned in relation to the risks associated with potential software defects. As the liability issue is complex and needs a separate analysis, in this paragraph it will be discussed only to the extent relevant for this essay.

In general, the discussion over the liability for the insurance distribution performed by robo-advisor is focused on answering the question who should assume such liability. Should it be a natural person (insurance intermediary), being the owner of the robo-advisor, producer of the robo-advisor, or programmer who

[18]Hermansson (2018), p. 239.

prepares and tests programs for robo-advisor? On its face, it seems that the liability should be primarily assumed by the insurance intermediary owning the robo-advisor as the action of the robo-advisor in fact reflects the actions of its owner and the architecture of the algorithm is part of the intermediary's organization (Marano 2019). On the other hand, it should be underlined that the robo-advisor works based on and within the limits of its own software where such software is normally developed by the third party—not the insurance intermediary. Hence, it seems plausible to consider also the possible liability of the software's developer. In conclusion, the overall research seems to provide for the following conclusion: the liability for robo-advisor's actions should depend either on the ownership or on the ability to influence its actions. This however could change considering the impact of machine learning that enables the computers to become fully independent.

The discussed problem has been already addressed by the European Parliament which adopted a resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics.[19] By adopting the aforementioned document, the European Parliament drawn the attention to the necessity of considering the responsibility of the robot's creator. Accordingly, the same consideration should be given to the responsibility of the creators of robo-advisor's software. Furthermore, an interesting recommendations proposed by this resolution is to consider a system whereby all potential liabilities resulting from the acts of autonomous robotics (with the capacity to be trained and make decisions independently) could be insured under a compulsory robot liability insurance scheme akin to motor vehicle insurance. This idea was, however, criticized by the Insurance Europe federation which claimed that *compulsory insurance only works in specific cases and when certain market pre-conditions are met; such as the availability of sufficient claims data, a high level of standardization and plentiful insurance capacity to manage risks and cover claims. (. . .) Instead of boosting the insurance market, a compulsory insurance scheme would likely lead to a less dynamic insurance market and high premiums. This is because an obligation to insure new risks without sufficient information and data would oblige insurers to factor into their premiums the uncertainty around future claims.*[20]

As to the IDD provisions, bearing in mind the general intention to guarantee the same level of protection regardless of the channel through which customers buy an insurance product,[21] it seems that the responsibility towards the customers falls always on the insurance distributor. Additionally, this conclusion is fostered by the aforementioned Article 12 of the Regulation suggesting the exclusive liability of the insurance intermediary or insurance undertaking. Nonetheless, considering the previous remarks, as the potential damage may occur because of the faulty software of

[19]European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

[20]See Press statement of the Insurance Europe available at: https://www.insuranceeurope.eu/concerns-raised-over-european-parliament-robotics-report.

[21]See recital No. 8 of the IDD.

the robo-advisor, recourse liability of the software developer towards the insurance distributor should be considered. Further, depending on the cause of the damage and the contractual arrangements applied between the insurance distributor and the software developer, the recourse liability could be recognized as a guarantee. For this essay, the authors refrained from analyzing the direct liability of the software developer towards the aggrieved party. This is because in the insurance market's practice, the insurance distributor usually acts as a co-creator of the IT solutions used within the insurance distribution process. Hence, in practice it would be difficult for the aggrieved party to find out and subsequently prove to the satisfaction of the court that a specified part of the software for which the responsibility lies on the developer caused the damage.

Finally, as to the liability issues, it is worth to mention the concept of *force majeure* which seems particularly interesting in the context of the consequences followed from the application of machine learning. Briefly, *force majeure* is generally intended to include occurrences beyond the reasonable control of a party, as a contractual clause *force majeure* frees both parties from liability or obligation when an extraordinary event or circumstance beyond the control of the parties occurs. In practice, most *force majeure* clauses do not exclude a party's non-performance entirely, but only suspend it for the duration of the *force majeure*. With this, since some actions taken by the robo-advisors might be independent in nature and beyond the reasonable control of its owner, it could possibly be argued that a faulty action of robo-advisor constitutes a case of *force majeure*.

5 Conclusions

Subject to all concerns indicated in this essay, the authors advocate that the IDD might be considered "digital-friendly", **at least for the time being**. However, as the digitalization process is moving fast-forward, it is highly probable that shortly this opinion will not be acceptable any longer. This, in turn, should induce the European legislator to keep looking for more universal and long-lasting solutions. Unfortunately, the future improvements do not seem to be prosperous. Over a year ago, the Joint Committee of the three European Supervisory Authorities—EBA,[22] EIOPA,[23] and ESMA[24]—published a report presenting the conclusions of its assessment on automation in financial advice in which the Joint Committee concluded that temporarily there is no need *to develop additional joint cross-sectoral requirements specific to this particular innovation* [i.e., automated advice].[25] Today, it seems

[22]The European Banking Authority.

[23]The European Insurance and Occupational Pensions Authority.

[24]The European Securities and Markets Authority.

[25]Report of the Joint Committee of the three European Supervisory Authorities (ESAs) – EBA, EIOPA and ESMA on automation in financial advice, available at: https://esas-joint-committee.

that it should not be further postponed, and a specific regulatory actions should be taken immediately as the issues to be regulated are multi-faced. Additionally, as it was rightly pointed out by head of personal insurance, general insurance and macroeconomics at Insurance Europe Nicolas Jeanmart—the different technological innovations present different risks and therefore a single regulatory approach to all such emerging technologies would not work.[26]

Finally, beyond the above presented for and against arguments regarding the thesis on the permissibility of robotic insurance mediation under the IDD, the authors' sense is that whatever the future of the robo-advisory will look like, it will be always crucial to maintain a human being as an ultimate decision-making authority (including discretion to override) within the whole distribution process. As yet, it is believed that robo-advisors may not provide a human touch that is essential to the adviser/client relationship.[27] Therefore, establishing a human as the last decision-making authority or "appeal authority" would be considered as the way of mitigating the risk of potential damages resulting from the lack of human factor or other risks related to e.g. faulty software. In short, the possibility of any kind of human control and verification is recommended to be built into every process of automated and algorithmic decision-making, including robo-advisors' activity.

One of the aims of this essay has been to open a discussion that invites to further verification of the insurance legislation and highlights the need to take the appropriate regulatory and legislative actions promptly. As coordinating these efforts is a natural role of the European legislator and the national regulators, we do hope that the conclusions expressed in their reports and the legal research will be followed with real improvements.

References

Accenture's Report (2017) The rise of insurtech, 28 April 2017. https://www.accenture.com/us-en/insight-rise-insurtech

Baker T, Dellaert B (2018) Regulating Robo advice across the financial services industry. Iowa Law Rev 103

Committee on Economic and Monetary Affairs' Report of 28 April 2017 on FinTech: the influence of technology on the future of the financial sector (2016/2243(INI)). http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+REPORT+A8-2017-0176+0+DOC+XML+V0//EN

Committee on Legal Affairs' Report of 27 January 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))

europa.eu/Pages/News/European-Supervisory-Authorities-publish-conclusions-on-automation-in-financial-advice.aspx, p. 5.

[26]See Press statement of the Insurance Europe available at: https://www.insuranceeurope.eu/concerns-raised-over-european-parliament-robotics-report.

[27]Iannarone Nicole (2018), pp. 152 and 153.

Ferguson B. Drafted version of the speech delivered on 11 October 2017 during 2017 Annual Conference on Robo Advice and Investing: From Niche to Mainstream. https://www.fca.org.uk/news/speeches/robo-advice-fca-perspective

Financial Conduct Authority, FCA's Business Plan 2017/2018. https://www.fca.org.uk/publications/corporate-documents/our-business-plan-2017-18

Hermansson C (2018) Can self-assessed financial risk measures explain and predict bank customers' objective financial risk? J Econ Behav Organ 148

Iannarone Nicole G (2018) Computer as confidant: digital investment advice and the fiduciary standard. Chic Kent Law Rev 93

Insurance Europe. Concerns raised over European Parliament robotics report. https://www.insuranceeurope.eu/concerns-raised-over-european-parliament-robotics-report

Insurance Europe. Insight briefing: supporting innovation in insurance in a digital age, Insurance Europe aisbl, February 2017. https://www.insuranceeurope.eu/insight-briefing-supporting-innovation-insurance-digital-age

Joint Committee of the three European Supervisory Authorities (ESAs) – EBA, EIOPA and ESMA report on automation in financial advice. https://esas-joint-committee.europa.eu/Pages/News/European-Supervisory-Authorities-publish-conclusions-on-automation-in-financial-advice.aspx

Lech J (2018) Machine learning u ubezpieczycieli? In Miesięcznik Ubezpieczeniowy, vol 15, No 5, ISSN 1732-2413

Marano P (2019) Navigating InsurTech: the digital intermediaries of insurance products and customer protection in the EU. Maastrich J Eur Comp Law 26(2):310

Schueffel P (2017) The Concise Fintech Compendium. School of Management Fribourg (HEG-FR), Fribourg, p 26

Strzelczyk BE (2017) Rise of the machines: the legal implications for investor protection with the rise of Robo-Advisors. DePaul Bus Comm Law J 16

Legislative Instruments

Commission Delegated Regulation (EU) 2017/2359 of 21 September 2017 supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to information requirements and conduct of business rules applicable to the distribution of insurance-based investment products (Text with EEA relevance) (OJ L 341, 20.12.2017, p. 8–18)

Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast) Text with EEA relevance (OJ L 26, 2.2.2016, p. 19–59)

Cyber Risks: Three Basic Structural Issues to Resolve

Leo P. Martinez

1 Introduction

A staple of Silicon Valley lore is Moore's Law. Moore's Law posits that computer processor speeds will double every 2 years.[1] To the extent that firms' reliance on digital platforms is correlated to Moore's law, and to the extent malefactors' ability to cause mischief is likewise correlated to Moore's law, we can expect that Moore's Law will eventually apply the same geometric relationship to the incidence of cyber-losses by firms.[2]

In a 2016 study, the Ponemon Institute estimated the probability that any given company will experience a material data breach within 24 months is 26%.[3] The average total cost of such a data breach is estimated to be $4 million per incident,

Comments regarding this paper can be directed to the author at martinez@uchastings.edu. I am grateful for the diligent and able research assistance of Paige Adaskaveg, Hastings class of 2019, Andrew Klair, Hastings class of 2020, and Michael (Jake) Winton, Hastings class of 2020. Errors are, of course, mine.

[1] Ostrander (2006), p. 1.

[2] Although this should be true, the empirical support for the proposition is weak. Perhaps there is a phase lag that reflects potential policyholder's lack of appreciation of the risk that is faced. For example, the prediction that the implementation of the European Union's General Data Policy Regulation would lead to an increased demand for cyber insurance also failed to materialize. Mengqi Sun (June 21, 2018) Europe's Privacy Law Fails to Stoke Demand for Cyber Insurance, WSJ B10.

[3] Ponemon (2016). Some of the material that follows paraphrases discussion in Martinez and Richmond (2018).

L. P. Martinez (✉)
University of California, Hastings College of the Law, San Francisco, CA, USA
e-mail: martinez@uchastings.edu

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_10

representing a 29% increase in the 3 years since 2013.[4] This represents costs incurred from network interruption, media liability, extortion liability, network security costs, reputational injury, and disclosure injury. Particularly vulnerable are medium-sized businesses that have large potential exposure to cyber risks but lack the sophisticated IT infrastructure necessary to deal with cyber-attack.[5] The problem of cyber loss is not a transitory one—it will only get worse and, as Moore's Law predicts, it will get worse at a rapidly increasing rate.[6]

This essay proceeds in a linear way. Section 2 begins with a working definition of cyber risks. Section 3 describes existing insurance coverage for cyber risks and deals with the difficulties of covering cyber risks. Section 4 describes the nearly complete lack of case law treatment of cyber risks either on the coverage side or the exclusion side. Finally, Sect. 5 provides a general outline for possible solutions.

The discussion that follows includes both first-party and third-party cases. While I appreciate the distinction between the two, the relatively small number of cases dealing with cyber risks suggests that we should glean information from whatever sources are available.[7]

2 Range of Cyber Risks or What's Included/What's Excluded

"Cyber" has become insurance industry shorthand for a variety of information technology risks, including but not limited to: hardware, software, IT consulting, cloud services, and data processing. It is in this very general sense that the term cyber is used in this essay. Because of the dearth of cases, issues involving first-party cyber losses and third-party cyber liability will be treated interchangeably under the rubric of "cyber risks."

The range of cyber risks today seems limited only by human ingenuity. The sheer number and variety of problems that exist make the creation of an effective and

[4]Ponemon (2016). An ironic example of the cobbler's children going unshod is the observation that lawyers, who should be especially vigilant about clients' cyber risk issues, are themselves often underinsured in this area. Stephens and Tilton (2017), p. 12 ("Only 17 percent of attorneys reported having a cyber insurance policy . . . ."). The penetration rate of cyber coverage among lawyers is marginally better than the 1/3 penetration rate among operating firms. Romanosky et al. (2017), p. 3.

[5]Stephens and Tilton (2017), pp. 12, 15.

[6]Dominitz (2017), pp. 32, 33 (describing cyber losses as "not just a passing fad").

[7]See Jerry and Mekel (2001), pp. 11–17 (discussing first-party and third-party insurance). While used interchangeably in this piece, third-party cyber risk cases are difficult to assess because the duty to defend lowers an insurer's threshold obligations. *OOIDA Risk Retention Grp., Inc. v. Griffin*, 2016 U.S. Dist. LEXIS 57469 at p. 15 (E.D. Va. 2016) ("burden is not especially onerous as an insurer's duty to defend"); Moreover, it is the insurer who bears the burden of proof regarding exclusions. *Selective Way Ins. Co. v. Crawl Space Door Sys.*, 162 F. Supp. 3d 547, 551 (E.D. Va. 2016).

predictable exclusion a daunting task. The National Association of Insurance Commissioners (NAIC)[8] and the Insurance Information Institute have both identified long lists of potential cyber problems.[9]

Other kinds of cyber risks apart from those compiled from the National Association of Insurance Commissioners (NAIC) and the Insurance Information Institute

[8]At the time *"Breaking Bad" in Cyberspace: A Challenge for the Insurance Industry* was written the list in footnote 9 was published on the NAIC website under the cybersecurity topics page. However, since 2014 the webpage has been updated and NAIC has removed the list below. NAIC's updates do not discount the validity of the list below, rather just that NAIC's focus on this topic has expanded. As of April 30, 2018, NAIC is considering creating a Cybersecurity Insurance Institute, demonstrating how this area of Insurance Law is expanding rapidly. For more information see, https://www.naic.org/cipr_topics/topic_cyber_risk.htm.

[9]Cope and Reynolds (2015).

The types of Coverage Identified by the National Association of Insurance Commissioners (NAIC) include the following:

- Liability for security or privacy breaches, including loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems;
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers;
- The costs associated with restoring, updating or replacing business assets stored electronically;
- Business interruption and extra expense related to a security or privacy breach;
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media (for an in-depth discussion of specific risks arising from the use of social media, please see Carrie E. Cope, Dirk E. Ehlers & Keith W. Mandell (2014) Social Media and Insurance: The Insider's Guide to Successful Risk Assessment and Management);
- Expenses related to cyber extortion or cyber terrorism; and
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings. Cope and Reynolds (2015), p. 29.

The types of cyber risk liability identified by The Insurance Information Institute include an equally impressive listing:

- Loss/Corruption of Data—covers damage to, or destruction of, valuable information assets because of viruses, malicious code and Trojan horses;
- Business Interruption—covers loss of business income because of an attack on a company's network that limits its ability to conduct business, such as a denial-of-service computer attack--coverage also includes extra expenses, forensic expenses and dependent business interruption;
- Liability—covers defense costs, settlements, judgments and, sometimes, punitive damages incurred by a company because of:
- Breach of privacy because of theft of data (such as credit cards, financial or health related data);
- Transmission of a computer virus or other liabilities resulting from a computer attack, which causes financial loss to third parties;
- Failure of security which causes network systems to be unavailable to third parties;
- Rendering of Internet Professional Services; and
- Allegations of copyright or trademark infringement, libel, slander, defamation or other 'media' activities in the company's website, such as postings by visitors on bulletin boards and in chat rooms—this also covers liabilities associated with banner ads for other businesses located on the site;

can be gleaned from various articles and secondary materials. These include systems restoration,[10] forensic review,[11] cost of substitute systems,[12] third-party notification,[13] interference with military operations,[14] and disruption of infrastructure.[15]

3 Scope of Existing Coverage

As cyber risks have grown, insurance products that cover these risks have arisen in a sporadic and often contradictory way.[16] This section first analyzes the current state of coverage and then examines potential gaps that exist in CGL policies,[17] specialty

- D&O/Management Liability—newly developed tailored D&O products provide broad all risks coverage, meaning that the risk is covered unless specifically excluded—all liability risks faced by directors, including cyber risks, are covered;
- Cyber Extortion—covers the 'settlement' of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers;
- Crisis Management—covers the costs to retain public relations assistance or advertising to rebuild a company's reputation after an incident—coverage is also available for the cost of notifying consumers of a release of private information, as well as the cost of providing credit-monitoring or other remediation services in the event of a covered incident;
- Criminal Rewards—covers the cost of posting a criminal reward fund for information leading to the arrest and conviction of a cybercriminal who has attacked a company's computer systems;
- Data Breach—covers the expenses and legal liability resulting from a data breach—policies may also provide access to services helping business owners to comply with regulatory requirements and to address customer concerns;
- Identity Theft—provides access to an identity theft call center in the event of stolen customer or employee personal information; and
- Social Media/Networking—insurers are looking to develop products that cover a company's social networking activities under one policy. Some cyber policies now provide coverage for certain social media liability exposures such as online defamation, advertising, libel and slander. Hartwig and Wilkinson (2014); Cope and Reynolds (2015), pp. 30–31.

[10]Romanosky et al. (2017), p. 14 (mentioning systems restoration in addition to data recovery and data re-creation).

[11]Romanosky et al. (2017), p. 14.

[12]Romanosky et al. (2017), p. 14.

[13]Stephens and Tilton (2017), p. 15.

[14]Wood et al. (2017), pp. 38–39.

[15]Wood et al. (2017), pp. 38–39.

[16]Buchanan et al. (2018), Latham & Watkins (2014) Cyber Insurance: A Last Line of Defense When Technology Fails. https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage.

[17]While Directors and Officers Liability (D&O) policies and Errors and Omissions Liability (E&O) policies are distinct from Commercial General Liability (CGL) policies, the potential gaps in coverage appear to be similar. Latham & Watkins (2014) Cyber Insurance: A Last Line of Defense When Technology Fails. https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage. Decisions on whether CGL, E&O, and D&O polices cover cyber risk events come

cyber policies, endorsements, and the gaps that exclusions can create in otherwise sound policies.

3.1 Overview of Existing Coverage

The long list of cyber risk possibilities has resulted in a wide array of insurance coverage products. This diversity in the market has led to several adverse results. First, the large number of insurance products and the lack of standard language has contributed to the lack of definitive case law that focuses on a small set of key concepts.[18] This problem is almost unbelievably basic. For example, some researchers point out that "[i]t is unclear if [mobile devices] are grouped into the standard 'computers, networks, and systems'" language found in many cyber policies.[19] It is instructive that the first cyber risk case was decided in 1991[20] and there have been only on the order of two dozen cases in the time since.

Second, the proliferation of insurance products has also made the task of selecting adequate insurance protection that much more difficult.[21] As one prominent lawyer reasoned, "it takes both expertise and care to spot the traps or coverage gaps that may lurk in any cyber policy form."[22] Certainly, the inclusion of non-lawyers as part of the team introduces even more moving parts into the equation including the complication of attorney-client privilege concerns.[23]

Third, and related to the previous point, insureds can face gaps in coverage because of cyber policies that are too narrowly tailored to meet actual needs.[24] This fine-tuning of cyber risk coverage needs to be addressed by the insurance industry. To begin, however, the coverage of cyber risks under standard CGL policies must be analyzed.

---

down to subtle differences in policy language. The definitional problems described within this article creates the ambiguity of coverage for cyber risks. Oshinsky and Lee (2010).

[18] Schwarcz (2017), pp. 1500–1502; Buchanan and Gallozzi (2018).

[19] Romanosky et al. (2017), p. 14.

[20] *Retail Sys., Inc. v. CNA Ins. Cos.*, 469 N.W.2d 735 (Minn. Ct. App. 1991).

[21] Dominitz (2017), pp. 36–37. This may also explain the large variation in pricing among available cyber loss policies. Latham & Watkins (2014) Cyber Insurance: A Last Line of Defense When Technology Fails. https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage.

[22] Buchanan and Gallozzi (2018).

[23] Buchanan and Gallozzi (2018).

[24] Nitardy (2017), p. 27; Latham & Watkins (2014) Cyber Insurance: A Last Line of Defense When Technology Fails. https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage.

3.2 The CGL Policy

The number of incidents involving cyber risks initially gave rise to an important threshold question: to what extent are cyber risks covered or excluded by general insurance policies? CGL insurance policies providing bodily injury, personal injury, and property damage coverages do not directly address the combination of first and third party cyber exposures.[25]

The traditional kinds of physical losses contemplated under CGL policies are (1) physical injuries to tangible property, including the resulting loss of *use* of tangible property that is physically injured, and (2) loss of *use* of tangible property that is not physically injured.[26] Thus, the early cases involving cyber claims under CGL policies concluded that the CGL policies covered only physical losses—data losses were not the physical kind of losses contemplated by the policies.[27] When cyber risks threaten solely economic losses, or merely losses of data without damage to tangible property, CGL policies are unlikely to provide coverage.

For example, in *Ward General Insurance Services, Inc. v. Employers Fire Insurance Co.*, California's Fourth Appellate District concluded that the loss of a database and the resulting economic loss was not "direct physical loss" due to the absence of damage to tangible property.[28] Similarly, the Fourth Circuit concluded in *America Online, Inc. v. St. Paul Mercury Insurance Co.* that although a storage method which "consists of the arrangement of 'hundreds of thousands of atoms' of 'cobalt, iron, and other magnetic materials' in a perceivable and unique pattern" is tangible property, the "data information, and instructions, which are codified in binary language for storage" are not.[29] The loss or damage solely to data itself does not fall within the purview of the CGL policy because data is intangible.[30]

[25]Latham & Watkins (2014) Cyber Insurance: A Last Line of Defense When Technology Fails. https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage. (a similar lack characterizes Directors and Officers Liability (D&O) policies and Errors and Omissions Liability (E&O) policies).

[26]Matthew Bender & Company, Inc. (2nd 2011) Appleman on Insurance Law & Practice Archive. 20-129 § 129.2.

[27]*Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 554 (2003) (data does not qualify as a "direct physical loss"); *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 95 (4th Cir. 2003) (while a hard drive is tangible property, the data, information, and instructions, which are codified in a binary language for storage on the hard drive, are not tangible property); *Union Pump Co. v. Centrifugal Tech., Inc.*, 2009 U.S. Dist. LEXIS 86352 (W.D. La. 2009) (electronic data is not tangible property).

[28]*Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 556 (2003).

[29]*America Online, Inc. v. St. Paul Mercury Ins. Co*., 347 F.3d 89, 95 (4th Cir. 2003).

[30]*America Online, Inc. v. St. Paul Mercury Ins. Co*., 347 F.3d 89, 96 (4th Cir. 2003).

To be sure, there are a few cases where the courts held CGL policies to provide some coverage, but these could be seen as exceptions to the general approach.[31] One line of cases held that physical damage to tangible property caused by cyber risks fell squarely within the boundaries of the CGL.[32] Another line of cases held that the loss of use or the diminution of reliability of cyber property could be covered physical loss under a CGL policy.[33] One could easily argue that these few "exceptions" were not exceptions at all but rather attenuated permutations of the basic idea that the CGL policies covered physical loss.

Even in the face of physical loss limitations, policyholders saw some initial success. In a few clear-cut cases the cyber loss was occasioned by a real physical loss. For example, in *Anthem Electronics, Inc. v. Pacific Employers Insurance Company*, Anthem Electronics manufactured several defective circuit boards.[34] These circuit boards caused damage to the scanners they were installed in, and the Ninth Circuit held the loss to be a physical loss.[35] A few cases went further, revealing a willingness of courts to adopt a flexible view of physical loss. One short line of cases was based on the courts' reliance on language borrowed from the federal computer fraud statute and other criminal statutes which make it an offense to cause damage to a protected computer and define damage as "any impairment to the integrity or availability of data, a program, a system, or information."[36] This broader

[31] *E.g. Ashland Hosp. Corp. v. Affiliated FM Ins. Co.*, 2013 U.S. Dist. LEXIS 114730 at 18-19 (E.D. Ky. 2013) (direct and physical loss can include loss of reliability); *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010) (loss of *use* of computer was a physical loss).

[32] *See, e.g., Retail Sys., Inc. v. CNA Ins. Cos.*, 469 N.W.2d 735 (Minn. Ct. App. 1991) (holding computer tapes were tangible property); *Centennial Ins. Co. v. Applied Health Care Sys., Inc.*, 710 F.2d 1288, 1290 (7th Cir. 1983) (a faulty controller in data processing system caused damage and a loss of customer data, court held insurer had a duty to defend under CGL as property damage); *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 132 N.M. 264, 266 (N.M. Ct. App. 2002) (district court found computer data in case "was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed.").

[33] *Ashland Hosp. Corp. v. Affiliated FM Ins. Co.*, 2013 U.S. Dist. LEXIS 114730 at 18-19 (E.D. Ky. 2013); *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010).

[34] *Anthem Elecs., Inc. v. Pac. Emplrs. Ins. Co.*, 302 F.3d 1049 1058-59 (9th Cir. 2002).

[35] *Anthem Elecs., Inc. v. Pac. Emplrs. Ins. Co.*, 302 F.3d 1049 1058-59 (9th Cir. 2002).

[36] *American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, 2000 U.S. Dist. LEXIS 7299; 2000 WL 726789 at 7 (dealing with a property damage policy, which insured against specific business interruption and service interruption losses). In *Ingram Micro*, Ingram's computer systems became inoperable because of a power outage. *Id.* at 1. Ingram made a claim to American, which American denied based on its determination that a power outage did not cause "direct *physical loss* or damage from any cause, howsoever or wheresoever incurring" to Ingram's computer system. *Id.* at 2 (emphasis added). The Court rejected American's argument that the computer system and the matrix switch were not "physically damaged" because despite the loss of the programming information, the computers were able to perform their intended functions. *Id.* at 5. Instead, the Court agreed with Ingram and found that "physical damage" was "not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality." *Id.* at 6. In finding that there was the requisite physical loss, the court borrowed from the federal computer fraud statute and other criminal statutes, which make it an offense to cause damage to a protected computer and which define damage as "any impairment to the integrity or

reading of loss was the key to recovery. Another case found that the loss of *use* of computer equipment could be a physical loss within the meaning of the policy language.[37]

The unlikely possibility of coverage for cyber risks under the standard CGL policy was reduced further yet by the Insurance Services Office (ISO).[38] The motivation for the change by the ISO seems to have been a desire to remove coverage for cyber risks from the CGL policy and isolate them in specialty policies.[39] Initially, the ISO CGL was ambiguous about whether damage to electronically stored data was covered, but a revision in 2001 to the general CGL policy removed coverage for damage to electronically stored data and a 2004 revision (Exclusion P) excluded damages resulting from loss of electronically stored data.[40] A further revision carved out bodily injury from Exclusion P, and two recent competing endorsements have added exclusions for any damages arising out of "[a]ny access to or disclosure of any person's or organization's confidential or personal information. . . "[41] These revisions have effectively removed coverage for property damages stemming from cyber breaches under ISO CGL policies and leave insureds with little possibility of coverage outside of specialty policies.

The result is that, with the exception of some, perhaps not so exceptional cases discussed below, a policyholder seeking some insulation against risk is left with an outcome best described as uncertain. By the same token, insurers who are interested in profiting from the sale of protection against cyber risks are forgoing the opportunity to provide needed coverage and to generate revenue.

---

availability of data, a program, a system, or information." *Id.* at 7. A subsequent Tennessee decision followed the *Ingram Micro* analysis. *Southeast Mental Health Ctr., Inc. v. Pac. Ins. Co.*, 439 F. Supp. 2d 831, 838 (W.D. Tenn. 2006).

[37] *State Auto Property & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113 (W.D. Okla. 2001) (while data was not tangible property, the loss of the use of the customer's computer was tangible property).

[38] Buchanan et al. (2018).

[39] Buchanan et al. (2018).

[40] Buchanan et al. (2018).

[41] *Id.*; Insurance Services Office, Inc. (2013) Exclusion — Access or Disclosure of Confidential or Personal Information and Data-Related Liability — With Limited Bodily Injury Exception, *CG 21 06 05 14*.

The competing endorsements are the two versions of a revised Exclusion P that the ISO published in May 2014: one with a "limited bodily injury exception" and one without. The one with the exception preserves coverage for bodily injury damages, such as an injury sustained when glucose monitoring sensors stop receiving data. ISO Form CG 21 06 05 14 (2015). The other version essentially reverts to the 2004 variant of Exclusion P—it excludes any such damages, regardless of whether they arose from bodily injury or property damage. ISO Form CG 21 07 05 14 (2015). As always, the admonition is to read the applicable policy and the endorsements it contains.

3.3 *Specialty Policies, Endorsements, and Cyber Risk Exclusions*

Because the CGL policies generally do not provide certainty of coverage for cyber risks, insurers and policyholders have resorted to stand-alone cyber policies or cyber endorsements to the extent they are available.[42] Newer coverage forms for cyber risks include cyber insurance policies, professional liability for technology firms, and products liability to name a few.[43] The problem is: as insurance policies and endorsements have become more nuanced, the coverage issues have multiplied. As evidenced below, even if the basic difficulties with the exclusions outlined above are overcome, insureds and insurers will still find a litany of challenges to crafting effective specialty policies for cyber-attacks.

Specialty policies are increasingly diverse and specific. There already exist over 60 markets for cyber insurance and liability limits extend to $500 million.[44] These policies, however, are still "unaligned on pricing, retentions, and sublimits for first-party coverages, in particular, such as forensics, business interruption, and notification expenses."[45] The diversity in the market leads to challenges for insureds trying to find a policy that specifically targets their needs.[46] Additionally, these coverages often have their own exclusions (beyond the ones listed below) which further limit coverage. Increasingly, these exclusions reduce coverage for the insured's own negligence whether it arises from specific human error or computer glitches.[47] This complexity means insureds need to use considerable time and effort or hire a cyber insurance expert to determine exactly what coverage they need.[48] While specialty policies currently exist, and their use is increasing,[49] the variance and complexity of the market can lead to confusion and gaps in coverage for even sophisticated insureds.

Exclusions that limit insurers' exposure further limit the coverages offered by insurance policies crafted to deal with cyber risks.[50] As is the case with coverage, the range of exclusions suggests that the initial novelty of coverage is further complicated. However, as will be discussed in Section III, the problem of novelty and the accompanying complications may well be overstated.

---

[42]Garrie and Mann (2014), pp. 389–390.

[43]O'Donnel and Oonk (2017), pp. 10–11 (citing broad array of available policy forms).

[44]Stephens and Tilton (2017), p. 18.

[45]Stephens and Tilton (2017), p. 18.

[46]Dominitz (2017), p. 33.

[47]Dominitz (2017), p. 33.

[48]Stephens and Tilton (2017), p. 18.

[49]Stephens and Tilton (2017), p. 15 ("Sixty percent of ALPS's insureds wisely retain the cyber coverage.").

[50]Garrie and Mann (2014), pp. 389–390.

Just as coverages seem to coalesce around a handful of problems, so too have exclusions tended to focus on a small set of issues.[51] According to a Rand research paper, the most common ten exclusions are: fines, penalties, fees from affected institutions; seizure or destruction of systems by government; IP Theft; acts of God; acts of terrorism, war, and military action; contractual liability; bodily injury; loss to systems not owned or operated; and negligent disregard for computer security.[52]

A related potential exclusion not mentioned above that affects cyber risk is the war exclusion. Because a large majority of cyber-attacks are conducted by state actors—that is, independent countries—insureds suffering cyber damages often face challenges by insurers based on these war exclusions.[53] War exclusions generally negate coverage for cyber risks and, even for the diligent policyholder, present significant coverage issues.[54] War exclusions exist in virtually all policies, including both CGL and specialty policies.[55]

To date, only a few of these exclusions have even existed in cases addressed by the courts in the context of cyber risk. Even when cases arise that concern cyber risk exclusions, the resolution typically turns on interpretations or other exclusions that do not implicate any aspect of cyber risk. This is not a great state of affairs. Both insurers and insureds are better served with predictable results. Insurers face a problem in drafting these policies because there is a lack of judicial information about how these policies will be interpreted by the courts. Without a thorough case history, insurers cannot confidently draft these policies to exclude (or price in) certain high-risk practices.[56] The "friction" of litigation in this context is an unalloyed disadvantage; to the extent insurance policy terms unique to cyber risks are vetted we are all better off.

4 Everything Old Is New Again

What has transpired since the ISO revisions to the CGL is somewhat remarkable. As noted above, there are only roughly two dozen cyber risk cases that have been decided since 2000. Of these cases, the early ones dealt with the possibility of

[51]Romanosky et al. (2017) (suggesting that 52% of exclusion types could be identified after an examination of only six policies).

[52]Romanosky et al. (2017).

[53]Buchanan et al. (2018).

Even if a potential policyholder is aware of the war exclusions and the consequent effect on coverage of cyber losses, it is an open question whether it is possible for even the most sophisticated of policyholders to avoid the war exclusions. Buchanan et al. (2018).

[54]Buchanan et al. (2018).

[55]Buchanan et al. (2018). The categorical statement in the text requires some qualification. There are as many as 13% of cyber policies that cover terrorism related losses. Romanosky et al. (2017).

[56]Schwarcz (2017), pp. 1500–1502.

coverage of cyber risks under the standard CGL policy. After the ISO revisions, the cases involving cyber risks have been decided based on principles that are well familiar to insurance practitioners.

While there is a dearth of defining case law governing cyber risks, and even basic terminology has not been well litigated, the reality is that legal principles particular to cyber risks have not been needed—at least they don't seem to have materialized since the ISO revisions.[57] A brief review of representative cases reveals this state of affairs regardless of whether coverage has been found or not.

4.1 Coverage for Cyber Risks Found

In *Travelers Indemnity Co. v. Portal Healthcare Solutions, LLC*,[58] Portal Healthcare was facing a lawsuit after medical records were accidentally made available through a simple internet search. Portal had a CGL policy with Travelers that provided coverage for injury arising from the "electronic publication of material that . . . gives unreasonable publicity to a person's private life."[59] Travelers denied coverage arguing that Portal did not "publish" the records by simply making them available to be accessed. However, the court disagreed and held that this was a "publication" under the policy and Travelers must provide coverage.[60] In reaching this decision, the court did not dip into a well of tailor-made cyber insurance terms, but instead utilized the age-old plain meaning line of reasoning to apply a different definition to "publicity" than the definition Travelers argued for.[61]

A further sampling of exclusions and their efficacy well illustrates the conventional approach to the problem. Exclusions for losses related to "software, data or other information that is electronic in form" have been held ineffective to preclude coverage for loss of *use* of computers.[62] For example, in *Eyeblaster, Inc. v. Federal Insurance Company*, the court found that the plain meaning of tangible property includes computers.[63] Since a computer is a tangible property, a "loss of the use of a

[57]Latham & Watkins (2014) Cyber Insurance: A Last Line of Defense When Technology Fails. https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage; Buchanan and Gallozzi (2018). (adding the lack of "standardization among cyber policies' wordings," as a factor); O'Donnel and Oonk (2017), pp. 10–11 (noting that the creation of new forms has added to the mass of untested language).

[58]35 F. Supp. 3d 765 (E.D. Va. 2014), *aff'd per curiam*, 644 Fed. Appx. 245 (4th Cir. 2016).

[59]35 F. Supp. 3d 765, 767 (E.D. Va. 2014), *aff'd per curiam*, 644 Fed. Appx. 245 (4th Cir. 2016).

[60]35 F. Supp. 3d 765, 770 (E.D. Va. 2014), *aff'd per curiam*, 644 Fed. Appx. 245 (4th Cir. 2016).

[61]35 F. Supp. 3d 765, 772 (E.D. Va. 2014), *aff'd per curiam*, 644 Fed. Appx. 245 (4th Cir. 2016). ("That Portal's conduct falls within the broader and primary definition of "publicity" suffices to establish that Portal gave unreasonable publicity to patients' private lives when it posted their medical records online without security restriction.").

[62]*Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010).

[63]*Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010).

computer constitutes 'property damage' within the meaning" of CGL policies.[64] In the absence of evidence from the Insurer showing that the computer remained functional, the court concluded that the allegations were "within the scope of the General Liability policy."[65]

A provision providing coverage against loss resulting from "the theft of any Insured property by Computer Fraud . . ." was deemed to cover third-party claims stemming from the electronic theft of customer credit card information in *Retail Ventures, Inc. v. National Union Fire Insurance Company*.[66] The loss was covered despite an exclusion which provided that "[c]overage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind" because the court held it did not preclude coverage for loss of nonproprietary customer information.[67] Specifically, the court found that reading the catchall term "information of any kind" to include all information not intended for disclosure "would swallow not only the other terms in [the] exclusion but also the coverage for computer fraud."[68]

In *First Bank of Delaware, Inc. v. Fidelity & Deposit Company of Maryland* the coverage provision read, "[t]he Insurer will pay on behalf of the Insured all loss resulting from any electronic risk claim first made against the Insured during the policy period or the extended reporting period, if applicable, (1) for an electronic publishing wrongful act or (2) that arises out of a loss event."[69] An exclusion provided the insurer shall not be liable for any claim against the insured "based upon or attributable to or arising from the actual or purported fraudulent use by any person or entity of any data or in any credit, debit, charge, access, convenience, customer identification or other card, including, but not limited to the card number."[70] Although the court found the coverage and exclusion unambiguous, the court nonetheless denied the exclusion effect on the basis that to enforce it would render the coverage illusory.[71] According to the court, "[t]he principle that a grant of coverage should not be rendered illusory protects the reasonable expectations of the purchaser."[72]

In gross, these cases show that the coverage for cyber risks is proceeding subject to already well-recognized rules. No special principle of cyber law seems to have emerged. The same seems to hold true for those cases that have resulted in a denial of coverage.

---

[64] *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010). (citing State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001)).

[65] *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010).

[66] *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821, 824-26 (6th Cir. 2012).

[67] *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821, 832 (6th Cir. 2012).

[68] *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821, 833 (6th Cir. 2012).

[69] *First Bank of Del., Inc. v. Fid. & Deposit Co. of Md.*, 2013 Del. Super. LEXIS 465 at 5–7.

[70] *First Bank of Del., Inc. v. Fid. & Deposit Co. of Md.*, 2013 Del. Super. LEXIS 465 at 16.

[71] *First Bank of Del., Inc. v. Fid. & Deposit Co. of Md.*, 2013 Del. Super. LEXIS 465 at 25.

[72] *First Bank of Del., Inc. v. Fid. & Deposit Co. of Md.*, 2013 Del. Super. LEXIS 465 at 25.

4.2 Coverage for Cyber Risks Denied

In *P.F. Chang's China Bistro, Inc. v. Federal Insurance Company*,[73] P.F. Chang's had a separate cyber liability policy which provided that "[Federal] shall pay for Loss on behalf of an Insured on account of any Claim first made against such Insured. . . for Injury."[74] The policy defined a "privacy injury" as an "injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record, or exposing access to such Person's Record."[75]

On June 10, 2014, P.F. Chang's learned that computer hackers had obtained 60,000 customer credit card numbers. Federal reimbursed P.F. Chang's more than $1.7 million from direct customer injuries, but when P.F. Chang's credit card servicer sought $1.9 million for costs incurred by their customers, Federal denied the claim. Federal argued that the credit card servicer did not itself sustain a Privacy Injury because it was not their records that were compromised during the data breach. The court agreed with Federal and held that they need not cover the loss.

There is a class of cases in which a grant of coverage for cyber risks was denied not based on cyber exclusions but rather on the grounds of causation—that is, the cyber issue was not, in fact, the cause of the loss.[76] Concurrent causation and proximate cause principles have not disappeared simply because we have a new cause.[77]

In the same way, the insured's breach of its duty of cooperation or at least breach of the insured's obligation to obtain insurer consent to settlement has been held to preclude recovery for a settlement involving infectious malware.[78] Another familiar kind of resolution, temporal limits relating to restoration expenses, has been held to be sufficient to deny coverage for damages occurring outside of a "period of restoration."[79]

Again, the larger point is that no new body of law particular to cyber risks has emerged and it is not clear that a critical mass of decisions is required to make sense of this area. The field is yet too new for any trend to emerge. At the same time, it can

[73] No. CV–15–01322–PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016).

[74] No. CV–15–01322–PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016) at 12.

[75] No. CV–15–01322–PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016) at 12.

[76] *InComm Holdings Inc. v. Great Am. Ins. Co.*, 2017 U.S. Dist. LEXIS 38132; 2017 WL 1021749 at 23 (policy language providing coverage for "computer fraud" did not cover fraud on the part of those who used telephones to defraud the insured); *Apache Corp. v. Great American Ins. Co.*, 662 Fed. Appx. 252, 258–259 (5th Cir. 2016) (computer was not direct cause of loss and use of email was "merely incidental" and noting every fraud that uses email is not a computer fraud).

[77] Dominitz (2017), pp. 34–35 (discussing causation issues).

[78] *First Commonwealth Bank v. St. Paul Mercury Ins. Co.*, 2014 U.S. Dist. LEXIS 141538; 2014 WL 4978383 at 10–11 (settlement with customer for damage caused to client by malware not covered because insured failed to obtain insurer consent).

[79] *WMS Indus. v. Fed. Ins. Co.*, 588 F. Supp. 2d 730, 733–734 (S.D. Miss. 2008) (potential network damage claim denied on the basis that the claim was not within the time window specified in the policy—"during the period of restoration").

be observed that the resort to familiar words is common. Thus, the appearance of familiar terms such as "use" and "proprietary" allows courts to fall back on the treatment of those terms in settled contexts for use in the cyber arena. Similarly, resort to familiar principles of illusory coverage as in *First Bank of Delaware, Inc. v. Fidelity & Deposit Company of Maryland* provides a means of resolution as well. Still, with many questions yet to be addressed by the courts, we will likely see more incarnations of cyber liability policies.[80]

5 Fixing It All

The issues raised by cyber risks present knotty problems, and easy solutions are elusive. One solution is for insurers to do nothing—not offer coverage at all, secure in the knowledge that CGL policies are unlikely to provide coverage. Another approach is to only offer policies with modest limits or sub-limits in an effort to limit risk.[81] Both of these approaches are unsatisfactory. First, there is need—insurance exists for a reason. Policyholders need to protect themselves against the risk of loss. Second, the money involved is significant—insurers are in business to make money, and insureds need protection. With this background, at least three approaches can be taken.

5.1 Resort to Cyber Security Firms

First, organizations can resort to various cyber security firms to head off problems before they occur.[82] Because each organization's system infrastructure and security posture is unique, cyber security firms often employ several vulnerability assessments which include simulated cyber attacks.[83] While these firms do provide accurate vulnerability assessments, their accuracy is immediately outdated as it is a point-in-time view of an organization's security posture.[84] The difficulty with security is that it is often very much an after-the-fact approach. The plans that emerge, almost by definition, are intricate and can address crucial aspects such as

[80]For an interesting discussion of whether exclusions for "acts of war" and "warlike activity" apply to state sponsored acts cyber-attacks, see Doherty (2017), p. 16.

[81]There is ample evidence that the use of modest limits or sublimits is widespread. Romanosky et al. (2017), p. 11; Buchanan and Gallozzi (2018). (suggesting that, in some cases, $100 million limits are far too low given the large potential losses. A more insidious observation is that modest limits or sublimits "are effectively exclusions masquerading as coverage grants . . . ." Buchanan and Gallozzi (2018).

[82]Stephens and Tilton (2017), pp. 12, 17.

[83]Enigbokan and Ajayi (2017), pp. 112, 114.

[84]Boyce (2001).

initial identification of a problem to response and recovery protocols.[85] While firms can guard against known risks, human ingenuity has so far been successful in circumventing security that is based solely on known risks.

5.2 Consolidation of Cyber Perils

Second, insurers could develop a small taxonomy of issues that can arise. By grouping issues under the umbrella of a defined rubric, effective and predictable exclusions might emerge.[86] So far, the experience with exclusions seems to show that this does not seem promising.

The long lists of cyber risks are destined to become longer yet, and our ability to predict the possibilities that can lead to a cyber loss is limited because cyber villains seem to have an ever-increasing repertoire. However, the possibilities can be managed by more generalist categories. While I resist any claim that the following is necessarily the best taxonomy, one has to start someplace, and my gentle suggestion is that the perfect taxonomy would contain significant elements of the categories below.

The first category of cyber risks would be those associated with conventional torts. These could include libel, defamation, and related torts committed using electronic means. This list might also include the civil equivalent of the criminal list below.

The second category of cyber risks would be those associated with crime. This list might include extortion, identity theft (theft is theft whatever the means used to commit it), and terrorism. This category might also include criminal rewards connected to the cyber-crime involved.

A third category of cyber risk would be the costs associated with cyber risks. This might be the broadest, and newest, type of loss. These might include the costs associated with restoring and replacing data, regulatory compliance (mentioned as a fourth category below), professional services, corruption of data, crisis management, public relations expenses, and security malfunctions.

A final category might include cyber risks that are accompanied by some sort of statutory or regulatory liability. For instance, certain provisions of the Health Insurance Portability and Accountability Act (HIPAA) govern the collection and storage of medical records and provide statutory damages for the negligent handling of patients' personal information.[87] The states are also entering this arena. For example, last spring New York's Department of Financial Services issued cyber-

[85] Stephens and Tilton (2017), pp. 12, 17.

[86] There is some indication that this is happening in a way. Researchers have discovered that six sample policies contained about 88% of the coverages available suggesting that the insurance industry itself is consolidating the perils it is willing to cover. Romanosky et al. (2017), p. 10.

[87] *See* 42 U.S.C. § 1320d–5.

security regulation 23 NYCRR 500.[88] The regulation requires companies to create a cybersecurity policy that fulfills statutory minimum standards to protect consumer information and information technology systems from cyber-attacks.[89] The large point is that federal and state government regulation in this area enlarges the range of cyber risks to include potential statutory liability.

The taxonomy above is harm-based while traditional insurance law has been peril-based. An argument can be made that the peril is so diffuse—given the different types of cyber risks—that the time has come to shed the peril-based approach and transition to a harm-based system. This transition is not as radical a proposal as it sounds. There is evidence that insurers base their premiums not on the insured's "attack surface" or technology/governance controls but rather on the insured's asset value.[90] If such is the case, the regime seems to have shifted to a harm-based system, and there may be little difference in moving to a pure harm-based system.

5.3 Risk Rating Mechanisms

Alternatively, insurers could use risk rating mechanisms. Similar to credit risk managers, the idea is to develop an overall cyber risk rating that insurers can use to assess risk and price the insurance product accordingly.[91] Risk rating firms accomplish this through evaluation of "publicly available data on security behaviors from collection points across the globe."[92] The data evaluated consists of compromised system reports, system configuration information, user behavior, and

[88]N.Y. Comp. Codes R. & Regs. tit. 23, § 500.00 (2017); Stephens and Tilton (2017), p. 12.

[89]N.Y. Comp. Codes R. & Regs. tit. 23, §§ 500.02-500.17 (2017) (These minimum standards include requirements for: penetration testing, vulnerability assessments, audit trail assessments, access privilege restrictions, application security, risk assessments, multi-factor authentication, limitations on data retention, training and monitoring requirements, incident response plans, encryption requirements, and specific notice to the superintendent of cyber events).

[90]Romanosky et al. (2017), pp. 19, 31. Applications for insurance seem to require only rudimentary information. *Id.* at 19.

[91]BitSight, Inc. Making Risk Management More Effective with Security Ratings. https://cdn2.hubspot.net/hubfs/277648/White_Papers/Making%20Risk%20Management%20More%20Effective%20with%20Security%20Ratings.pdf?t=1529692882780&utm_campaign=resource-center&utm_source=hs_automation&utm_medium=email&utm_content=12350311&_hsenc=p2ANqtz-9Z69TfjcYiqDG1sxGgigc_ol5AWlkpr0LApLGvyMDKfq_aaYPVgOGwqRX8Cpn1KMQo_6dhpDNeAEHyiUlikfdjJ-zCqDcr0O8IwWW_V2SF6fL53K0&_hsmi=12350311.

[92]BitSight, Inc. Making Risk Management More Effective with Security Ratings. https://cdn2.hubspot.net/hubfs/277648/White_Papers/Making%20Risk%20Management%20More%20Effective%20with%20Security%20Ratings.pdf?t=1529692882780&utm_campaign=resource-center&utm_source=hs_automation&utm_medium=email&utm_content=12350311&_hsenc=p2ANqtz-9Z69TfjcYiqDG1sxGgigc_ol5AWlkpr0LApLGvyMDKfq_aaYPVgOGwqRX8Cpn1KMQo_6dhpDNeAEHyiUlikfdjJ-zCqDcr0O8IwWW_V2SF6fL53K0&_hsmi=12350311.

data breach events.[93] Risk rating firms then report risk ratings on a daily basis to security professionals, risk managers, and underwriters. This provides insureds with benchmarks for security performance, visibility into security risks posed by third parties, and real-time awareness of security risk changes.[94] These firms strive to create systems that shed light on the risks an organization faces within a landscape of ever-changing threats. Having real-time awareness of security risks allows insurers to reduce loss ratios by: "addressing security events on their insured's network or extended ecosystem before the claim occurs"; "improve underwriter effectiveness" by "setting underwriter thresholds based on security ratings"; and allowing insurers to "identify and mitigate concentration risk[s]" across their portfolios.[95]

To work, the insurance policies would almost have to be "all risk" policies because of the definitional problems outlined above. This approach has merit, but the experience is lacking. Currently, one company reported it has 70% of the security rating market with over 1000 customers,[96] demonstrating there is some adoption in the market, but even this is a drop in the bucket of experience. In sum, much work and uncertainty remain.

6 Conclusion

Cyber risks raise the classic question of whether existing legal regimes are up to the task of dealing with new technologies. Initially, the expectation was that cyber loss coverage was going to be different. That does not seem to be the case. So far, case history suggests that conventional insurance law has been up to the task of dealing with cyber risks. A caveat is in order, however, as the courts so far have not had to deal with the intricacies of cyber coverage or cyber exclusions.[97]

The wilderness of insurance coverage has always necessitated vigilance by policyholders when assessing coverage. However, that wilderness has, by now, been tamed with settled judicial interpretations and well-defined potential perils

[93]BitSight, Inc. Making Risk Management More Effective with Security Ratings. https://cdn2.hubspot.net/hubfs/277648/White_Papers/Making%20Risk%20Management%20More%20Effective%20with%20Security%20Ratings.pdf?t=1529692882780&utm_campaign=resource-center&utm_source=hs_automation&utm_medium=email&utm_content=12350311&_hsenc=p2ANqtz-9Z69TfjcYiqDG1sxGgigc_ol5AWlkpr0LApLGvyMDKfq_aaYPVgOGwqRX8Cpn1KMQo_6dhpDNeAEHyiUlikfdjJ-zCqDcr0O8IwWW_V2SF6fL53K0&_hsmi=12350311.

[94]BitSight, Inc. Making Risk Management More Effective with Security Ratings. https://cdn2.hubspot.net/hubfs/277648/White_Papers/Making%20Risk%20Management%20More%20Effective%20with%20Security%20Ratings.pdf?t=1529692882780&utm_campaign=resource-center&utm_source=hs_automation&utm_medium=email&utm_content=12350311&_hsenc=p2ANqtz-9Z69TfjcYiqDG1sxGgigc_ol5AWlkpr0LApLGvyMDKfq_aaYPVgOGwqRX8Cpn1KMQo_6dhpDNeAEHyiUlikfdjJ-zCqDcr0O8IwWW_V2SF6fL53K0&_hsmi=12350311.

[95]BitSight Technologies (2018) https://www.bitsighttech.com/security-ratings-cyber-insurance.

[96]BitSight Technologies (2018) https://www.bitsighttech.com/bitsight-vs-competitors.

[97]Nitardy (2017), pp. 26, 31 (questioning whether insurance law can evolve with technology).

which policyholders use to accurately predict claim outcomes. Yet, with cyber risks, the paths are neither well-trod nor carefully maintained; there is no certainty of court-vetted terms or even a well-defined set of potential perils.[98] Until these paths emerge, the prescription to "understand the cyber-physical risks involved" and to "understand how all policy language will respond to those risks" cannot be overstated.[99]

Looking forward, while recognizing that the range of cyber risks will only increase, a solution that involves some combination of "all cyber risks" is worth exploring. Indeed, to the extent insurers are assessing risk based on asset value and using an "all risk" approach to rating mechanisms, this idea is not as radical as it seems. As noted above, the policyholders' needs are great, and insurers have before them an equally great opportunity. The solution to the cyber risk problem will not be simple, will not be conventional, and will not be obvious. But, if done right, cyber risk insurance can become a benefit to insureds and insurers alike.

References

42 U.S.C. § 1320d–5

America Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 95 (4th Cir. 2003)

American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., 2000 U.S. Dist. LEXIS 7299; 2000 WL 726789 at 7

Anthem Elecs., Inc. v. Pac. Emplrs. Ins. Co., 302 F.3d 1049 1058-59 (9th Cir. 2002)

Apache Corp. v. Great American Ins. Co., 662 Fed. Appx. 252, 258-59 (5th Cir. 2016)

Ashland Hosp. Corp. v. Affiliated FM Ins. Co., 2013 U.S. Dist. LEXIS 114730 at 18-19 (E.D. Ky. 2013)

Ashland Hosp. Corp. v. Affiliated FM Ins. Co., 2013 U.S. Dist. LEXIS 114730 at 18-19 (E.D. Ky. 2013)

BitSight, Inc. Making Risk Management More Effective with Security Ratings. https://cdn2.hubspot.net/hubfs/277648/White_Papers/Making%20Risk%20Management%20More%20Effective%20with%20Security%20Ratings.pdf?t=1529692882780&utm_campaign=resource-center&utm_source=hs_automation&utm_medium=email&utm_content=12350311&_hsenc=p2ANqtz-9Z69TfjcYiqDG1sxGgigc_ol5AWlkpr0LApLGvyMDKfq_aaYPVgOGwqRX8Cpn1KMQo_6dhpDNeAEHyiUlikfdjJ-zCqDcr0O8IwWW_V2SF6fL53K0&_hsmi=12350311

Boyce R (2001) Vulnerability assessments: the pro-active steps to secure your organization. SANS Institute. https://www.sans.org/reading-room/whitepapers/threats/vulnerability-assessments-pro-active-steps-secure-organization-453

Buchanan J, Cho D, Rawsthorne P (2018) When things get hacked: coverage for cyber-physical risks. ABA Litigation Section, Insurance Coverage Litigation Committee. https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2016_insurance_coverage_litigation_committee/written_materials/2_cyber_physical_harms_paper_final.authcheckdam.pdf

Buchanan JG, Gallozzi MS (2018) Kicking the tires on a new cyber policy: top tips and traps. American Bar Ass'n. https://www.americanbar.org/groups/litigation/committees/insurance-coverage/articles/2017/cyber-policy-tips-traps.html

[98] Jerry and Mekel (2001), pp. 7, 30; Nitardy (2017), pp. 26, 31; Buchanan and Gallozzi (2018).

[99] Buchanan et al. (2018).

Centennial Ins. Co. v. Applied Health Care Sys., Inc., 710 F.2d 1288, 1290 (7th Cir. 1983)
Computer Corner, Inc. v. Fireman's Fund Ins. Co., 132 N.M. 264, 266 (N.M. Ct. App. 2002)
Cope CE, Reynolds I (2015) "Breaking Bad" in Cyberspace: A Challenge for the Insurance Industry. Emerging Issues 7296
Doherty KR (2017) The Art of (Cyber) War. Intell Prop Technol Law J 29(6):16
Dominitz EJ (2017) To err is human; to insure, divine: shouldn't cyber insurance cover data breach losses arising (in whole or in part) from negligence? The Brief 46(4):32, 33 (describing cyber losses as "not just a passing fad")
Enigbokan O, Ajayi N (2017) Managing cybercrimes through the implementation of security measures. J Inf Warf 16:112, 114
Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 802 (8th Cir. 2010)
First Bank of Del., Inc. v. Fid. & Deposit Co. of Md., 2013 Del. Super. LEXIS 465 at 5-7
First Commonwealth Bank v. St. Paul Mercury Ins. Co., 2014 U.S. Dist. LEXIS 141538; 2014 WL 4978383 at 10-11
Garrie D, Mann M (2014) Cyber-security insurance: navigating the landscape of a growing field. J Marshal J Inf Technol Priv Law 31:389–390
Hartwig RP, Wilkinson C (2014) Cyber risks: the growing threat. Insurance Information Institute. http://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf
InComm Holdings Inc. v. Great Am. Ins. Co., 2017 U.S. Dist. LEXIS 38132; 2017 WL 1021749 at 23
Insurance Services Office, Inc. (2013) Exclusion — Access or Disclosure of Confidential or Personal Information and Data-Related Liability — With Limited Bodily Injury Exception, *CG 21 06 05 14*
Jerry RH, Mekel ML (2001) Cybercoverage for cyber-risks: an overview of insurers' responses to the perils of E-Commerce. Conn Inst Law J 7:11–17
Latham & Watkins (2014) Cyber Insurance: A Last Line of Defense When Technology Fails. https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage
Martinez LP, Richmond DR (2018) Insurance law, 8th edn. West Publishing Co
Matthew Bender & Company, Inc. (2nd 2011) Appleman on Insurance Law & Practice Archive. 20-129 § 129.2
N.Y. Comp. Codes R. & Regs. tit. 23, § 500.00 (2017)
N.Y. Comp. Codes R. & Regs. tit. 23, §§ 500.02-500.17 (2017)
Nitardy ME (2017) Fraud involving a computer is not automatically "Computer Fraud". Brief 46 (4):27
O'Donnel B, Oonk LA (2017) Changes in latitudes, changes in attitudes: looking back over 25 years of coverage litigation. Brief 47:10–11
OOIDA Risk Retention Grp., Inc. v. Griffin, 2016 U.S. Dist. LEXIS 57469 at p. 15 (E.D. Va. 2016)
Oshinsky J, Lee K (2010) Insurance coverage for cyber crimes. L.A. DAILY J. 14 April 2010. https://jenner.com/system/assets/publications/435/original/Oshinsky_Lee_Coverage_for_Cyber_Crimes_LA_Daily_Journal.pdf?1313595662
Ostrander B (2006) Chasing Moore's Law: information technology policy in the United States. J High Technol Law 5:1
P.F. Chang's China Bistro, Inc. v. Federal Insurance Company, No. CV–15–01322–PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016)
Ponemon L (2016) 2016 Cost of data breach study: global analysis. Ponemon Institute. Available at https://securityintelligence.com/media/2016-cost-data-breach-study/
Retail Sys., Inc. v. CNA Ins. Cos., 469 N.W.2d 735 (Minn. Ct. App. 1991)
Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821, 824-26 (6th Cir. 2012)
Romanosky S et al (2017) Content analysis of cyber insurance polices. Rand Corp WR-1208:3, 14
Schwarcz D (2017) Coverage information in insurance law. Minn Law Rev 101:1500-02
Selective Way Ins. Co. v. Crawl Space Door Sys., 162 F. Supp. 3d 547, 551 (E.D. Va. 2016)
Southeast Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831, 838 (W.D. Tenn. 2006)

State Auto Property & Cas. Ins. Co. v. Midwest Computers & More, 147 F. Supp. 2d 1113 (W.D. Okla. 2001)

Stephens JF, Tilton MW (2017) Lawyers still lag behind in network and information security risk management: clients and regulators demand more. Brief 46(4):12, 15

Sun M (June 21, 2018) Europe's Privacy Law Fails to Stoke Demand for Cyber Insurance, WSJ B10

Travelers Indemnity Co. v. Portal Healthcare Solutions, LLC, 35 F. Supp. 3d 765 (E.D. Va. 2014), *aff'd per curiam*, 644 Fed. Appx. 245 (4th Cir. 2016)

Union Pump Co. v. Centrifugal Tech., Inc., 2009 U.S. Dist. LEXIS 86352 (W.D. La. 2009) (electronic data is not tangible property)

Ward General Ins. Services, Inc. v. Employers Fire Ins. Co., 114 Cal. App. 4th 548, 556 (2003)

WMS Indus. v. Fed. Ins. Co., 588 F. Supp. 2d 730, 733-34 (S.D. Miss. 2008)

Wood SA et al (2017) Aviation and cybersecurity: an introduction to the problem and the developing law. Brief 46(4):38–39

Cybersecurity and Environmental Impact: Insurance as a Better Protection Mechanism for Liability from Incidents in Oil and Gas Operations

Kyriaki Noussia

1 Introduction

The globalisation of environmental risk poses a mounting challenge to policy makers. We are nowadays faced with a situation whereby the rules of responsibility for harm production remain underdeveloped, in spite of the negotiation and implementation of numerous international environmental agreements. In addition, those agreements lack detailed provisions stipulating the responsibility of state and non-state actors for environmental damage and state practice often reflects a widespread reluctance to pursue environmental liability through inter-state claims and a preference for increasing the importance of private liability attached to operators of risk-bearing activities as the main mechanism for progressing environmental liability.[1]

The civil liability regime for marine and oil pollution was the first of these regimes to broaden compensation obligations beyond personal injury and property damage provisions to environmental impairment and has served as a model for liability rule development for all activities related to oil and gas expropriation and its transportation.[2]

Several types of insurance might respond to pay for losses stemming from an oil spill, including, insurance policies for first-party property, "business interruption" and loss of production income insurance, directors & officers liability (D&O) insurance, event cancellation insurance, trade disruption insurance, environmental

[1] Noussia (2011), pp. 98–107.

[2] Mason (2002), pp. 1–3; Sandvik and Suikkari (1997), pp. 64–65.

K. Noussia (✉)
Law School, University of Exeter, Exeter, UK
e-mail: k.noussia@exeter.ac.uk

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_11

liability insurance, marine insurance, comprehensive general liability insurance, insurance for operator's extra expenses—occurred for the control of the well, physical damage insurance, workers compensation or employers liability insurance.[3,4]

2 The Deep Water Horizon and the Saudi Aramco Incidents: The Facts in a Nutshell

On 20th April, 2010, the Deepwater Horizon, a semi-submersible mobile offshore drilling rig owned and operated by Transocean Ltd., caught fire and sank in the Gulf of Mexico, off the shores of Louisiana. The rig was drilling a prospect known as "Macondo", some 50 miles off the coast of Louisiana, in 5000 feet of water. BP Plc—along with its partners Anadarko Petroleum Corp. and Mitsui Oil Exploration Co.—acquired the prospect in 2008 in a sale of leases run by the U.S.A. government's Minerals Management Services. The well had been drilled to 18,000 feet when a blow-out occurred. The explosion, and fire that followed, killed 11 out of the 126-man crew. A day-and-a-half later the rig collapsed into the sea and sunk, and oil begun to spread across the surface of the water, eventually making landfall to the north-east.[5] BP, being the majority stakeholder in the "Macondo oil well", was largely identified with the spill. Anadarko Petroleum Corp. and Mitsui Oil Exploration Co. own 25% and 10% stakes in the well, respectively, and hence also a share in the cost of responding to the oil spill. The oil platform was being leased by Transocean Ltd. to BP Plc., and following the accident sat on the sea floor over 5000 feet below sea level. Before the explosion on April 20, 2010, Halliburton Co. had been engaged in cementing operations on the well, and cementing operations have previously been associated with other oil well accidents. The explosion and fire occurred in spite of the existence of specialised oil spill prevention equipment—called a blowout preventer (BOP)—i.e. a failsafe protection against an ongoing oil spill, manufactured by Cameron International Corp.,[6] and especially designed to avert this type of disaster.[7] The failure of the BOP left the well unsecured and leaking from the marine riser. BP Plc set up an escrow account of US $20 billion to meet an unspecified number of claims for consequential losses arising from the oil spill.[8] The amount of oil and gas, escaping from the subsurface well had been estimated to have been in the range of 35,000–60,000 barrels of oil a day, making the incident the

[3]Kellner et al. (2010).

[4]Noussia (2011), pp. 98–107.

[5]Focus Magazine (2010), p. 3.

[6]Kotula, Insurance, pollution exclusions, and the Deepwater Horizon Gulf of Mexico oil spill, http://www.lexisnexis.com/Community/emergingissues/blogs/gulf_oil_spill.aspx.

[7]King (2010), p. 3.

[8]Focus Magazine (2010), p. 3.

largest oil spill in U.S.A. history.[9] The "Macondo oil well", was initially sealed in mid July 2010, 87 days after the incident occurred, it was then subsequently further sealed in early August 2010, having reached the amount of 4.1 million oil barrels, and finally cemented on 19th September 2010. However, the termination of the oil spillage does not, necessarily, entail a simultaneous end to the legal aspects of it. The imposition of fines, the adjudication of class action law suits by the thousands of victims, the cleansing and environmental rehabilitation operations have been, only, some of the consequences of the oil spillage.

In 2012, the oil and gas world witnessed the worst hack ever seen. A monstrous cyber attack on Saudi Aramco, one of the world's largest oil companies, almost halted the world's oil production and almost created a worldwide economic crash.[10] In a matter of hours, 35,000 computers were partially wiped or totally destroyed. Without a way to pay them, gasoline tank trucks seeking refills had to be turned away. Saudi Aramco's ability to supply 10% of the world's oil was suddenly at risk and suddenly one of the most valuable companies on Earth was propelled back into 1970s technology, using typewriters and faxes. When it comes to sheer cost, comparison with other cyber attacks pale in comparison. Indeed, the average person may have never heard about Saudi Aramco—or this hack. However, consciously or not we all felt its mysterious reverberations. The incident entails one of the computer technicians on Saudi Aramco's information technology team opening what proved to be a scam email and innocently clicking on a bad link, hence without knowing it, allowing the hackers in. The actual attack began during the Islamic holy month of Ramadan, when most Saudi Aramco employees were on holiday. Initially, on the morning of Wednesday, Aug. 15, 2012, the few employees noticed their computers were acting weird. Screens started flickering. Files began to disappear. Some computers just shut down without explanation. In a frantic rush, Saudi Aramco's computer technicians ripped cables out of the backs of computer servers at data centres all over the world. Every office was physically unplugged from the Internet to prevent the virus from spreading further. Oil production remained steady at 9.5 million barrels per day, according to company records. Drilling, pumping—all of that was automated, but the rest of the business was in turmoil. Managing supplies, shipping, contracts with governments and business partners—all of that was forced to happen on paper. Without internet at the office, corporate email was gone. Office phones were dead. Employees wrote reports on typewriters. Contracts were passed around with interoffice mail. Lengthy, lucrative deals needing signatures were faxed one page at a time. The company temporarily stopped selling oil to domestic gas tank trucks. After seventeen days, the corporation relented and started giving oil away for free to keep it flowing within Saudi Arabia. A massive army of IT people were hired

[9]Deepwater Horizon Unified Command, U.S. Scientific Team Draws on New Data, Multiple Scientific Methodologies to Reach Updated Estimate of Oil Flows from BP's Well, June 15, 2010, at http://www.deepwaterhorizonresponse.com/go/doc/2931/661583; Winter (2010); King (2010), p. 3.

[10]Pagliery (2015).

as independent consultants to help secure all of Saudi Aramco's satellite offices in Africa, Europe and the Middle East. The corporate giant also flexed its muscle. It flew representatives directly to computer factory floors in Southeast Asia to purchase every computer hard drive currently on the manufacturing line. In one fell swoop, it bought 50,000 hard drives hence causing a temporary worldwide shortage on hard drives. Five months later, with a newly secured computer network and an expanded cybersecurity team, Saudi Aramco brought its system back online. However, the repercussion and ramifications were still to be felt for many months to follow. It is a blessing in disguise that no connection to networks was possible for storage tanks at that time. The attack was a wake-up call for the possible ramifications of a possible further cyber attack in the oil and gas sector.[11]

Both the BP Oil Spill and the Saudi Aramco cyber attack force a response in the regulatory landscape for environmental pollution liability and at the same time have triggered changes in the insurance industry landscape both in terms of environmental and cyber related risk coverage.

3 The Environmental (Marine & Oil) Pollution Liability Legal Regime and Its Impact on Insurance Schemes

The marine and oil pollution liability legal regime has been developed via the various conventions, resolutions and codes that the United Nations International Maritime Organisation (IMO) has enacted. The 1973/78 International Convention for the Prevention of Pollution from Ships (MARPOL) stands as the core treaty in this area.[12] MARPOL followed as one of the consequential measures adopted after the Torrey canyon oil disaster of 1967.[13] However, the immensity of the Exxon Valdez incident in 1989 prompted the imposition of further measures; hence, the Oil Pollution Act 1990 (OPA) was enacted in the U.S.A. in 1990, which imposed stronger duties of care to ship-owners and also included a right of action against operators. Not least, it also shifted the burden of accountability, i.e. liability, towards the harm producer. However, it is the International Convention on Civil Liability for Oil Pollution (CLC) 1992 and the International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (Fund) 1992, in force as of 1996, which have set the current terms of application of claims for compensation within contracting states.[14,15]

[11]Pagliery (2015).

[12]Its Annex I, concerned with oil pollution, contains detailed technical provisions designed to eliminate intentional discharges. MARPOL is credited as instrumental in significantly reducing discharges from marine transportation; Mason (2002), p. 4.

[13]Mason (2002), p. 4.

[14]Mason (2002), pp. 6–7; Little and Hamilton (1997), pp. 554–557; Gauci (1999), pp. 29–36.

[15]Noussia (2011), pp. 98–107.

The international regime for the compensation of pollution damage caused by oil spills from tankers is based on two treaties adopted under the auspices of the IMO, the CLC 1992 and the Fund 1992 Conventions, which replace two corresponding Conventions adopted in 1969 and 1971 respectively.[16] Article I(6) of the CLC 1969 defined pollution damage as "loss or damage caused outside the ship carrying oil by contamination resulting from the escape or discharge of oil from the ship, wherever, such escape or discharge may occur, and includes the cost of preventive measures and further loss of damage caused by preventive measures". While it was clear from the beginning that this wording covered economic losses connected with property damage or personal injury, the absence of any reference to environmental damage left this aspect to the interpretation of national courts as per the, each time, domestic implementation of the CLC.[17] However, because of some destabilising liberal court rulings on damage, the environmental damage Article I(6) of the CLC 1992 was transformed and hence pollution damages was defined as: "a) loss or damage caused outside the ship by contamination resulting from the escape or discharge from the ship, wherever such escape or discharge may occur, provided that compensation for impairment of the environment other than losses of profit from such impairment shall be limited to costs of reasonable measures of reinstatement actually undertaken or to be undertaken (emphasis added), and b) the costs of preventive measures and further loss of damage caused by preventive measures".[18] As a system of economic compensation for oil spill damage, the recovery of environmental reinstatement costs under the CLC/ Fund Conventions' regime has turned on whether they are deemed acceptable under the international rules.[19]

The existence of a spatial delimitation of oil pollution liability under the international conventions has always deferred to the sovereign rights of contracting parties, for, both the CLC 1969 (Article II) and the Fund Convention 1971 (Article 3) apply only to pollution damage caused or impacting on the territory, including the territorial sea, of Member States. However, the broadening of the geographical scope of the liability conventions was considered essential and was reinforced by an international agreement, which clarified that the liability Conventions cover measures—wherever taken—to prevent oil pollution damage within a territorial sea or EEZ.[20] As incorporated into CLC 1992 (Article II) and the Fund Convention 1992 (Article 3), the oil pollution liability conventions are geographically defined as applying exclusively: (a) to pollution damage caused: (i) in the territory, including the territorial sea, of a Contracting State, and (ii) in the exclusive economic zone (EEZ) of a Contracting State, established in accordance with international law, or, if a Contracting State has not established such a zone, in an area beyond and adjacent to the territorial sea of that State determined by that State in accordance with international law and

[16]Jacobsson (2007), pp. 138–139.

[17]Mason (2002), pp. 7–8; Wetterstein (1994), pp. 230–247.

[18]Mason (2002), p. 7; International Maritime Organisation (1996).

[19]Mason (2002), p. 8.

[20]Mason (2002), pp. 11–12; International Maritime Organisation (1996), pp. 48, 69.

extending not more than 200 nautical miles from the baselines from which the breadth of the territorial sea is measured; and (b) to preventive measures—wherever taken—to prevent or minimise such damage.[21]

The CLC 1992 lays down the principle of strict liability for ship-owners and creates a system of compulsory liability insurance. Ship-owners are normally entitled to limit their liability to an amount which is linked to the tonnage of the ship. The CLC also set up the International Oil Pollution Compensation Fund that provides additional compensation to victims when compensation under the 1992 CLC is inadequate.[22] The 1992 Fund Convention accepts claims in relation to loss of earnings suffered by the owners or users of contaminated property because of a spill (i.e. consequential loss). An important group of claims comprises those relating to "pure economic loss", i.e. loss of earnings sustained by persons whose property has not been polluted. To qualify for compensation, a sufficient causation link between the contamination and the loss or damage sustained by the claimant must exist.[23]

The strict marine oil pollution civil liability model, which was imposed by the CLC 1992 and the Fund 1992 Conventions, has been further extended to the International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea, (HN) 1996 and the International Convention on Liability for Bunker Oil Pollution Damage, (BOPD) 2001.[24] These Conventions broadly share the environmental reinstatement provisions and jurisdictional scope of CLC 1992. Significantly though, the BOPD Convention 2001, which covers fuel oil spills from vessels other than tankers, breaks with the liability channelling provisions of the CLC 1992, by exposing to compensation claims operators and charterers as well as registered owners, all with rights of limitation. This notable shift to multiple liabilities indicates pressure from the U.S.A. and the European Commission on IMO to accord more with the existing American liability norms in this area of oil pollution, and it also reflects the need to make up for the absence of a second tier of supplementary compensation—as under the Fund Convention.[25]

In the USA, the previous, i.e. the Obama administration outlined new drilling regulations, and, in January 2017, the Environmental Protection Agency (EPA) introduced several changes to companies' risk management plans. Contrary to the above, the current, i.e. the Trump administration proposed to rollback the offshore drilling safety regulations to ease restrictions on fossil fuel companies and generate more domestic energy production, in an effort also to reduce "unnecessary burdens" on the energy industry. The proposal would also delay some of the compliance dates of the Obama-era amendments and cancel certain provisions that address accident

[21]Mason (2002), pp. 11–12; International Maritime Organisation (1996), pp. 48, 69.

[22]Jacobsson (2007), pp. 138–139.

[23]Jacobsson (2007), p. 141.

[24]Mason (2002), p. 20; Little (1998), pp. 554–567; Wren (1999), pp. 335–349.

[25]Mason (2002), p. 20; Wu (2001).

prevention. Such a proposal was under public consultation until the middle of June 2018 whereby further legislative action was to be awaited.

Moreover, the Trump administration issued on May 11, 2017 Executive Order 13800 on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" ("E.O. 13800" or "the cybersecurity E.O."), which directed key departments and agencies to: (i) report on U.S. government international engagement priorities in cyberspace; (ii) develop strategies to strengthen the deterrence posture of the United States in cyberspace; and, (iii) enable the United States to engage proactively with all partners to address key issues in cyberspace. In May 2018, the U.S. Department of State drafted a report as a response, which advances the goal of strengthening coordinated U.S. government cooperation with foreign partners and allies to address shared threats in cyberspace, thereby improving the cybersecurity of the nation. It describes the United States' priority policies, five primary objectives and corresponding actions, and three principal means of engagement to ensure continued benefits and minimised risks in cyberspace. The US Cyberspace Policy enhances international cooperation and seeks to ensure that the Internet and other connected networks and technologies remain valuable and viable tools for future generations. Through cooperation with foreign partners and allies, and engagement with all stakeholders as appropriate, the US aims to (a) increase international stability and reduce the risk of conflict stemming from the use of cyberspace, (b) identify, detect, disrupt, and deter malicious cyber actors; protect, respond to, and recover from threats posed by those actors; and enhance the resilience of the global cyber ecosystem, including critical infrastructure, (c) advance an international regulatory environment that supports innovation and respects the global nature of cyberspace, (d) uphold an open and interoperable Internet where human rights are protected and freely exercised and where cross-border data flows are preserved, (e) maintain the essential role of non-governmental stakeholders in how cyberspace is governed.[26]

In the aftermath of the DWH and Saudi Aramco incidents, it is crucial to consider the willingness of the global offshore energy insurance market to participate in efforts to establish and fix a new liability limit for environmental pollution liability insurance. Such a new limit of liability will have to be informed by the availability of insurance coverage on adequate terms and conditions in the global commercial insurance market for offshore energy facilities. It will have to consider the vulnerability of the insurability of future offshore oil spill hazards and the impact of global financial market conditions on insurance market's capacity for underwriting 'catastrophe' or 'peak' risks, including oil spill damages.[27]

[26]Office of the Coordinator for Cyber Issues, Recommendations to the President on Protecting American Cyber Interests through International Engagement, 31/5/2018 https://www.state.gov/documents/organization/282224.pdf.

[27]King (2010), pp. 15–20.

Later though, energy insurance underwriters reassessed their risk exposures in response to newly perceived operational risks involving blowouts, fires, explosions, lost control of well and other non-hurricane risks.

The proposed increase in the limit of liability required under the Oil Pollution Act (OPA) carried at least four of its elements and consequences in the offshore energy insurance and reinsurance market: (a) first, 'operators' extra expense' (OEE) and 'excess liabilities' coverage had to be prioritised in terms of a single limit before the balance of the OEE insurance limits used for pollution clean-up and containment of oil spills; (b) second, given the enormity of the BP oil spill coverage has since been at a much higher premium; (c) third, private commercial insurers were expected to not be the same willing to commit financial capital in underwriting unknown new risks, if no extra high premiums were to be agreed, for, in effect the BP oil spill had triggered a 'hard' energy insurance market involving scarcity of coverage and high prices; (d) fourth, many insurance market experts supported a more efficient pre-disaster risk financing approach to managing and financing large-scale oil spill disasters through 'reinsurance sidecars', catastrophe bonds ('CAT bonds') or energy insurance financial futures and options.

4 The Environmental Pollution Insurance Regime and the Structure of the (Offshore) Energy Insurance Market

The (offshore) energy insurance market is highly specialised and because the limits of insurance are usually in excess of US $1 billion, there is no single insurer who covers the entire risk exposure. Consequently, operators of offshore drilling units, production platforms, undersea pipelines and systems for loading oil onto vessels at offshore mooring points, typically insure their property and liability risk exposures on a subscription basis through specialised brokers who negotiate with underwriters in the energy field. Most subscription transactions are negotiated and placed in the London and Bermuda insurance market, usually through Lloyds of London and scores of global reinsurance companies and intermediaries. In the past two decades, the formal organisational structure of the ocean-marine industry underwent a significant cultural and institutional transformation whereby the ocean marine insurance market has become more concentrated with fewer, larger insurers due to overall insurance industry consolidation.

In addition, the size of the ocean marine insurance industry, as a proportion of the overall property and casualty (P&C) insurance industry, has also significantly declined in premium total percentages, and hence from the above, an industry once dominated by individual freestanding mono-line underwriters (i.e. managing agencies/pools) became reportedly dominated by small marine underwriting units subsumed within multiline insurers, either in the commercial or speciality lines divisions. Most of the offshore energy insurers, who traditionally were defined by

their willingness to assume risk without relying on technical analysis, now require professional engineers to evaluate risk and quantify exposures. Some of them even claim, that marine insurance underwriting is now guided not by experienced and knowledgeable underwriters but by computer simulation models and estimates of exposure promulgated by actuaries and quantitative approaches.[28]

Oil and gas firms, whether they have experienced cyber attacks or not, are incentivised to assure that their business processes are resilient in the face of cyber events, internally as well as externally. By adopting methods for examining their systemic risk to cyber events, firms can become aware of the risks they face because of their interdependencies with other firms. Acting to address these risks will make their own business more responsive; consequently, their business sector will also become more resilient. Thus, latent market forces result in the protection of critical infrastructures. Such market forces are strengthened by government initiatives and market response through insurance schemes coverage. Solutions entail the enactment by governments of policies that result in disseminating information about cyber incidents and the serving and deployment of market mechanisms that will serve to address critical infrastructure and other business concerns.[29]

5 Initiatives Taken and Regulatory Approaches

In the UK, the Oil Spill Prevention and Response Advisory Group (OSPRAG) was established in May 2010 to provide a focal point for a review of industry practices. This was a joint government-industry body which reviewed regulation and arrangements for oil spill prevention and response and the adequacy of financial provisions in relation to a UCS response. Indemnities and insurance were matters which OSPRAG specifically looked at, and it finally recommended the creation of an Oil Spill Response Forum to be governed by the Oil & Gas UK.

Its other principal recommendation was the development of the OSPRAG capping device. The UK House of Commons Energy & Climate Change Select Committee (HC Committee) made recommendations in relation to the liabilities and compensation costs that can arise from oil spills. These concerned among other things the OPOL limit and coverage, but also clarity on liability and the ability to pay for an accident. The OPOL limit was substantially increased from US $120 million to US $250 million.

In 2011 a Review Panel was set up in the UK, the purpose of which was to consider findings from official reports that had been published—and were continuing to emerge—into the circumstances surrounding the tragic accident that befell Transocean's DWH rig in the process of drilling BP's Macondo well in April 2010. However, the principal role of the Review Panel exercise was to examine the

[28]Noussia (2011), pp. 98–107, 101–103.

[29]Dynes et al. (2008), p. 27.

recommendations which emerged from these various reports, and inter alia to review the extent to which they might inform modification or improvement of the regulatory regime. The insurance implications were also to be considered.[30] The Panel were concerned that a mechanism should be in place for rapid distribution of compensation after an oil spill had taken place and sought clarification as to who would consider claims and authorise payments. The Department of Energy and Climate Change (DECC) advised that the Operator would administer the funding of all activities. If the operator defaulted then OPOL would step in. However, during discussions with industry representatives, it was clear that there were no set procedures in relation to claims and it was recognised that guidance and good practice on such mechanisms should be an area considered as part of the current work underway under the auspices of Oil Spill Prevention and Response Advisory Group (OSPRAG) and the Indemnity and Insurance Review Group (IIRG).

The insurance industry expressed the view that work should be done to ensure that OPOL has appropriate mechanisms in place to deal with claims in the event of an incident in an effective and timely manner. The Panel recommended that liability and insurance issues should be taken forward as a matter of urgency and that a clear claims and compensation procedure would have to be adopted by all operators, considering the evaluation that is to be carried out of the Gulf Coast Claims Facility once all claims in relation to Macondo would have been paid out.

Other actions taken by the UK include an increase in environmental inspectors and inspections on mobile rigs. A response from the Energy and Climate Change Committee stressed inter alia that the Offshore Pollution Liability Association limit of US $250 million was insufficient and covered only direct damage.[31]

At the EU level, in October 2011 the European Commission proposed a Regulation on the safety of offshore oil and gas prospection, exploration and production activities that aimed to extend the scope of the Environmental Liability Directive (ELD) to include liability for pollution caused to all marine waters. The proposal also called for assessment of the financial capacity of offshore oil licence applicants, including financial security measures.

While insurance can play a role as a tool to transfer the risk of environmental damage caused by EU industries, it cannot provide a complete or feasible solution for the cover of risks in the offshore oil sector. Offshore risks are rare, yet severe, highly complex and extremely difficult to quantify. Few insurers are able to offer this cover and global insurance capacity is highly limited, in contrast with other insurance markets.

The ELD would require complete restoration of the offshore marine environment to its baseline condition following an oil spill. However, the precise level of biodiversity is unknown in such waters, so insurers cannot assess potential damage

[30]Department of Energy and Climate Change, 'Offshore oil and gas in the UK: an independent review of the regulatory regime' (December 2011, U.K.) https://www.gov.uk/government/publications/offshore-oil-and-gas-in-the-uk-independent-review-of-the-regulatory-regime.

[31]Nordquist and Fausser (2014), p. 127.

accurately enough to be able to offer cover. Oil spills cause damage that can last for decades for which the ELD would require the operator (i.e. the offshore oil company) to pay the full economic cost of remediation.

Given the amount of capital, insurers would need to provide sufficient cover, comply with solvency legislation and provide adequate returns to investors, a mandatory insurance regime for this risk would lead to significantly higher insurance costs. Insurers unable to offer the mandated cover would then be likely to leave the EU market altogether, thereby reducing competition and further limiting the availability of insurance.

The greatest impact of rising insurance costs under a mandatory scheme would be felt by the smaller offshore oil contractors, which would be unable to obtain insurance and, thus, forced to leave the market. Lack of insurer capital would translate into reduced underwriting capacity. Because offshore energy sector is global, perhaps an international (rather than an EU) solution to its risks would be more appropriate.

In effect, an extension of the ELD and the possible introduction of mandatory financial security measures into an insurance market in which the necessary preconditions do not exist is likely to lead to higher insurance costs, diminished insurance capacity and less product innovation and competition. However, it has been felt that greater insurance protection and coverage was needed.

Following the above initiatives, in 2013 the OSD Directive, i.e. Directive 2013/30/EU[32] (Offshore Safety Directive—OSD) was introduced, as a way to define the elements of a comprehensive EU-wide framework for preventing major accidents and limiting their consequences. The ratification of the Offshore Protocol of the Barcelona Convention by the Council[33] was also part of the EU response to the Deepwater Horizon disaster. The OSD creates a harmonised EU-wide regulatory regime that establishes a goal-setting regulatory framework built around the concept of a 'safety case' (a Report on Major Hazards) and enforced by offshore regulators whose competence and independence the OSD aims to ensure; it also fosters effective cooperation between such regulators. Furthermore, the OSD introduces EU-wide requirements on transparency, including the sharing of information on accidents and near misses as well as on other indicators of the safety performance of industry and regulators in the sector.

With regards to liability for offshore accidents and their consequences, the OSD channels it unequivocally to offshore licensees, i.e. the individual or joint holders of authorisations for oil/gas prospection, exploration, and/or production operations

[32]Directive 2013/30/EU of the European Parliament and the Council of 12 June 2013 on the safety of offshore oil and gas operations and amending Directive 2004/35/EC, OJ L 178 of 28.6.2013, p. 66.

[33]Council Decision of 17 December 2012 on the accession of the European Union to the Protocol for the Protection of the Mediterranean Sea against pollution resulting from exploration and exploitation of the continental shelf and the seabed and its subsoil (2013/5/EU).

issued under the Directive 94/22/EC.[34] It also makes the licensees strictly liable for any environmental damage resulting from their operations.

Nevertheless, the OSD does not aim to harmonise the liability rules in the EU for other forms of damage and loss that may result from offshore operations, reflecting the inconclusive results of the corresponding analyses in the impact assessment during the OSD's preparatory stages. This situation is likely to change with the implementation of the OSD. Articles 4(1) to 4(3) of the OSD put in place exposure-based financial security requirements, obliging Member States to take due account of license applicants' 'financial capabilities, including any financial security, to cover liabilities potentially deriving from the offshore oil and gas operations in question.' In addition, Article 4(3) of the OSD also requires Member States to 'facilitate the deployment of sustainable financial instruments and other arrangements to assist applicants for licences in demonstrating their financial capacity.' Several steps could be taken here, including broadening the forms of coverage accepted by national authorities. The provisions in the OSD are further echoed by Offshore Protocol of the Barcelona Convention, which has recently become a part of the EU acquis.[35] This Protocol stipulates in its Article 27(2)(b) that Parties shall ensure that operators have and maintain insurance cover or other financial security for damages caused by activities covered by the Protocol.

The experience of the ELD shows that a competitive market for financial security instruments—pools, insurance, bonds, guarantees etc.—can develop following a significant EU regulatory change, albeit with a time lag to allow for market players to adjust to the new requirements.[36] The availability and uptake of financial security instruments for offshore accident risk can therefore be expected to improve in the years following the implementation of the OSD in national law.

Although financial security instruments to cover all damage from the most infrequent and costly offshore accidents are not readily available from the insurance market, the market appears to have the depth and innovation necessary to cater to all oil and gas companies operating under the current liability obligations. Furthermore, the market for financial security instruments can be expected to adapt to new requirements introduced by Article 4 of the OSD, particularly if national authorities broaden the forms of financial instrument coverage they accept. The decision on whether to accept or require membership of a mutual insurance scheme like OPOL for offshore licensing was best left to Member States as it is closely linked to their national liability regimes, the characteristics of the scheme in question, the licensees in their waters and the risks faced by these licensees. The significant regional

[34]Directive 94/22/EC of the European Parliament and of the Council of 30 May 1994 on the conditions for granting and using authorizations for the prospection, exploration and production of hydrocarbons, OJ L 164 of 30.6.1994, p. 3.

[35]Council Decision of 17 December 2012, *supra* note 55 at p. 13.

[36]Report from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions under Article 14(2) of Directive 2004/35/CE on the environmental liability with regard to the prevention and remedying of environmental damage, 12/10/2010, COM(2010) 581 final.

differences in offshore operations within the EEA—and therefore the kinds and levels of risk faced by operators—could lead to an unjustified cross-subsidisation of risk between these regions and potential moral hazard in case of a one-size-fits-all solution.

In the US, the Oil Pollution Act 1990 (OPA 90), 33 U.S.C. § 2702(a), imposed strict liability for 'removal costs and damages' on the 'responsible party'. The U.S. Coast Guard designated B.P. as the 'responsible party' for the oil and gas flowing from the subsea well and Transocean as the 'responsible party' for any pollution caused by the Deepwater Horizon itself on or above the surface of the water.

Internationally wide one of the most significant step taken was the establishment of a requirement for a Safety and Environmental Management System (SEM). Implementation of Safety and Environmental Management Systems (SEMs) begun in November 2011 as a proactive, goal-oriented risk management system similar in many ways to the systems used in the North Sea by the United Kingdom and Norway and on the outer continental shelves of Canada and Australia, requiring companies to develop, implement, and manage a safety and environmental management system in accordance with the American Petroleum Institute's (API's) Recommended Practice 75 for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities. SEMs were prior voluntary but now are compulsory and required to adhere to objectives such as focusing attention on human error on incidents; improving safety and environmental records continuously; encouraging the use of performance-based operating practices; collaborating with the industry to promote the interests of offshore-worker safety and environmental protection.[37]

6 Cybersecurity Implications for the Energy Sector

As the energy sector seeks to improve its efficiency and reliability, infrastructure operators must be aware that the increased use of the internet of things also increases vulnerability to cyber attacks across the energy value chain.

Cyber risk must not be considered purely as an IT risk but it should be addressed as an enterprise-wide concern and as a key operational risk that requires effective and comprehensive risk management, including governance and oversight from the board of directors and executive team. The energy sector must take a systemic approach and assess cyber risks across the entire energy supply chain, to improve the protection of energy systems and limit any possible domino effects that might be caused by a failure in one area of the value chain.

Nevertheless, measures that require supply chain compliance or cross-border cooperation are more difficult to implement and require increased cooperation across

[37]Nordquist and Fausser (2014), pp. 133–139.

sectors. Companies should implement measures to prevent, detect and respond to cyber threats. Better information from the energy industry will help the insurance industry improve its coverage of energy assets. Still, energy companies also need to identify more clearly where insurance is most needed to fill the protection gap, and they must work with underwriters to further develop cyber insurance products.

Cyber insurance is one mechanism to help offset the potential financial impacts of a cyber attack. Demand for this type of product in the energy sector, especially utilities, has grown rapidly in the USA over the past years, and is picking up throughout other regions, especially in Europe. Indeed, the UK and US governments among others are encouraging large and small companies alike to increase their cyber insurance coverage to effectively boost their overall resilience to cyber attacks. Insurers should continue to develop appropriate cyber insurance products and learn how their existing portfolios are impacted by cyber incidents.[38]

7 Writing Cyber Liability Insurance Coverage

As the potential for loss from cyber risk is increasing, it is not surprising that the market for cyber liability insurance is expected to have an exponential growth, not least because business learn, often the hard way, that the traditional insurance policies they have in place do not adequately cover for cyber risks. Cyber liability policies are by their nature unique and may include one or more types of coverage such as: (a) liability for security or privacy breaches, including loss of confidential information by allowing or failing to prevent unauthorised access to computer systems; (b) the costs associated with a privacy breach (such as, e.g. consumer notification and support post such a breach); (c) the costs associated with restoring business assets stored electronically; (d) business interruption and consequential losses related to a security or privacy breach; (e) expenses related to cyber extortion and cyber terrorism; (f) losses or corruption of data; (g) liability because of breach of privacy from theft of data, or transmission of a computer virus, or failure of network security or rendering of internet professional services; (h) D&O management liability costs; (i) crisis management costs.[39]

[38] World Energy Council (2016).

[39] Cope and Reynolds (2015), pp. 86–89.

8 Conclusions

The insurance industry itself has been criticised as failing to keep up with changes in the legal and regulatory environment post the BP Oil Spill and the Saudi Aramco incidents. The Director of Performance Management at Lloyd's has noted that the environment has become more onerous.[40]

A review of the energy class in the Lloyd's market revealed concerns about the way in which risks were assessed and priced and the way in which exposures has been managed. In effect, what has been noticed is a material imbalance between premiums charged and exposures assumed. A major problem with the insurance of such risks is the discrepancy between the large amounts of capital needed to underwrite and the modest returns generated. Similarly, the size of claims from individual events such as the BP oil spill dwarf the premiums received. Moreover, there is a structural issue in the sense that package policies lack the transparency necessary to reveal energy sector risks and aggregations of risk are difficult to assess and manage.[41] It is not unreasonable to foresee that the market for insuring pollution risks will 'dry out' completely.

A potential solution for confronting the risk of having an insurance market completely unwilling to insure pollution risks, would be to seek government support for an industry initiative which would entail the insurance industry as well as operators and contractors to act together in their common interest. Such a solution would have the overall aim to let governments take the measure of the problem and step in to provide legal stability so that a viable allocation of liability can emerge and insurance markets can adapt. Any apportionment of liability would, however, have to consider who is best able to pay for the risk.[42]

The attention paid by the global community to the potential for damage resulting from oil and rig installations is, of course, partially, but not solely, the result of the 'hype' after the Deep Water Horizon ("DWH") accident in 2010 and the Saudi Aramco incident in 2012.

Notwithstanding the above suggestions, the question, which arises, is to what extent the risk of an oil production related accident (offshore or not) such as the DWH oil spill or any oil production related accident (offshore or not) owed to an even such as the cyber attack in Saudi Aramco in 2012, also exists for future operations in oil and gas and the assessment of the ways in which such insurance risks could be better addressed.

---

[40]CIR, 'Lloyd's: Offshore energy underwriting 'out of step" (21 September 2011) accessed 14 June 2018 at http://www.cirmagazine.com/cir/lloyds-offshore-energy-underwriting-out-of-step.php; 'Bolt criticises energy underwriters' (22 September 2011*) Insurance Insight*.

[41]In a letter to all CEOs and active underwriters dated 29 July 2011 Mr Bolt stated that it is 'a requirement for 2012 plan approval that all Energy Liabilities written at Lloyd's are underwritten in stand-alone policies; compliance with this requirement is a precondition of Lloyd's approval of Syndicate Business Plans for Energy Liability.'

[42]Cameron (2012), pp. 209–210.

However, long before that question were to be posed and answered, prevention mechanisms should be in place and are of major importance. Safety regulation by public and private actors is an important issue to ensure the safe functioning of offshore facilities and to prevent potential accidents. Operators therefore will have strong incentives to invest in safety to prevent such risks from similar accidents from happening. Liability rules also have an important influence on the potential risks to which the offshore facilities are exposed; therefore, insurance coverage will subsequently also be influenced and affected.

One approach to better respond to a future risk oil and gas pollution or cyber risk equal or bigger to the ones entailed in the DWH and Saudi Aramco accidents, is to try and alleviate any involved risk by making the insurance scheme mandatory. It has been suggested that making the use of insurance mandatory in place of any financial responsibility requirement (such as for example that available under the US Oil Pollution Act of 1990 (OPA)), would mean that the coverage of the existing insurance market of around US $1 billion—at least as far as the offshore liability is concerned—would have to be raised to provide a substantially higher amount of coverage. However, such an option would constitute a major challenge to the insurance market.[43] It is unlikely that the commercial insurance market would be able and willing to provide amounts of coverage of such risks higher than the amounts already available today. In fact, post the DWH and the Saudi Aramco incidents the available amounts of coverage have even reduced instead of having increased.

For Europe, a similar facility could be developed as well, but stakeholders would—without a regulatory duty to participate in it—undoubtedly have the same reservations. One should note here that full insurance coverage probably will never be available as insurance can never provide full coverage for all liability, as, first of all, there are risks which are simply uninsurable (e.g. damage which is intentionally caused); and secondly because insurance coverage will be more limited than liability, as it is limited to sudden and accidental incidents and based on particular exclusions which exist to avoid entrepreneurial risks and to reduce the risk of accumulation, which in its turn entails that any insurance coverage provided by the insurance market will necessarily not be the same as full coverage for all potential liability.

Following the DWH and Saudi Aramco accidents, the London market has been adapted to have casualty offerings for the energy market including follow-form excess liability limits available up to $50mn, with catastrophic, high excess limits available of up to $150mn.[44] However, because there are no easy solutions, it is essential that policy makers refrain from mandating pooling between operators of oil and rig installations but, instead, solicit for the creation of industry-wide pooling by providing high standards of safety regulation to enhance safety regulation that in turn

[43]Faure and Wang (2016), pp. 236–265.

[44]Sutherland (2015).

could facilitate and assist mutual monitoring by operators and encourage pooling arrangements.[45]

Because oil pollution damage can occur from of an offshore oil expropriation incident or because of cybersecurity attacks in oil and gas companies' headquarters—as the experience of both the DWH and Saudi Aramco incidents have taught us—hence, also oil spill related costs can accrue. The jump in such oil spill-related costs is a reminder of how difficult it can be for a company to draw a line. It is also a stark reminder of (a) how difficult it is to anticipate the actual losses occurred during oil pollution and other general or cyber-related liability incidents from either offshore oil and gas operations or cybersecurity incidents as well as (b) of the intricacies of placing caps in such liabilities. Not least, post the DWH and Saudi Aramco incidents, insurers have tended to add crisis management services to their environmental insurance solutions. Regulators have also appeared as stepping up their enforcement of environmental and other laws. Although environmental incidents are unlikely to occur if companies are proactive in implementing proper risk management and health & safety procedures, nevertheless as the experience of the DWH and the Saudi Aramco incidents have shown, when they do, they are expensive to put right. Hence the role of insurance and of adequate coverage is utterly important. Possible recommendations for future steps could include the introduction and collection of data on damages resulting from such incidents to help better address insurance coverage needs. Another solution could be the promulgation of the idea of the creation of an international organisation to monitor safety standards, and, hence, also help streamline the operation of the natural resources industry and the smooth functioning of the insurance industry. In effect, all affected interests would benefit from more uniform dealing with consideration of risk in operations globally. Moreover, an internationally agreed risk, upon determination of an "acceptable" level of such a risk would allow commensurate levels of safety to be sought in a wide variety of environmental and technological circumstances and conditions. The establishment of an international standard could identify a safety goal of all elements of the drilling industry to meet rather than being lulled into the complacency that often results from purely prescriptive approaches. This makes more imperative the need to also streamline the insurance coverage offered and calls for an effort to establish a stable "soft" insurance market. Indeed, business leaders who have security as part of their overall business strategy discussion are better positioned to balance the technologies, processes and resources needed to anticipate constantly evolving cyber risks. But in the energy, utilities, mining and industry (EUMI) sectors, the focus should not just be on corporate IT systems as there are just as significant security threats to operational technology. A cyber attack on an operational technology environment can have serious and wide-ranging consequences beyond just financial losses, including prolonged outages of critical services, environmental damage and even the loss of human life. There are highly skilled and motivated adversaries actively seeking to exploit the security weaknesses

[45]Sutherland (2015).

in operational technology networks, process control systems and critical infrastructure. Their motivations range from economic benefit and espionage through to malicious disruption and destruction. While many operators in these sectors have recognised the need to increase focus and spending on the security of their corporate IT systems, this has not been matched for operational technology systems, leading to critical vulnerabilities.[46] Businesses with operational technology networks need to be in a position to assess, identify and rectify cybersecurity vulnerabilities if they are to prevent malicious attacks that exploit these vulnerabilities. Maintaining a secure and resilient operational technology environment requires a comprehensive strategy that covers security governance and process, implementation of the right technology and employing people with the right skills. Relevant and adequate skills are another key element to maintaining secure operational technology networks. Investment in the right technology is another key characteristic of a resilient operational technology network. This makes more imperative the need to also streamline the insurance coverage offered and calls for an effort to establish a stable and "soft" insurance market.

References

Cameron P (2012) Liability for catastrophic risk in the oil and gas industry. IELR 6:207–219

Cope C, Reynolds I (2015) "Breaking Bad" in cyber space: a challenge for the insurance industry. New Appleman on Insurance, Current Critical Issues in Insurance Law, Spring, pp 85–102

Deepwater Horizon Unified Command, U.S. scientific team draws on new data, multiple scientific methodologies to reach updated estimate of oil flows from BP's well, June 15, 2010. http://www.deepwaterhorizonresponse.com/go/doc/2931/661583

Department of Energy and Climate Change, 'Offshore oil and gas in the UK: an independent review of the regulatory regime' (December 2011, U.K.). https://www.gov.uk/government/publications/offshore-oil-and-gas-in-the-uk-independent-review-of-the-regulatory-regime

Dynes S, Goetz E, Freeman M (2008) Cyber-security: are economic incentives adequate? In: Goetz E, Shenoi S (eds) IFIP international federation for information processing, volume 253, critical infrastructure protection. Springer, Boston, pp 15–27

Faure M, Wang H (2016) The use of financial market instruments to cover liability following a major offshore accident. In: Faure M (ed) Civil liability and financial security for offshore oil and gas activities. CUP, pp 236–265

Focus Magazine (2010) Macondo: assessing the implications, oil and energy trends. Focus Magazine 35:3–6

Gauci GM (1999) Protection of the marine environment through the international ship-source oil pollution compensation regimes. Rev Eur Community Int Environ Law 8(1):29–36

International Maritime Organisation (1996) Civil liability for oil pollution damage: texts of conventions on liability and compensation for oil pollution damage. IMO, London

Jacobsson M (2007) The international oil pollution compensation funds and the international regime of compensation for oil pollution damage. In: Basedow J, Magnus U, Wolfrum R (eds) Pollution of the sea – prevention and compensation, Hamburg studies on maritime affairs,

[46] https://www.pwc.com.au/publications/cyber-savvy-securing-operational-technology-assets.html.

vol 10. Springer, Berlin, Heidelberg, New York, pp 138–150. https://www.state.gov/documents/organization/282224.pdf
Kellner LB et al (2010) Insurance coverage issues for third-party businesses and municipalities with losses due to the oil rig explosion in the Gulf of Mexico, Insurance Coverage Alert, Dickstein Shapiro LLP, May 2010
King RO (2010) Deepwater horizon oil spill disaster: risk, recovery, and insurance implications, Congressional Research Service, 7-5700, www.crs.gov, R41320, July 12, 2010, p 3
Kotula M, Insurance, pollution exclusions, and the DWH Gulf of Mexico oil spill. http://www.lexisnexis.com/Community/emergingissues/blogs/gulf_oil_spill.aspx
Little (1998) The hazardous and noxious substances convention: a new horizon in the regulation of marine pollution. LMCLQ 4:554–567
Little G, Hamilton J (1997) Compensation for catastrophic oil spills: a trans-Atlantic comparison. LMCLQ 4:554–557
Mason M (2002) Transnational compensation for oil pollution damage: examining changing spatialities of environmental liability, LSE Research Papers in Environmental and Spatial Analysis (RPESA), no. 69. Department of Geography and Environment, London School of Economics and Political Science, London
Nordquist M, Fausser A (2014) Offshore drilling in the outer continental shelf: international best practices and safety standards in the wake of the DWH explosion and oil spill. In: Lodge M, Nordquist M (eds) Peaceful order in the world's oceans. Brill
Noussia K (2011) The BP oil spill – environmental pollution liability and other legal ramifications. Eur Energy Environ Law Rev 20(3):98–101
Office of the Coordinator for Cyber Issues, Recommendations to the President on Protecting American Cyber Interests through International Engagement, 31/5/2018. https://www.state.gov/documents/organization/282224.pdf
Pagliery J (2015) The inside story of the biggest hack in history, CNN Business, 8/5/2015. https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html
Sandvik B, Suikkari S (1997) Harm and reparation in international treaty regimes: an overview. In: Wetterstein P (ed) Harm to the environment: the right to compensation and the assessment of damages. Clarendon Press, Oxford, pp 57–71
Staff Reporter, 'Lloyd's: offshore energy underwriting 'out of step". http://www.cirmagazine.com/cir/lloyds-offshore-energy-underwriting-out-of-step.php
Sutherland S (2015) Paying for pollution? AIG - Insider Quarterly's Winter 2015 Issue. https://www.pwc.com.au/publications/cyber-savvy-securing-operational-technology-assets.html
Wetterstein (1994) Trends in maritime environmental impairment liability. LMCLQ 2:230–247
Winter A (2010) USGS director quietly wages fearless war on oil spill. The New York Times, June 16, 2010. http://www.nytimes.com/gwire/2010/06/16/16greenwire-usgs-director-quietly-wages-fearless-war-on-oi-83792.html
World Energy Council (2016) World energy perspectives, the road to resilience: managing cyber risk (Used by permission of the World Energy Council. www.worldenergy.org)
Wren (1999) The hazardous and noxious substances convention. In: Nordquist MH, Moore JN (eds) Current maritime issues and the international maritime organisation. Kluwer Law International, The Hague, pp 335–349
Wu (2001) Liability and compensation for bunker pollution. Thomas Miller P&I Ltd., New Jersey

Part IV
Autonomous Vehicles and Transportation

Autonomous Vehicles: Legal Considerations and Dilemmas

Kyriaki Noussia

1 Introduction

As humans are replaced by reliable software that neither drinks alcohol, suffers from stress, nor ignores traffic regulations, accidents are forecasted to have been reduced by 90% by the time that mass circulation of autonomous vehicles will be allowed in public roads, while at the same time a new driving/to be transported population (e.g. children, the elderly, and the disabled) will emerge. Such vehicles will either be autonomous vehicles owned by their passengers or interconnected autonomous vehicles, i.e. autonomous vehicles which will be used via certain sharing platforms (e.g. Uber) to carry the population from destination A to B. Depending on the level of automation, such driving population may be drivers as well, i.e. able to intervene if needed or just passengers, i.e. either not able to intervene or not needing to do so.

The greater safety and reliability of interconnected autonomous vehicles sharing important information immediately will lead to shorter safety distances between cars.

However, even in a world where all vehicles are autonomous, the risk of accidents will not be zero and the damages that may be caused pose important legal questions that have yet to be answered.

Whether be it interconnected autonomous vehicles or autonomous vehicles, such vehicles will need to be programmed to respond to situations of necessity and have a "moral exception" capability, via algorithms regulating emergency situations and encompassing patterns of behaviour, such as when the necessity of safeguarding a specific interest unavoidably demands another to be injured.

K. Noussia (✉)
Law School, University of Exeter, Exeter, UK
e-mail: k.noussia@exeter.ac.uk

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_12

Notwithstanding the above remarks, what the aim should be is to prevent the legal system from accepting the legitimacy of fatal outcomes, for no life is worth less than any other, be it a young or elderly person.

It is argued that in relation to autonomous vehicles, emergency algorithms are being set up to promote the interests of the passenger in the driverless car. However, the aim of regulating conflicts involving several people based on the sole benefit of individual interests of a person is something that, at least from a normative perspective, remains unacceptable. Hence, there has to be legislative regulation to control the direction of crash algorithms.

The fundamental problem to be tackled here is how to provide clear guidelines to car programmers on conflict resolution, i.e. how to determine a 'standard of behaviour' for the car and not necessarily to assess the legal liability when the autonomous vehicle deviates from the regulatory standard.

Programming crash algorithms of autonomous vehicles poses an ethical and legal challenge that is paramount. There are many issues and parameters to consider. First, there is the difficulty of addressing the behaviour of such vehicles, namely also robots in their function, as robots agents, rather than simple instruments of human interaction, because ultimately humans will have to use those "robots", i.e. the programmed autonomous vehicles under a legal relationship of agency as they (autonomous vehicles robots) will perform complex cognitive tasks, such as driving themselves whilst avoiding other cars.

Furthermore, it follows from the above that the fact that a human may let the car drive by itself, does not mean that the legal effects of the decisions of that car should necessarily fall upon the human as joint and several liability might be attributed to several parties (designers, manufacturers, dealers and users of autonomous vehicles).

Not least, as far as the protection of third parties is concerned in the case of autonomous vehicles, there are both issues of contractual and extra-contractual/tortious liability to consider. In the case of autonomous vehicles acting as robots chauffeurs, humans effectively grant autonomous vehicles the necessary authority to autonomously drive themselves and there is the potential of anyone being affected by the reckless behaviour of the self-driven autonomous vehicles. From the point of view of contract law, such autonomous vehicles will in effect accept offers, or make contracts, to autonomously drive individuals, and the personal accountability of self-driven robot autonomous vehicles, would guarantee that obligations for damages, caused by such self-driven robot autonomous vehicles, would be met.

However, there are many issues to consider here. For example, such self-driven robot autonomous vehicles, acting as intermediates in social life, would be offering services to third parties not directly concerned by the enforcement of rights and obligations created by the self-driven autonomous vehicles robots' business.

Indeed, liability would have to be attributed in the form of liability of individuals for unlawful or accidental damages caused to others, because of their personal fault. Other forms of liability would also have to be considered, such as strict liability or liability for the negligent control of artificial agents and even vicarious responsibility for the autonomous acts of individuals' artificial intelligence (AI) employees.

2 Distribution of Liability

2.1 Civil Liability, Negligence and Product Liability

Negligence is a type of tort based on a defendant's conduct; the four requirements to establish liability are well known: i.e. that all road users owe fellow users a duty of care and will be liable if breach of that duty causes damage. There is no strict liability for road accidents but the courts have insisted on a high level of care: an inexperienced driver is measured by the standard of the experienced driver, and must take his victim as he finds him and anticipate potential carelessness on the part of others.

In a semi-autonomous vehicle context like the present one we are experiencing, it may not be clear whether it was driver error or software failure that is responsible for an accident. This is made more complex because the shared responsibility between driver and computer over different aspects of the operation of the vehicle may well vary between manufacturers, vehicle types, and road environments or conditions.

English tort law is concerned with any product, including a car, that is dangerous and injures a person or damages property, with liability based on the foreseeability of damage to members of the public through defective manufacturing. It applies to car manufacturers but also to those further down the sales channel; for example, resellers that do not follow manufacturer instructions. Any of the following that suffer personal injury or damage to property can bring a claim: buyer, hirer, passenger or bystander. They can claim for physical damage (other than for the defective product itself) but not financial loss, even if the complaint is based on a failure to provide a warning rather than for a defect.

The duty of the manufacturer is, of course, only to do what is reasonable, rather than to guard against every risk, however small. However, in a semi-autonomous vehicle context, it may be challenging to determine whether the duty of care to do what is reasonable in the circumstances has been satisfied. As the technology evolves, it may not be clear whether instructions have been followed and whether there is sufficient evidence of defectiveness versus a failure on the part of the driver.[1]

2.2 Autonomous Vehicles and Liability

Autonomous vehicles are complex industrial products subject to very specific regulations providing for compliance to technical standards. The applicable regulation in the European Union is the EU Machinery Directive. Cars are also products, and as such, are regulated by the EU Product Liability Directive.

Manufacturers have a strict liability for the products they put on the market. This means that the producer is liable for personal injury and property damage caused by a defect in the product, without the necessity for the claimant to demonstrate a fault.

[1] Syed (2017), pp. 12–13.

Development risk and contributory fault by the user of the product may be used for defence.

Distributing proportionate responsibility between the parties responsible for designing and manufacturing the various parts of the vehicle (software, sensors, actuators), maintenance and safety contractors, traffic operators or internet services interacting with the vehicle, might prove difficult.

This gets even more complex when we are dealing with autonomous vehicles as such cars could in the future be adaptive through machine learning abilities, a feature that will certainly involve unpredictability in behaviour. In this respect, the fully autonomous vehicle will also be a self-learning vehicle that will transcend the traditional legal status of a car and will become an artefact that has the possibility to move freely with the capacity to act and decide beyond the control of humans. So far, autonomy is limited to deterministic processes. However, even in the case of future full automation in all cases where a human is in the loop, responsibility will be distributed between the operator of the car and the manufacturer. The operator must be able to take over control from the car if required and could be deemed responsible in case of misjudgment of the situation by human or by car. Hence, the interface between human and machine must be clear and that operators will have to be trained about the functions of the vehicle to understand when they must take control of the car. The responsibility for damages occurring in full automation mode and not attributable to a machine defect is still an area to be investigated by the law. Setting standards for autonomous vehicles behaviour and their care will prove difficult, at least in the near future. Setting a full responsibility for manufacturers could also be considered by extending existing rules on product liability. This could however cripple commercial deployment of autonomous cars and thus limit their potential benefits to society or make their use difficult as insurance premiums may skyrocket and be non-affordable.[2]

In relation to insurance and liability, the mass market adoption of autonomous vehicles will depend on the cost of ownership as well as the availability and cost of insurance as insurers will need to price new insurance products with premiums initially calculated with little empirical data. Given that the product liability component will be recovered from manufacturers, they may need to co-develop with insurers new products and risk share to help make insurance available and encourage greater adoption of their vehicles. The regulators now explore whether the driver should be required to hold both third-party and product liability insurance. Then, the injured party could recover efficiently and the driver's insurer could later seek to recover from the manufacturer. However, other than the question of who has to hold which types of insurance and the amount needed, there should be no change to the *role* of insurance. If the accident was because of software error, the injured party should be able to claim from the driver (or their insurer), who should seek to recover from the manufacturer (or their insurer). In reality, any other approach would be impractical. It will be important for regulators to ensure a framework where any of

[2]Kermorgant and Siary (2016), p. 93; Langheim (2016).

the parties that suffer personal injury or damage to property can bring a claim and be in no worse position than they are in now.[3]

2.3 Limitations of and Gaps in the Current Legal Framework

The current EU system of appropriation of risks related to motor vehicles generally works well. Based on the review of the Product Liability Directive and Motor Insurance Directive as well as the public consultations carried out by the European Commission, the majority of stakeholders believe that the current EU liability framework provides a working system that ensures an appropriate balance of interests and responsibilities of all parties involved.

The results of the European Commission's 2017 public consultation on the Product Liability Directive indicate that 82.5% of respondents representing organisations believe that the Product Liability Directive provides for a fair balance between the interests of producers and those of the consumers. Private individuals and other respondents seem however to be less confident, as in total only 68% believe that the Directive provides for a fair balance between the interests of producers and those of consumers. Respondents also consider that the, roll-out and in particular the mass penetration of autonomous vehicles into the market would likely have a significant effect on the existing system of appropriation of risks relating to motor vehicles. The current liability system is based on the understanding that there are two main types of risk relating to the operation of motor vehicles: first, the failure of the hardware, i.e. it is the product that triggers product liability, and second, the action of (and/or damage to) a driver, which triggers liability under national traffic laws and is also covered by the Motor Insurance Directive.

Considering the nature of autonomous vehicles as products characterised by increased complexity of hardware and software as well as crucial reliance on connectivity and networks, at least six main risks affecting liability can be identified. The existing risks, i.e. failure of hardware and liability based on personal conduct of a driver will be substantially impacted. This could potentially lead to a shift in risk distribution between for example consumer and producer.

The new risks that would emerge with the rollout of autonomous vehicles are currently not specifically covered by the EU liability framework. Thus, the current set of rules would have to be interpreted in such a way as to account for the 'new risks'. This legal ambiguity could lead to increase in litigation and possible divergent interpretation in various Member States.

Finally, the current rules of evidence, i.e. the rules establishing fault and therefore liability would need to be adjusted, possibly through the introduction of legislation on detection technology, i.e. event data recorders.[4]

[3] Syed (2017), p. 14.

[4] Evas (2018).

2.4 Existing Risks: Shift in Liability

The rollout of autonomous vehicles calls for a fitness check of the current regulatory framework on liability to understand (i) how risks would be allocated among the parties involved and (ii) whether current balance between the parties would be preserved.

The key question is whether the process of digitalisation in the automotive industry, in particularly the rollout and the mass adoption of autonomous vehicles, would affect the current balance between parties in risk appropriation. If rollout of autonomous vehicles would result in liability transfer between the parties, the question is whether and to what extent an adjustment and/or introduction of a new regulation would be necessary.

Autonomous vehicles require special regulatory attention and a review of the current framework not only because of their significant economic and societal value but also because autonomous vehicles are a disruptive technology that have the potential to change what is now our conventional understandings of a product, mobility, ownership and security. In other words, rollout and mass adoption of autonomous vehicles are not another upgrade or improvement of the traditional product of the automotive industry, a vehicle, but rather a qualitatively new product.

This new product is technologically sophisticated with many components, software, hardware and algorithms where, among other things, the line between product and service becomes increasingly blurred.[5]

2.5 Product Liability Directive and Motor Insurance Directive

The Product Liability Directive is generally a fair instrument for balancing the distribution of risks between producers and consumers of products. However, if applied to the mobility system based on autonomous vehicles, existing gaps and limitations could potentially limit the scope and effectiveness of the Product Liability Directive and affect the existing balance between the parties.

The three main groups of issues are the following:

- First, the Product Liability Directive has limited substantive scope and covers only liability of producers for defective products. The concept of 'defectiveness' is narrowly defined and difficult to establish for technically complex products such as autonomous vehicles. As it stands now, damage arising for example from a vehicle's wear and tear, bad repair, the way vehicle has been used, the road situation, or weather conditions will be not covered by the Product Liability Directive. Developers, producers, component makers, importers, distributors, and car-dealers could rely on a number of defences provided by the Product

[5]Evas (2018).

Liability Directive to minimise liability, which in relation to highly technological products, could provide a wide safety net for producers to the disadvantage of consumers.

For this reason, several parties (including rental companies and other service providers, pure developers of the operating technology and testing companies) will not incur risk-based liability for defectiveness, but only fault-based liability. The definition of product also remains an open question, more specifically whether software is a product.

- Second, the cost of scientifically unknown risks will be shouldered by the injured party.
- Third, the high-tech nature of autonomous vehicles combined with the broad provisions of the Product Liability Directive on defences, in particular in relation to the concept of 'reasonableness' may overburden national courts. National courts interpreting and applying the Product Liability Directive to disputes involving autonomous vehicles will be called upon to settle very complex technological issues.

Overall, the application of the Product Liability Directive to autonomous vehicles will provide a certain degree of protection. However, there are a number of legal and factual issues that, if not addressed, could potentially lead to decreased scope of protection and increased costs for consumers as well as increased legal uncertainty for all parties involved. Specifically, these issues include: the limited reach and meaning of product liability, and the limited list of liable persons and evidentiary burdens currently provided under the Product Liability Directive.

Another legal mechanism to claim compensation for damages caused by motor vehicles is to rely on traffic liability rules. Substantive traffic liability rules and levels of compensation fall within the competence of the Member States. National rules are divergent and include fault-based systems, mixed, and strict-liability systems (no fault).

At the EU level, the Motor insurance Directive regulates procedural, adjunct issues relating to motor insurance policy. For example, importantly, it covers the obligation for all EU vehicles to hold third-party liability insurance and establishes the mechanisms for the simplified settlement of claims. Autonomous vehicles will fall under the definition of a vehicle currently included in Article 1 of the Motor insurance Directive and, thus, all damages to persons others than the driver or user, keeper or owner of the vehicle will be covered by mandatory insurance as provided by the Motor insurance Directive, subject to the limitation provided by the Motor insurance Directive.

Currently, the national systems are based on the assumption that the driver is in the control of the operation of the vehicle. In the fault-based systems in particular, the link between fault of the driver and the accident is crucial to establish the right to compensation. The introduction of autonomous vehicles assumes that a human driver will be fully replaced by technology. Therefore, the 'fault' of the driver becomes a notion that needs to be reconsidered and or adjusted accordingly. Adjustment of the risk-based system would be necessary, specifically in relation to

the concept of driver-victim. Overall, if the current framework is not reviewed in the light of special features relating to autonomous vehicles as a product, application of the Product Liability Directive to autonomous vehicles will have a significant negative impact on consumer protection. Thus, while the current system of risk allocation would in principle be able to deal with the introduction of autonomous vehicles, there would be a shift in the current balance between the parties involved.

Application of the current EU liability framework to the rollout and adoption of autonomous vehicles highlights a number of existing gaps and shortcomings that could potentially disturb the current balance in risk allocation. Both industry and consumers need legal clarity on whether the current liability system is to be maintained or regulatory changes are to be introduced.[6]

3 Ethical Considerations: An Overview

Whilst the impact of autonomous vehicles technologies is set to be positive by and large, a number of ethical implications must be addressed, the most significant being the question of whose safety the autonomous vehicle will be programmed to protect in the event of an accident and the way in which such scenarios would have to be dealt with in advance through the programming of certain accident prevention and handling algorithms accordingly. If the case may be whose life to save, that of the autonomous vehicle passenger or of the pedestrian/other vehicle user, intuition tells us we should save the most number of lives.

What other qualitative considerations should be taken into account? Under what criteria should they be classified and prioritised? In other words, should a person abiding by the law be preferred over someone acting against it? Should young be prioritised over the elderly or disabled?

One view is that harm should be directed towards the occupants of the autonomous vehicle, given that they are responsible for introducing a machine of potential danger to the public roads.

Manufacturers such as Mercedes Benz have proclaimed that their cars will prioritise the lives of the people inside the car. How will this affect the insurance and insurability of such vehicles? Such issues remain to be resolved in a socially ethical way and one way of tackling such a challenge could be to impose the need to have ethical algorithms consistent among different manufacturers to ensure predictably and equality for the consumer users.[7]

[6] Evas (2018).

[7] Jeffcott and Inglis (2017), pp. 19–25.

4 Cyber Security and Big Data Issues

Communication of data constitutes a threat for human security, as all security issues triggered by the internet would also exist in the case of vehicle communication. No matter how secured and robust the system might be, data exchange can never be trusted to be perfectly secure; therefore, even the most powerful cyber-encryption scheme would fail to protect, should an attacker alter the physical measurements and therefore the input to the encryption scheme.

Privacy is likely to be jeopardised by the images and data captured by various vehicles, even if the exact nature and quality of data that will be collected is yet unknown. Personal data protection and processing is provided for by the GDPR and autonomous vehicles should be compliant with rules. Car manufacturers argue that to avert/circumvent prejudicial treatment of the right to privacy, data will be deleted after a relatively short time lapse. Nevertheless, since vehicles will communicate with each other and infrastructure beacons, the question may be asked, how can it be ascertained that the data will actually be erased. It is acknowledged that legal restrictions may be imposed on the right to privacy if these restrictions genuinely meet objectives of general interest and that the collection of information is proportionate with its intended use and limited to that. Safety and responsibility monitoring will require that data is recorded and that it is accessible to third parties such as insurance companies or courts. The proper balance with privacy could be anonymisation of all data processed by the car. Car manufacturers will have to devise a standard harmonised documentation clearly informing users of the interconnected anonymisation about what/which data will be collected, for what purpose, the way it will be processed and shared, when and how it will be deleted and enabling recording of consent from users. Another challenge is posed by the fact that most Cloud providers are based in the USA, hence one need understand whether the law and practice of the United States offer an adequate protection to European citizens' personal data protection. In addition, the right for third parties to access to real time data, event data recorder information will require specific regulation as we can imagine how tempting it could be for insurers or public authorities to use this data to monitor speed limit infractions, to develop better insurance policies or to sell various products or services.[8]

Recital 50 of the GDPR states that if the processing is compatible with the purposes for which personal data were initially collected, no legal basis separate from that which allowed the collection of the personal data is required. This constitutes a considerable shift from the general rule that processing of personal data is prohibited unless covered by existing permissions. The issue to consider is whether this change in the law is associated with considerable disadvantages for the data subject, and whether it significantly facilitates processing activities on the side of the data controller. Taking a closer look at the new provision on the compatibility assessment in Article 6 (4) of the GDPR it appears that the interests of the data

[8]Kermorgant and Siary (2016), pp. 93–97; Langheim (2016).

controller to further process the data and interests of the data subject shall be balanced. This is also reflected in Article 6 (1) (e) GDPR, which provides that processing of personal data shall be lawful if processing is necessary for the purposes of the legitimate interest of the controller or of a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. Article 9 (2) of the GDPR, which concerns special categories of personal data, such as health data or genetic data, provides specific legal grounds for processing such personal data, generally stricter than those in Article 6 (1) GDPR and factors such as the nature of the data needs to be considered, as well as the possible consequences for the data subject. Nevertheless, one cannot deny that there is a danger of misuse by the data controllers through overemphasising their own interests.[9]

The GDPR retains the purpose limitation principle as one of its basic elements. Consequently, data controllers will, in the future, have to specify the purpose of the collection, which must be clearly and specifically identified. Further processing of personal data under the GDPR will also need to be compatible with the original purpose for which the data was collected. Personal data should not be kept in a form that permits identification of data subjects any longer than the purpose of the collection or reuse.

The legal situation for data controllers wishing to process personal data in Big Data applications has not significantly changed. It will remain a core issue how to specify the purpose of the collection and further use of the personal data before, or at least no later than, the time of collection. Involved stakeholders should work together in addressing the challenges and highlight privacy as a core value and a necessity of Big Data. Technology should be used as a support tool to achieve this aim.[10]

4.1 Fair and Lawful Processing

Personal data may only be processed 'fairly and lawfully'. Processing personal data is only considered fair when this is done in a transparent way for the data subject, which means that the persons concerned must be aware of the processing. The GDPR provides limitative criteria to determine the lawfulness of data processing.

Personal data may only be collected for specified, explicit and legitimate purposes. This implies that before processing takes place, the purposes must have been determined, and brought to the knowledge of data subjects. Any processing beyond the original purposes is illicit.

[9]Forgo et al. (2017), pp. 37–38; Corrales et al. (2017).

[10]Forgo et al. (2017), pp. 37–38; Corrales et al. (2017).

The GDPR requires that when personal data are processed using new technologies, while there is a high risk for the rights and freedoms of individuals, a data protection impact assessment must be carried out before processing takes place.

Thus, connected autonomous vehicles tracing technology must be aimed at processing as little personal data as possible and privacy settings should avoid collection and processing of personal data by default as much as possible.

Data subjects have the right to access the personal data processed that relate to them, in an intelligible form, also regarding the sources from which data are obtained.

The GDPR institutes, from a consumer protection perspective, a fair system for appointing liability to controllers and processors who infringe its provisions. For example, the connected autonomous vehicles producer who collects and stores personal data through tracing technology for the improvement of 'his own' connected autonomous vehicle driving technology, and who does not obey the GDPR, will be liable for compensating damage resulting from a data breach. The same producer however, cannot be held liable when he has provided just the same—unsafe—tracing technology, where he neither determines the means and purposes for data processing nor processes under the responsibility of a controller. When for example the consumer himself decides to share certain personal data with others using tracing technology, the producer of the technology cannot be held liable under the GDPR, as long as he is not an actor in the data processing chain.

The Product Liability Directive provides that a producer can be held liable when a defective product he has put into circulation causes damage to persons or goods. It may thus be that the connected autonomous vehicle producer, who marketed tracing technology that lacks the level of information safety the public may reasonably expect, could be liable for the resulting damage. However, the damage resulting from unsafe tracing technology does not consist of personal injury or death or damage 'intended and/or used for private consumption' by the injured person, will not have to be compensated by the producer. Thus, a significant portion of potential damage resulting from the abuse of vulnerabilities in connected autonomous vehicle tracing technology is not covered within the EU regulatory framework on liability and data protection to date.[11]

5 Insurance Issues

The EU Motor Insurance Directive 2009/103 provides for mandatory insurance for the use of a car. Car insurance is based on human driver capability and this well-established logic is becoming problematic in respect of autonomous cars as the risk is transferred to the machine.

[11] Evas (2018).

Because of this risk transfer, liability will increase for manufacturers, who will have to provide for further insurance coverage in this respect. It is said that autonomous driving will lead to less car accidents. Insurance companies need to consider this evolution.

Though insurers will require to know and understand the user habits or behaviours less than what was needed beforehand, doubtlessly they will want to know more precisely the various types and models of technology embedded in the car (and above all the duration required to take control of the car), to evaluate the risk and thus to evaluate the financial hazard of such a car.

Insurers will have to perform new statistics on the reliability of driving car by car, technical solution by technical solution. They will (have to) create new databases to offer adequate premiums. This work will involve lots of investment and consequently a premium price reduction will not be on the agenda before years. Risk based responsibility systems already exist for cars but insurance costs are mutualised and actuarial calculations are based on the predictability of traffic accidents which is not compatible (in the near future) with the new levels of risk and unpredictability created by autonomous cars. Insurance companies will request access to data information carried by cars.

Indeed, to deal correctly with liability in case of accident, it will be necessary to obtain data recorded by the car (speed, when the car asked the human to take control of the car, etc.). Hence, it might be necessary to define clear rules for the storage of personal driver data in an event data recorder and to allow the manufacturer and the insurer to analyse this data in case of an accident.[12]

The insurance industry has been at the forefront of the technological advancements experienced by society over the last few decades. With new technologies come new risks, which insurers need to understand to be able to price their policies accordingly.[13]

Currently, the vehicles we drive already hold a wealth of information, either through telematics boxes which are fitted because of pay as you drive style insurance products or through systems built into the vehicles themselves, record data useful to insurers. They can use this data to understand the cause of and the severity of an accident, the location of a stolen vehicle, and some of these technologies even record the number of passengers in the vehicle at the time of an accident and even tell whether seatbelts and other safety measures were correctly deployed.

Insurers do not simply collect data, but use technology to provide better services to their customers and the public at large. They share accident information or provide information to the Motor Insurers' Database that allows the prompt identification of an insurer in the event of an accident, or provides the police with information on the insurance position of vehicles, which in turn allows them to remove uninsured drivers from our roads. They share information with other insurers that helps in the combating of fraud and financial crime.

[12]Kermorgant and Siary (2016), pp. 93–94; Langheim (2016).

[13]Rowe (2018), p. 302.

Hence, the insurance industry is certainly demonstrating its willingness to innovate to create new and novel ways of dealing with claims and to do so it is innovating for various reasons, to provide a competitive advantage, to streamline operations, to reduce costs, and to provide customer facing services.

In the UK the Automated and Electric Vehicles Act 2018 shows that both the government and the industry are thinking about the impact of autonomous vehicles as the latter have the potential to radically change the nature of motor insurance and the claims that they generate.

As computers take over the opportunities for human error abates, however, technological failure may well mean that when an accident does occur, it could be more serious.

The volume of information that will be available to assist insurers and others understand the cause of accidents will be immense and artificial intelligence (AI) has the potential to transform the way in which claims are handled through the application of algorithms to route new claims and to automate decision making processes such that a claim could in theory be settled in minutes, including a full consideration of potential fraud indicators. Connected devices, part of the Internet of Things (IoT), will be able to identify potential risks and report them to insurers as well as bringing them to the attention of the consumer. The whole basis of risk and mitigation of risk will change and some insurers are already responding to it. For example, Aviva have created their Digital Garage, whilst Allianz have created their Digital Factory and other major insurers are creating similar innovation hubs. These organisations are developing the future of insurance and how they utilise connected devices and artificial intelligence (AI) to enhance their customer proposition through the creation of new products and services and creating efficiencies.[14]

Notwithstanding the above considerations and realisations, there are also far reaching legal insurance implications related to self-driven autonomous vehicles. The insurance lobby has affirmed that insurance will be required to cover the cost of any incidents caused by failure in the software and some insurers are already distributing products protecting motorists against claims caused by hacking or software failure of systems.

It is questionable how much protection such insurance will afford and in the case of novel circumstances additional insurance may be of benefit such as the case where a hacked vehicle crashes. In such a case, the injured individual should still be able to bring a case against the motorist's insurance even if the driver and manufacturer are not liable for causing the accident. One possible interpretation entails that, where the driver is "in control" existing insurance covers such a claim, whereas where control has been passed to the vehicle the manufacturer would be liable for a defective product and the harm caused by it and the way for compensation to be achieved through a successful insurance claim would be to have a natural extension of the existing policy for the motor insurer to compensate the innocent third parties.[15]

[14]Rowe (2018), p. 305.

[15]Jeffcott and Inglis (2017), pp. 19–25.

There are also significant data protection issues to consider as a large amount of data is gathered by motor vehicles, i.e. GPS can track the location of a vehicle and Bluetooth can connect the car with a motorist's mobile telephone and to guarantee security and safety, the sharing of data able to allow accident investigators to ascertain liability, should be available. One of the many challenges posed herein is the way in which manufacturers will deal with data susceptible to security breaches.[16] Also, another question that arises involves the criteria based on which the police will have access to data and for what purpose as there is a danger here to end up with a situation where the police are given access to an unprecedented and non-acceptable in amount level of information detrimental to the right to privacy.

5.1 New Risks Relating to Software Failure

The current EU legal framework applicable to motor vehicles is, in principle, able to settle liability and insurance issues. However, the application of the existing rules to autonomous vehicles will likely shift the existing balance in liability distribution between consumers and producers, as well as further accentuate existing gaps and potentially contribute to legal and administrative costs arising from uncertainty.

If the current EU framework is not adjusted, in addition to the existing gaps in the current EU legal framework, the introduction of autonomous vehicles will contribute to the emergence of new gaps and legal grey areas.

This is because the current legal framework was not designed to deal with the liability issues of autonomous vehicles, which are technologically complex and stand distinctly apart from the motor vehicles currently on the roads.

Four main categories of risk relating to the liability issues associated with autonomous vehicles are likely to emerge or become significantly more prominent with the mass rollout and use of the autonomous vehicle. These new risks relating to software failure include:

- risks relating to the failure of the operating software that enables the autonomous vehicles to function;
- risks relating to network failures;
- risks relating to hacking and cybercrime, and
- risks/externalities relating to programming choice.

These four issues are not at all or not sufficiently addressed under the current Product Liability Directive or Motor insurance Directive framework.

[16]Jeffcott and Inglis (2017), pp. 19–25.

Risks Relating to Software Failure

This set of issues concerns situations where damage results from a failure in the autonomous vehicles' operating software. The legal concerns relating to software failure in autonomous vehicles are connected with two main issues: first, when and under what conditions the software producer (rather than the car producer) could bear the cost; and second, under what conditions failure of the software can be considered within the scope of the Product Liability Directive's 'defectiveness' standard.

Under the Product Liability Directive, the legal question as to whether the software is a product is not settled. If the software could be considered a product, then the questions raised would concern:

(a) under what conditions software could be considered 'defective' within the meaning of the Product Liability Directive, and what would be the scope of 'reasonable expectation' and 'development risk' defences; and
(b) against which party the autonomous vehicle user should direct liability claims, i.e. the car producer or the software producer. Under the current Product Liability Directive framework—provided the software is considered a product—the autonomous vehicle driver or operator's right to compensation will depend on the reasons for the software failure. The risks relating to the operating software are covered by the PLD only if those risks could have been scientifically discovered before the autonomous vehicles' rollout from the factory. Risks discovered or emerging after the time of production are not covered. The possible right of compensation under traffic liability rules for damages caused by software failure will depend on national traffic liability laws and, as it stands now, will differ widely among Member States.

Risks Relating to Network Failure

This set of risks relates to the situation where damage occurs because of network failures. Autonomous vehicles will be heavily dependent on the network. Therefore, the central question is who and under what conditions would be liable for autonomous vehicle inability to obtain data or communicate with other traffic participants owing to network problems. Here, besides the autonomous vehicle user and car producer, a network provider could arguably potentially be a liable party.

The attribution of risks for network failure under the Product Liability Directive will ultimately depend on whether the vehicle's network connection is a part of the package offered by the producer. If being connected is part of the package provided by the producer, then the car manufacturer is liable under the Product Liability Directive for network problems, subject to the limitations and defences available under the Product Liability Directive. As in other cases relating to proof of defects under the Product Liability Directive, the reasonable expectation test and other defences are for the courts to apply to decide on the outcome. For the autonomous

vehicles producer to be liable for the software or network failure, it must be proven that the vehicle was already 'defective' at the time it left the production line. This proof of 'defectiveness', under the current Product Liability Directive is already difficult for the standard hardware failures of motor vehicles currently on the roads, but will be even more difficult and uncertain for the software or network failures of autonomous vehicles.

The right to compensation under national traffic liability laws for damages caused by the network failure will again differ greatly among Member States.

Hacking and Cybercrime

Considering the nature of autonomous vehicles, hacking as well as issues relating to data and the protection of privacy, will become significant new risks that are not yet covered by legislation specific to motor vehicles. Similarly to the risks emanating from software and network failures, the autonomous vehicle producer could be liable for the damages resulting from a third party hacking the software of the vehicle if defects in the autonomous vehicle at the time of production could be proven. The technology used by the producer will have to be robust enough to protect the user of the autonomous vehicle against hacking attacks and malware. Product defects would be very difficult to prove. Moreover, it would be even more difficult to attribute liability if all necessary software was installed but cybercrime nevertheless occurred.

The Product Liability Directive seems to provide a very limited and uncertain avenue for compensation claims. General civil liability rules in cases of hacking and other cybercrimes are not harmonised in the EU.

Producers of autonomous vehicles, in their capacity as controllers of personal data, can in principle be held liable under the Data Protection Directive (DPD) and the new General Regulation on Data Protection (GDPR). This is however subject to number of limitations. Producers can be held liable only if they fail to appropriately act to protect data from being hacked or if they infringe other obligations under the DPD or GDPR. However, it is not clear whether and to what extent the producers of autonomous vehicles can be held liable if they are not a controller of a processor of data within the meaning of the DPD or GDPR.

Furthermore, the issue of whether the operator, or owner or keeper of an autonomous vehicle could be held liable for the damage resulting from his or her own failure to install or update software would be determined by national laws, which currently provide varying responses.

Programming Choice

This set of risks concerns liability for programming choices causing damages. The central question here is when and under what conditions the producer of the autonomous vehicle could be held liable for programming choices. Can

programming choice be considered a 'design defect', thus making a car manufacturer liable for a defective product?

Furthermore, how broadly or narrowly should the design risk defence be interpreted by courts as specifically applies to the injuries suffered by third parties because of autonomous vehicle programming choices. The current Product Liability Directive framework is not specifically designed to address those complex legal issues. Under current Product Liability Directive framework, the autonomous vehicle producer would be liable for damages resulting from software, network and programming failures only for product defects that could be attributed to the production process. Malfunctioning of the software or network from 'wear and tear' or malfunctioning of the software or network because of actions by other parties (hacking, bad repair, etc.) and resulting damages caused by the autonomous vehicle are not within the scope of the liability covered by the Product Liability Directive.

To conclude, if not specifically addressed by the legislator, the current Product Liability Directive framework would result in many uncertainties relating to the new groups of risks identified above. While prima facie not totally excluded from the scope of the Product Liability Directive, it would in practice be likely to be extremely difficult if not impossible for these risks to be covered by the Product Liability Directive. The Motor Insurance Directive framework and national traffic laws also present limitations and difficulties for both existing and new risks.

As substantive traffic liability rules are not harmonised at the EU level, there are many national differences, which in fact mean that EU citizens are protected differently in different Member States. Risk-based national systems seem to be better suited to meeting the challenges of the autonomous vehicles, however, they are also limited by a number of considerations, such as for example the scope of compensation for damages caused to property or driver-victim.

6 Conclusions

An interconnected system of vehicle computers and roadside cameras and sensors could create many data pools able to be usefully parsed for insights to help improve traffic management systems and help corroborate other evidence in criminal and civil legal actions.

However, the data will include personally identifiable information generated and/or held by a number of different legal entities, public and private (manufacturers, operators and service providers), and any collection and processing of personal and sensitive data will need to be conducted in accordance with the requirements of overlapping data privacy regimes. Accordingly, that is no reason why such complexity should not be resolvable and the risks addressed as the technologies emerge that collect or generate the personal information.

Whilst insurers and the claims industry may not necessarily be as advanced as some other sectors in the application of technologies, it is clear that technology has

been utilised successfully within the sector where it has provided a clear benefit. Technology will continue to shape the industry, which has welcomed the digital revolution, but needs frame and safeguard the privacy of the assured user of the autonomous vehicles. A welcomes step is the GDPR, however with most Cloud providers are based in the USA, the best legal protection to European citizens' personal data needs to be carefully considered.[17]

The political world has recognised that autonomous vehicles technologies represent an opportunity for new inward investment and provide some risk mitigation for its domestic car industries. Transport regulators deserve credit for being proactive in thinking early and deeply as to how to pragmatically clear the path to achieving vital transport and environmental goals. Traditional industry incumbents that were slow at first are now matching the pioneering efforts of Silicon Valley technologists who took a huge financial and reputational risk to bring us the autonomous vehicles.[18]

In terms of the legal and regulatory frameworks, as we are likely to face a driverless evolution rather than revolution, some problems can be solved by interpretation, some require new law and secondary guidance, but all can be solved.[19]

References

Corrales MM, Fenwick N, Forgo N (eds) (2017) New technology, big data and the law. Springer

Evas T (2018) A common EU approach to liability rules and insurance for connected and autonomous vehicles, European Added Value Assessment. European Parliament, EPRS, PE 6015.635., Feb. 2018

Forgo N, Haenold S, Schuetze B (2017) The principle of purpose limitation and big data. In: Corrales M, Fenwick M, Forgo N (eds) New technology, big data and the law. Springer, pp 17–43

Jeffcott O, Inglis R (2017) Driverless cars: ethical and legal dilemmas. JPI Law 1:19–25

Kermorgant G, Siary O (2016) Is the law ready for autonomous cars? In: Langheim J (ed) Energy consumption and autonomous driving. Springer, pp 89–101

Langheim J (ed) (2016) Energy consumption and autonomous driving. Springer

Rowe K (2018) The rise of the machines: a new risk for claims? JPI Law 4:302–307

Syed N (2017) Regulating autonomous vehicles. CTLR 23(1):11–15

[17]Kermorgant and Siary (2016), pp. 93–97; Langheim (2016).

[18]Syed (2017), p. 15.

[19]Syed (2017), p. 15.

Will Autonomous Cars Put an End to the Traditional Third Party Liability Insurance Coverage?

Viviane Mardirossian

1 Introduction

Mistakes happen all the time, and can be made by everyone because we are all humans. Misfortunes become part of our lives and we learn from our faults every day. However, if on one hand making mistakes can be an apprenticeship, on the other hand, the one that suffers the consequences of that mistake can have the life compromised forever. When it comes to accidents involving motor vehicles, there are hundreds of millions of examples where a simple mistake from the driver has extinguished entire families and there was no way the situation could be undone. Autonomous vehicles entered the market with the promise—even proven by facts—that accidents can be reduced by 90%.[1] Researchers are trying to demonstrate that without the "human" factor, streets would be safer and death rates because of collisions would drop significantly. However, as it will be possible to observe in this study, until today the entire motor liability industry was based on having the figure of the driver to sustain the majority of the consequences of any car accident and, if we gradually extinguish the human factor in the driving activity, one of the most seen theories nowadays, among others, say that there will be a shift of liability from the driver to the vehicle manufacturers or even further, to any other one from

I dedicate this article to my husband Denis, who contributed with his critics and comments, always making me grow as a professional, and to my little Alice who was still kicking inside my belly at the time I wrote it and who will be able to experience this new world of autonomous vehicles as a reality.

[1] Bertoncello and Wee (2015), McKinsey & Company Automotive & Assembly.

V. Mardirossian (✉)
General Reinsurance AG, Rep. Office, Sao Paulo, Brazil
e-mail: viviane.mardirossian@genre.com

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_13

the manufacturers supplier chain. Although it seems very simplistic, there are several implications, including insurance issues on the matter that are not easy to solve, this way we can assume that changes will be likely gradual, since the legislation has yet to adapt itself to support that new environment.

To give an overview of the current system, Sect. 2 of this study was broken down into three sections that will provide as background information some aspects that help the reader to understand how traditional third party liability related to motor vehicles was addressed until now and the important steps taken so far in the vehicle industry that can end up by changing the way insurance companies operate in respect of this particular risk.

As part of the background analysis, Sect. 2.1 presents the concept of "driver" we had to date and how this is intended to change with the evolution of automated and autonomous technology in the vehicle industry, when the figure of the driver that until now was one of the bases for the liability attribution is supposed to disappear. Section 2.2 goes through the evolution of the autonomous technology until the moment and Sect. 2.3 shows examples of countries that are already adapting their legislation to the new world to prepare their legal environment to welcome the autonomous reality.

The discussion on legal implications and impacts on liability can be found in Sect. 3, where the reader will see what has been already said about the topic and solutions proposed by several authors, what can considerably change the way insurance companies operate their motor third party liability product, as it will be presented in Sect. 4. Finally, Sect. 5 provides a general conclusion on the subject, with an overview on possible solutions.

2 Background Information

2.1 Changing the Classic Concept of the "Driver" to Embrace the Autonomous Reality

When the first car was developed by Carl Benz back in 1879,[2] the main idea was to give people the opportunity of going from one place to another without making physical effort and in a faster way than using people's own legs. The "car" was very simple, but it required someone to guide the machine and be responsible for the direction it would take, that human figure behind the wheels would be called "the driver". "Driver" and "operator" are broad terms that, in general, refer to anyone who "drives", "operates", or "is in actual physical control of" a vehicle.[3] In traditional vehicles, the human driver is responsible for all the interaction between the vehicle

[2]Daimler, "*Company History*". https://www.daimler.com/company/tradition/company-history/1885-1886.html.

[3]Mentioned by Smith (2014), p. 464.

and the surrounding environment. He/she is the one who will evaluate the conditions, distances, speed, and decide which actions to take.

The classic concept of the driver can be seen in several legislations and conventions around the world. One example to illustrate that classic characterization can be found in the Geneva and in the Vienna Conventions on Road Traffic, a compilation of rules that was made to facilitate international road traffic and increase road safety through the adoption of uniform traffic rules. Both conventions took place at a time when not even computers were as popular as they are now, so even less could it be possible to imagine cars circulating on the streets without human drivers on the inside. Considering this, it was possible to observe several debates during the last years about the need of modifying parts of the conventions for them to be aligned with new technologies, and this need was addressed especially concerning one particular article that brings the figure of the driver and the actions it should be responsible for. By analyzing Article 8, paragraph 5, of the Vienna Convention, it is noticeable the requirement of every vehicle or combination to have a driver who is at all times able to control the vehicle.[4] Apart from that requirement, the convention also defines that this driver should be able to perform all maneuvers required from him,[5] leaving very clear that he is at the entire time responsible for consequences arising from the driving activity.

The classic concept of "driver" brought by the convention was subject to discussion in the seventy-fourth session of the Global Forum for Road Traffic Safety. The discussions went over the understanding of the convention with regard to the use of automated driving functions, potentially focusing on Article 8 that is especially related to the driver figure.[6] The focus was directed to automated functions that

[4]Convention on Road Traffic, done at Vienna on 8 November 1968. "*Article 8. DRIVERS. 1. Every moving vehicle or combination of vehicles shall have a driver. 2. It is recommended that domestic legislation should provide that pack, draught or saddle animals, and, except in such special areas as may be marked at the entry, cattle, singly or in herds, or flocks, shall have a driver. 3. Every driver shall possess the necessary physical and mental ability and be in a fit physical and mental condition to drive. 4. Every driver of a power-driven vehicle shall possess the knowledge and skill necessary for driving the vehicle; however, this requirement shall not be a bar to driving practice by learner-drivers in conformity with domestic legislation. 5. Every driver shall at all times be able to control his vehicle or to guide his animals.*"

[5]Idem. "*Article 13. 1. Every driver of a vehicle shall in all circumstances have his vehicle under control so as to be able to exercise due and proper care and to be at all times in a position to perform all maneuvers required of him. He shall, when adjusting the speed of his vehicle, pay constant regard to the circumstances, in particular the lie of the land, the state of the road, the condition and load of his vehicle, the weather conditions and the density of traffic, so as to be able to stop his vehicle within his range of forward vision and short of any foreseeable obstruction. He shall slow down and if necessary stop whenever circumstances so require, and particularly when visibility is not good".*

[6]In this sense, see Antje von Ungern-Sternberg, "*Völker-und europarechtliche Implikationen Autonomen Fahrens*", p. 5. "*Das Wiener Übereinkommen lässt an mehreren Stellen die traditionelle Vorstellung erkennen, das sein Kraftfahrzeug durch einen Fahrer geführt wird. Zunächst definiert das Abkommen bei den Begriffsbestimmungen:*

Art. 1 Begriffsbestimmungen

are already available and those that are expected to be available within the next years and if those technologies were "covered" by the amendment of the 1968 Vienna Convention.[7] Members of the IWG-AD[8] reached an understanding that functions equivalent to SAE[9] Level 3 and SAE Level 4 are in line with the convention as last amended, considering both still require a driver, but there was no particular mention to SAE Level 5.[10]

In relation to the Vienna Convention, different views regarding the importance of its amendment have been expressed across Europe.[11] In Germany, for example, the amendment was welcomed by Thomas Weber, head of group research at Daimler and head of development at Mercedes-Benz. Other German experts did not see the convention as so much of a hindrance in relation at least in regard to the highly, but not fully automated vehicles,[12] and the reason is that although SAE Level 3 and SAE Level 4 cars do not have the need for the driver to be in control of the car the entire time, they do need a human in their interior to take action if needed, therefore this would perfectly be in line with the need expressed in the convention. Thus, the question that arises is: With the possible extinction of the classic human figure of the driver, how can liability be addressed and how insurance companies will adapt their underwriting and pricing methods to reflect those changes?

In this scenario, when it comes to insurance matters, it is known that motor liability insurance is compulsory in Europe, for example, and in determining the premium to be charged for insurance coverage, insurers must estimate the expected losses for the individual being insured.[13] Until now it is known that insurance companies from several countries use the profile system to evaluate the risks from a motor third party liability insurance portfolio and that the profile was entirely based on the information they have collected about each driver. Thus, they could group them in such a way that those with a similar possibility of loss are charged the same rate.[14] The use of variables like gender, age, marital status, address and even the frequency the car is used during the week are some of the factors that insurers consider while evaluating the risk. With automated and autonomous cars, this

v) "Führer" ist jede Person, die ein Kraftfahrzeug ode rein anderes Fahrzeug (Fahrräder eingeschlossen) lenkt oder die auf einer Strasse Vieh, einzeln oder in Henden, oder Zug-, Saum- oder Reittiere leitet".

[7]Informal document No. 2, Economic Commission for Europe, Inland Transport Committee, Global Forum for Road Traffic Safety. https://www.unece.org/fileadmin/DAM/trans/doc/2017/wp1/ECE-TRANS-WP1-2017-Informal-2e.pdf.

[8]Informal Working Group of Experts on Automated Driving.

[9]SAE International is the US based Society of Automotive Engineers.

[10]As we will see in the automation classification in Sect. 2.2, SAE Level 5 is the one that is fully automated with the machine performing all activities and therefore there is no need for a wheel, or a driver.

[11]The Vienna Convention was ratified by most of the continent.

[12]Schreurs and Steuwer (2016), p. 165.

[13]Luperto and Porrini (2005), p. 3.

[14]Luperto and Porrini (2005), p. 3.

evaluation will most likely suffer severe amendments or be completely changed if insurance companies develop a complete new product to substitute the traditional motor third party liability policy. For the transition period, small amendments such as questions related to the vehicle manufacturer and other technical aspects can be adopted in addition to the "driver" profile. However, there is still no standardized opinion on how the driver (or lack of driver) issue will be addressed by insurance companies, but some studies came to the conclusion that the current law probably does not prohibit automated vehicles, it may just discourage their introduction or complicate their operation.[15]

2.2 *Evolution of Vehicle Automation*

As part of the background, it is interesting to describe where we are in terms of automation in the automobile industry. When it comes to levels of automation, in first place it is important to clarify that the expression "autonomous vehicle", in theory, refers only to those cars that do not need a human behind its wheels (normally known as "the driver") and can perceive its surroundings alone, thanks to the technology involved in their structure. On the other hand, cars that have some kind of control by a machine but still need a human can be called "automated" and as far as the automation stage increases, the nearest the car comes of being finally classified as "autonomous vehicle". The Society of Automotive Engineers, a US based association published the classification of six different automation stages, that goes from Stage 0, that would be a car with no automation at all, until Stage 5, that is the full autonomous car.[16]

[15]Bryant Walker Smith writes in the conclusion of his article "*Automated Vehicles Are Probably Legal in the United States*" (2014), p. 516, that "*Key issues include the precise definition of these human-machine systems, the concept of control under the Geneva Convention, the potential for future regulation by the National Highway Traffic Safety Administration, and the application of myriad state laws concerning drivers and driving behavior. Five near-term recommendations might provide some initial clarity without placing law too far ahead of technology.*

First, regulators and standards organizations should work to develop common vocabularies and definitions that are meaningful in both law and engineering and accessible to the public and the media.

Second, the United States should closely monitor efforts to amend or interpret the Vienna Convention as an example for or caution regarding any potential effort to clarify the Geneva Convention.

Third, NHTSA should provide guidance about the likely scope and schedule of any initial regulatory action it may take with respect to automated vehicles.

Fourth, states should closely examine their vehicle codes to determine how those codes would or should apply to automated vehicles both with and without an identifiable human operator. (...)", p. 516.

[16]See website of National Highway Traffic Safety Administration in https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.

It is important to note that only Stage 5 is a fully automated example and as some studies show, those types of vehicles will have no wheel and consequently the figure of the driver will not exist anymore. Other levels of automation will still depend on having someone to take control of the vehicle, when needed, like Stage 3 for example, where the driver remains with the responsibility of acting, and also in Stage 4 when this responsibility could be questioned in concrete cases when there must be a complete evaluation of the conditions at the time of the accident.

Concerning new technologies that are being observed in vehicles that use automation, Google for example is working on a variant called Simultaneous Localisation and Mapping (SLAM), that according to the explanation from Hugh Durrant-Whyte, Fellow, IEEE and Tim Bailey,[17] it is the process by which a mobile robot can build a map of an environment and at the same time use this map to compute its own location. Other companies such as Apple, Audi, BMW, Tesla, and Volvo are also investing large amounts of money in researches for their future driverless cars. Apple already increased the number of its self-driving test fleet from 3 to 45 in March 2018, taking over the lead against Tesla and Uber.[18]

Considering the technology is still relatively new and no extensive database can evaluate how those vehicles will be doing in the future, it will be a challenge for insurance companies, at least at this current phase, to identify the key aspects they will consider for the adapted or brand new products to come. Different from a human driver, the movement choices from those cars are made by a computer system and their movements are not intuitively revealed through cognitive introspection and projection, what can clearly challenge certain basic assumptions from our existing legal structure[19] and current risk evaluation tools used by insurance companies.

- Stage 0: No automation at all, the human driver does everything.
- Stage 1: An automated system installed in the car can sometimes assist the human driver and conduct some parts of the driving activity (e.g. cruise control and park assistance).
- Stage 2: Slightly differs from Stage 1, here an automated system installed in the car can conduct some parts of the driving activity but the human driver shall still monitor the surroundings and perform the main driving activity.
- Stage 3: In this stage, rather than only one activity, the automated system can do both, conduct part of the driving activity and monitor the surroundings in some occasions. Anyhow, the human driver must be prepared to take back control when needed.
- Stage 4: At this point the automated system can perform all the tasks from Stage 3 and the human driver does not necessarily need to take back control, but it is important to notice that the automated system has limits of operation and certain conditions and/or surroundings can represent restrictions to the full operation of the system.
- Stage 5: Stage where the expression "autonomous car" can finally be used. Here the automated system performs all the driving tasks and there is no need of a human to be behind the wheels.

[17]Hugh Durrant-Whyte, Fellow, IEEE, and Tim Bailey, "*Simultaneous Localisation and Mapping (SLAM): Part I The Essential Algorithms*".

[18]Hall (2018).

[19]Surden and Williams (2016), p. 130. Autonomous vehicles use sensors or radar sensors to gather information about the nearby environment and this information is sent to the vehicle's onboard computers. In this sense, the authors continue to explain with citation of Richard Wallace & Gary

2.3 *Countries That Already Have Addressed the Autonomous Cars Subject in Their Legislation*

Testing autonomous cars on the streets require legal permissions and each country must review and check if their legislation is open for amendments and allowances for those types of tests. A recent study considering 20 countries[20] evaluated each one openness and preparedness for autonomous vehicles considering mainly 4 pillars: (i) Policy and legislation; (ii) Technology and innovation; (iii) Infrastructure; and (iv) Consumer acceptance. If we chose to look at the indexes attributed to the countries with higher insurance premium income for Motor Third Party Liability Insurance and that use to have the highest amounts for damage compensations, those being the US, United Kingdom, Germany, France and Spain, US was the one with the better classification and gained the 3rd position on the rank, followed by the United Kingdom (5th), Germany (6th), France (13th), and Spain (15th).

Concerning the United States, it is known that it is one of the most developed countries when it comes to the autonomous cars topic. According to the data provided by the National Conference of State Legislatures ('NCSL'), the number of states considering legislation for autonomous vehicles in the US increases every year; just in 2017, 33 states have introduced legislation and in 2016, there were 20 states adopting it. So we come to a scenario where from total US 56 states, 27 already have enacted legislation about the subject, 7 states have executive orders on the matter, 3 have both and 19 have none.[21] NHTSA[22] is the federal agency that has thus far been the most visible and active in promoting automated vehicles in the country,[23] it has broad authority to regulate these new technologies and has various regulatory tools and methods that can be applied in addressing these new potential challenges.[24] Some common features of their regulation regard the definitions of autonomous driving and autonomous vehicles employed and the conditions for obtaining operating and testing permissions. Liability issues are also beginning to gain attention,[25] currently in most of the US states it is illegal to circulate with a

---

Silberg, KPMG & CTR for auto Research, "Self-Driving Cars, The Next Revolution, Center for Automotive Research" (2012): "*In sum, many discussions of self-driving technology focus on sensors, but it is important to emphasize the degree to which self-driving functionality often depends upon pre-built digital maps. Different research strategies rely upon pre-built maps to a greater or lesser degree. In general, when a vehicle can combine past information from pre-built digital maps along with live information from its sensors about its surroundings, this is often the most effective strategy for achieve highly reliable autonomous driving*", p. 140.

[20]KPMG (2018).

[21]National Conference of State Legislatures, "*Autonomous Vehicles Self-Driving Vehicles Enacted Legislation*". http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx#enacted.

[22]National Highway Traffic Safety Administration.

[23]Kohler and Colbert-Taylor (2014), p. 108.

[24]Wood et al. (2012), p. 1426.

[25]Schreurs and Steuwer (2016), p. 160.

motor vehicle that does not have liability insurance coverage; on the other hand there are some states that require only that the person who is operating the car is financially responsible to compensate anyone if an injury or damage is caused.[26] State laws set the minimum amounts of insurance and driving without the mandatory coverage may result in fines.

Concerning the United Kingdom, the Department for Transport has determined that it is legal for driverless cars to operate on any public roads without permits or extra insurance.[27] Another positive point is that by not ratifying the Vienna Convention on Road Traffic and allowing the piloting of fully autonomous vehicles on public roads without need for primary legislation, the UK has created a supportive environment for the development of autonomous vehicles technologies.[28] Apart from the incentives, the UK's Centre for Connected and Autonomous Vehicles has an active program to support development and deployment of autonomous vehicles in the country.[29] The Centre works with government, industry, academia, and regulators to make the UK one of the world's premier development locations for autonomous vehicles.[30] Concerning the current scenario regarding liability, it is mandatory to have a motor third party liability insurance policy; uninsured drivers are subject to penalties and can be even disqualified from driving.[31]

[26]New Hampshire does not have a compulsory insurance liability law and Virginia requires drivers to have insurance or register an uninsured vehicle for a significant fee.

[27]Department for Transport, "*The Pathway to Driverless Cars: Summary report and action plan*", p. 20, highlights UK as being a premium location to develop automated vehicles: "*We believe the UK is uniquely positioned to become a premium location globally for the development of these technologies. Those wishing to conduct tests are not limited to the test track or certain geographical areas, and do not need to obtain certificates or permits. Provided they have insurance arranged, they are not required to provide a surety bond*". https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf.

[28]KPMG (2018), p. 21.

[29]UK Connected & Autonomous Vehicle Research & Development Projects 2018, p. 8. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737778/ccav-research-and-development-projects.pdf.

The Centre currently focuses on three areas: Regulation, Research and Development and Testing Infrastructure. There are several projects they are involved in, among them, there is one named after "Venturer" that aims to investigate the barriers to the adoption of connected and autonomous vehicles in the UK. Its objectives include the development of an understanding of the public acceptance, and also legal and insurance blockers to autonomous vehicles. It intend to test cases developed by social, legal and insurance experts using a fully immersive simulator and controlled road network. See page 12.

[30]UK Connected & Autonomous Vehicle Research & Development Projects 2018, p. 2. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737778/ccav-research-and-development-projects.pdf.

[31]Road Traffic Act 1988. "*143 Users of motor vehicles to be insured or secured against third-party risks. (1) Subject to the provisions of this Part of this Act – (a) a person must not use a motor vehicle on a road [or the public place] unless there is in force in relation to the use of the vehicle by that person such a policy of insurance or such a security in respect of third party risks as complies with the requirements of this Part of this Act, and (b) a person must not cause or permit any other person to use a motor vehicle on a road [or other public place] unless there is in force in relation to the use*

Germany, worldwide known for its powerful cars and highways without speed limits still faces two problems when it comes to self-driving cars: consumer acceptance and the fact that Germany signed and ratified the 1968 Vienna Convention on Road Traffic.[32] However, on the policy and legislation aspect, in 2017 it was allowed in the country to test self-driving cars on public roads[33] as long as the authorities have provided an exemption. Germans are also investing in innovative technologies and high tech mobility strategies that include requirements that the software that controls the cars must be programmed to avoid injury or death of people at all cost, this way German regulators want to assure that when an accident is inevitable, the software must choose whichever action will hurt people the least.[34] Currently Germany has severe rules when the subject is motor third party liability. The Road Traffic Regulation establishes some basic rules on the traffic in the country but the text still only refers to persons operating vehicles, what probably will have to face some amendments to follow the progress with autonomous cars tests. Under the 'Pflichtversicherungsgesetz',[35] dated April 5 1965, the owner of a motor vehicle is obliged to have a third party liability insurance to cover any damages caused by the use of the vehicle.[36]

As per the latest news, France is establishing a legislative framework that will allow the testing of autonomous cars on public roads by 2019. As announced lately by President Emmanuel Macron, Stage 4 vehicles will be used on roads around the country with no human operator behind the wheel, as the current legislation requires. Currently, test with driverless cars are heavily restricted to time and location, but the country expects to have by the beginning of 2019 the legislative framework

---

of the vehicle by that other person such a policy of insurance or such a security in respect of third party risks as complies with the requirements of this Part of this Act. (2) If a person acts in contravention of subsection (1) above he is guilty of an offence. (3) A person charged with using a motor vehicle in contravention of this section shall not be convicted if he proves – (a) that the vehicle did not belong to him and was not in his possession under a contract of hiring or of loan, (b) that he was using the vehicle in the course of his employment, and (c) that he neither knew nor had reason that there was not in force in relation to the vehicle such a policy of insurance or security as mentioned in subsection (1) above. (4) This Part of this Act does not apply to invalid carriages.

144. Exceptions from requirement of third-party insurance or security. (1) Section 143 of this Act does not apply to a vehicle owned by a person who has deposited and keeps deposited with the Accountant General of the [Senior Courts] the sum of [£500,000] at a time when the vehicle is being driven under the owner's control."

[32]See discussion in Sect. 2.1.

[33]The Drive, May 12th, 2017, "*German Green-Lights Self-Driving Cars with New Law*". http://www.thedrive.com/tech/10215/germany-green-lights-self-driving-cars-with-new-law.

[34]Technology News, August 23rd, 2017 "*Germany draws up rules of the road for driverless cars*". https://www.reuters.com/article/us-autos-autonomous-germany/germany-draws-up-rules-of-the-road-for-driverless-cars-idUSKCN1B31MT.

[35]*Gesetz über die Pflichtversicherung für Kraftfahrzeughalter*, that means law for compulsory insurance for car owners.

[36]Minimum amount established for coverage is 7,500,000 Euros for bodily injury and 1,220,000 for material damages.

authorizing the experiments. A more wide regulatory framework is expected, allowing the circulation of autonomous vehicles on the streets by 2022.[37] In respect of insurance and liability, since 1958 it was already mandatory in the country to have motor insurance to make sure that any victim from car accidents would be indemnified for material and bodily injury damages.[38] In July 1985, the law called "Loi Badinter" came into force and defined the indemnity procedures in case of accidents involving motor vehicles.[39] Motor third party liability insurance in France is well known for being unlimited regarding the sum insured, with autonomous vehicles replacing the human drivers, the need for an unlimited coverage may be subject to reevaluation.

Spain is working to expand rules for self-driving vehicles and on modifications to the insurance law. So far, the regulation of autonomous-driving tests comes from an instruction approved in November 2015 by the "Dirección General de Trafico (DGT)" and is related to all self-driving cars up to Stage 5. In January 2018, DGT and Mobileye agreed to a collaboration to reduce accidents in the roads and prepare the country's infrastructure and regulatory policy for autonomous vehicles. It was said that this collaboration will transform Barcelona into a laboratory by putting 5000 vehicles[40] in the city equipped with the Mobileye 8 connect technology. On the liability aspect at present times, motor third party liability insurance coverage is mandatory by law and not having one can result in the application of fines.[41,42]

[37]Autovista Group, April 3rd, 2018, "*France to amend legislation for autonomous vehicle trials*". https://www.autovistagroup.com/news-and-insights/france-amend-legislation-autonomous-vehicle-trials.

[38]Loi no. 58-208 du 27 février 1958 Institution d'une obligation d'assurance en matière de circulation de véhicules terrestres a moteur. "*Art. 1. – Tout personne civile ou morale, dont la responsabilité civile peut être engagée en raison de dommages corporels ou matériels causés à des tiers par un véhicule terrestre à moteur, ainsi que par ses moteurs ou semi-remorques, doit, pour faire circuler les-dits véhicules, être couverte par une assurance garantissant cette responsabilité […]*".

[39]Law no. 85-677 dated July 5 1985, "*Loi n°. 85-677 du 5 juillet 1985 tendant à l'amélioration de la situation des victims d'accidents de la circulation et à l'accélération des procédures d'indemnisation*".

[40]Automotive News Europe, August 15th, 2018, "*Spain works toward framework for autonomous driving*". http://europe.autonews.com/article/20180815/ANE/180809786/spain-works-toward-framework-for-autonomous-driving.

[41]Fines can reach up to 3000 Euros plus all the costs of the accident together with other sanctions established by the decree. The amounts of the mandatory coverage established by the Decree 8/2004, dated October 29 is 70,000,000 Euros per claim, related to personal injuries and 15,000,000 Euros for material damages.

[42]Legislative Decree 8/2004 dated October 29 approves the text of the law on civil liability and insurance regarding the circulation of motor vehicles. A translated version of the original text would be: "*Article 4. Territorial scope and quantitative limits. 1. The compulsory insurance provided for in this Law shall guarantee the coverage of motor third party liability for vehicles with habitual parking in Spain, through the payment of a single premium, throughout the territory of the European Economic Area and of the States adhering to the Agreement between the national insurance offices of the Member States of the European Economic Area and other associated*

Until the moment, the most advanced country when it comes to legislation and policy, innovation, infrastructure and consumer acceptance regarding autonomous cars is Netherlands.[43] In February 2017, the Dutch Cabinet approved a bill that removed legal restrictions and made possible for driverless vehicles to carry out much more extensive testing of self-driving vehicles, without the physical presence of the driver in the vehicle.[44,45] There are some projects that helped to spread the technology through the country, one example is the Dutch Automated Vehicle Initiative ("DAVI"), that not only develops high automated vehicles for research and demonstrations on public roads but also tries to proof the safety and focuses on human factors on automated driving.[46] On the motor third party liability aspect, currently, such as for the other countries that are part of the European Union, it is mandatory in the country to have insurance and the owner of the vehicle is the one who will be held responsible irrespective of the driver.

As observed, most of the legislation and regulation available until the moment on the subject is all about allowing or not tests with autonomous vehicles on the streets or on other practical aspects such as requirements to have an autonomous vehicles circulating, none of them went into an in depth liability analysis in case of an accident involving an autonomous car or even which insurance policy should respond when there is no driver behind the wheels. The traditional motor third party liability insurance is mandatory for the countries mentioned above, but no detailed amendment was made neither in their legislation nor in their regulation focusing on the new environment to come. Some countries benefit of not having in their legislation a particular mention to the "driver" figure, or, they did not sign or ratified the Vienna Convention, but it is inevitable that the need for a more focused approach in a very near future will be needed. This way, since there is still nothing

States. This coverage shall include any type of stay of the insured vehicle in the territory of another State Member of the European Economic Area during the term of the contract. 2. The amounts of the compulsory insurance coverage will be: a) Personal damages, 70 million euros per claim, whatever the number of victims. B) Material damages, 15 million euros per claim. The above amounts will be updated according to the European consumer price index, in the same percentage as the European Commission for the review of the minimum amounts set out in Article 1, section (2) of Council Directive 84/5/EEC, of 30 December 1983 on the approximation of the laws of the States Member relating to liability insurance resulting from the circulation of motor vehicles (...)".

[43]KPMG (2018), p. 13, "*The Dutch ecosystem for AVs is ready. The intensively-used Dutch roads are very well developed and maintained and other indicators like telecoms infrastructure are also very strong. In addition, the Dutch government Ministry of Infrastructure has opened the public roads to large-scale tests with self-driving passenger cars and lorries*".

[44]Global Legal Monitor. "*Netherlands: Legislation to allow more testing of driverless vehicles*". http://www.loc.gov/law/foreign-news/article/netherlands-legislation-to-allow-more-testing-of-driverless-vehicles/.

[45]*Experimenteerwet Zelfrijdende Auto* loses legal restrictions so that manufacturers have more opportunities to conduct elaborate tests.

[46]See in www.davi.connekt.nl. "DAVI implements automation technology in real cars that can be driven on existing roads in normal traffic".

concrete on the liability definition so far, Sect. 3 was reserved to present some of the discussions, thesis, and solutions that could be found on the subject so far.

3 Future Predictions: What Has Already Been Said and What Can Be Expected to Occur?

As mentioned, considering that the topic is relatively new, there is still a lack in jurisprudence involving liability and autonomous vehicles. Traditional liability becomes exponentially more confusing and difficult to apply, when the driver of a vehicle is not a human but rather a complex system of interconnected machinery.[47] Although some real accident examples could be seen, such as the crash involving an Uber vehicle in March 2018,[48] standardized rules that address the subject are still rare.

As it was possible to observe in Sect. 2.1, until now liability after a vehicle crash could be mainly attributable to the driver, in some other cases to the vehicle malfunction or even to the road conditions, but the figure of a human person was necessary. Fully autonomous cars are not supposed to have a driver, they will act according to the software installed on them, and if they cause any damages there will be no physical figure of the driver to "easily" solve the liability attribution discussion. Considering this change will be rather gradual than fast, we may experience for a long period of time a transition period with a mix of automated and autonomous cars. Are we legally prepared to handle this scenario?

There are several papers, mainly from the US that raise some theories on what can happen to properly assign liability in the future. After analyzing some of the theories, it is possible to distinguish the following possible future scenarios:

- For automated vehicles, check if the driver had conditions to act when needed, if so, driver can still be held liable;
- For autonomous vehicles, manufacturer of the autonomous vehicle as the main responsible in case of an accident;
- For autonomous vehicles, manufacturer as the responsible but there is the need to analyze the entire chain of providers, including software developers; and
- For automated and autonomous vehicles, no-fault system as the solution for the liability impasse.

Concerning the likelihood of acting in case there is a need to, mainly the case for automated vehicles, Jeffrey K. Gurney addresses the liability analysis by bringing an interesting comparison between what he classifies as four types of drivers: The

[47]Funkhouser (2013), p. 440.

[48]The New York Times, March 19th, 2018, "*Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam*". https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html.

"Distracted Driver", the "Diminished Capabilities Driver", the "Disabled Driver" and the "Attentive Driver".[49] After checking the four examples, the conclusion is that each situation must be analyzed in a separate manner and he makes a point when mentioning that courts should not expect every driver to be an "Attentive Driver" to protect liability, otherwise some of the purposes of the autonomous vehicles would be defeated. That is because unlike drivers in traditional vehicles, the figure of the driver in autonomous vehicles is normally not paying attention, since it is not expected for him to act and he can then focus his attention on something else. One of the main ideas of not having to drive or pay attention to the traffic would be, apart from the locomotion itself, a way of increasing people productivity, as they do not have to perform the action of driving. This way, they could use their commuting time to work or do some other task. On the other hand, the driver will not always be able to intervene when necessary, as observed in the examples mentioned above (Diminished Capabilities Driver/Disabled Driver[50]).

A solution that was presented for manufacturers, to try to correctly determine if the driver or the machine were in charge of the vehicle control at the time of the accident, is the installation of devices such as black boxes inside the cars.[51] This mechanism, known as Event Data Recorder ("EDR") is analogous to the Flight Data Recorder ("FDR") that can be found in airplanes, it transmits the information about the airplane, its functionality, and an eventual pilot error. By analyzing this information, investigators can easily determine whether the cause of a plane crash was because of human error or a mechanical failure. If this theory is applied to automated vehicles, manufacturers would have more details around the occurrences when claims start to appear.

Most of the analyzed authors bring, in some aspect of their work, the possibility of the manufacturer of the vehicle to be held liable for the damages in case of a crash

[49]Gurney (2013), p. 247 makes the following distinction between the drivers: "*1. The Distracted Driver (...) is the autonomous car user who is not paying attention; it could be someone reading a book like Sarah, using a cell phone, eating a snack, or any other situation. Essentially, the Distracted Driver purposefully engages in a task other than driving, thus relying on the autonomous vehicle completely. 2. The Diminished Capabilities Driver (...) is the person whose driving capabilities are diminished for some reason; it could be an elderly person like Richard, an intoxicated person, or a minor. This person typically would not be driving because of his or her diminished capabilities and would have to rely on others. Thus, the Diminished Capabilities Driver could benefit greatly from the convenience and independence an autonomous vehicle provides. 3. The Disabled Driver (...) is the person who cannot drive a traditional vehicle because of a physical disability, such as blindness or an amputated limb. Thus, the Disabled Driver relies entirely on the autonomous nature of the car in the event of a computer malfunction. 4. The Attentive Driver (...) is the user who watches the road and surroundings in the same way he or she would while driving a traditional vehicle. The Attentive Driver may not trust the autonomous ability of the vehicle such that he or she constantly checks that the car is driving correctly, or the Attentive Driver may simply not have any other tasks to address while in the vehicle. The key is that the Attentive Driver has the potential to foresee and prevent accidents, unlike the Distracted, Diminished Capabilities, and Disabled Drivers*", pp. 255–257.

[50]Gurney (2013), pp. 255–257.

[51]Bose (2015), p. 1344.

and this shifting of liability from the driver to the vehicle would occur gradually, already with partial autonomous systems and could end up by shifting entirely to the vehicle and the components of its accident avoidance system when it comes to a fully autonomous vehicle.[52]

In this scenario, manufacturers should be liable for most accidents caused when the vehicle is in autonomous mode, considering it was probably the manufacturer technology's fault since the technology itself was operating the vehicle and not a traditional driver,[53] but even so, it is important to observe some details that would configure exceptions to that assumption, such as maintenance liability, that can make the owner of the vehicle responsible under the argument of negligence for not having taken care of the vehicle as he should have done. Once an owner is aware that the automobile is not acting as it should, the owner may be negligent in continuing to drive the car until the issue is adequately addressed.[54] In case of the following situation, where the owner of an autonomous vehicle received a notification to proceed with a critical software update of the vehicle within 24 h and the owner does not observe that detail and continue to circulate with the car, liability may be directed to the owner, and in the insurance field, discussion around the coverage can be generated if this is compared to gross negligence.[55] That leads to a possible conclusion that for liability definitions matter, it will still be important to separate owner's negligence from product liability.

Making reference to the software update as mentioned above, it is important to remember that manufacturers handle with several different vehicle parts providers, including software developers and the manufacturer of a component used in the autonomous system. Not to forget the road designer as well, in case of an intelligent road system that helps control the vehicle. Following that line of thinking, the third possible scenario would be the assumption that manufacturers may be held responsible for what we call "the final product", but there is an entire chain behind, that in case of an in-depth analysis after a crash, other parties could be held liable together or in lieu of the manufacturer.

As it was possible to observe during our research, when an autonomous vehicle crash, there is a high probability that something may have go wrong with the collision system or the vehicle has encountered conditions that it was not adequately programmed to address[56] but it is always necessary to do a full analysis, especially when we are still talking about a mixed environment where normal or automated cars still circulate on the streets. As all the machines, autonomous vehicles would probably also present some use conditions that must be carefully observed by the user, an interesting example would be if the instruction manual advices the owner

[52]Marchant and Lindor (2012), p. 1326.

[53]Gurney (2013), p. 271.

[54]Bose (2015), p. 1338.

[55]New Atlas, June 8th, 2016, "*UK company launches insurance policy for autonomous cars*". https://newatlas.com/adrian-flux-driverless-car-insurance/43739/.

[56]Marchant and Lindor (2012), p. 1328.

not to use the autonomous vehicle in certain weather conditions or specific types of traffic patterns and the owner ignores this warning there is when the driver or owner may be held at least partially at fault.[57]

To support any of the three first scenarios, which may to some extent bring manufacturer's liability into consideration, it is known that product liability law has yet to be adapted to reflect technology aspects, and courts and legislatures need to take steps to hold autonomous technology manufacturers liable when accidents occur.[58]

Finally, different from the other three scenarios, adopting a no-fault system is another theory that in the opinion of some authors could solve the issue with autonomous vehicles, especially for insurers. This theory is about removing the liability attribution factor for motor vehicle accident injury, no fault insurance claims arising from automated and autonomous cars would be made to each car insurance policy and there would be no need to evaluate who or what was really responsible for the damages. As known, this system is already in force in Canada, for example, and its basis consists in each insured being indemnified for losses by its own insurance company, regardless of fault in the incident generating the losses.

4 How Can Insurance Industry Adapt Itself to the New Reality?

Motor third party liability insurance, the way we know exists since the Road Traffic Act 1930[59] first introduced it in the United Kingdom, and each country adapted the idea to create products that would attend its own population. It is also an industry that handles considerable amounts of money in insurance premiums per year and the main idea behind this type of insurance is to compensate victims of car accidents.

It is known that liability is independent from insurance, and an individual can still be sued by the victim if he is deemed responsible for one accident regardless of having or not an insurance policy to respond for the damages. However, in praxis it is easy to see that in some countries where there is not a strong liability culture, people that do not seek for assistance when the responsible for an accident had no insurance policy to respond for damages. Since this type of insurance coverage is not mandatory worldwide, several families suffer severe financial consequences after losing an important member of the family after a car accident.

As mentioned, the traditional insurance for this type of liability is mandatory in the European Union, for example. Directive 2009/103/EC of the European

[57]Marchant and Lindor (2012), p. 2012.

[58]Gurney (2013), p. 272.

[59]Road Traffic Act, 1930 "*Chapter 43. An Act to make provision for the regulation of traffic on roads and of motor vehicles and otherwise with respect to roads and vehicles thereon, to make provision for the protection of third parties against risks arising out of the use of motor vehicles and in connection with such protection to amend the Assurance Companies Act, 1909 (...)*".

Parliament and of the Council,[60] soon to be amended by Proposal 2018/0168,[61] stipulates that member states are obliged to guarantee insurance cover at least in respect of certain amounts to protect victims of car accidents. Those minimum amounts should not only be updated to consider the inflation, but should also be increased in real terms to improve the protection of the victims. The directive does not make any particular mention to the "driver", or any special requirement for it to be a human being, nevertheless, for most of the existent insurance systems, the basic element to measure the risk exposure is the classification of the driver. Liability nowadays is still linked with the driver and as mentioned in Sect. 2.1, some countries even use a driver profile questionnaire to evaluate their exposure and define the premium for the coverage. When there is no driver, or the driver is not necessarily the main one to control the car, there will be the need of a new approach of the motor liability insurance product and the way insurance companies look at the risk.

Although technology seems to develop relatively fast, the transition from manual operated vehicles to autonomous cars will be gradual, and can even take some additional time depending on the geographic area, but it is imperative that insurance companies must already start rethinking their current products and their pricing systems. Focusing on analyzing the impacts of this scenario in the insurance industry, Deloitte has developed an actuarial model of potential future premium revenue streams according to the expected evolution of driving and mobility preferences. They estimate premiums of USD 145 billion in 2040 representing a nearly 70% decrease in premiums that the insurance industry would collect,[62] but it all will depend on the pace the changes could occur.

From a pricing and ratemaking perspective, they also argue that insurers and their actuaries will have to alter or overhaul the existing rating algorithms as shared mobility and autonomous vehicles proliferate, since there will be a considerable change in the risk profiles for policyholders (no human driver profile anymore) and the use of the car-year as the base exposure may need to change.[63] On the claims and reserving side there will also be considerable impacts, since actuaries normally use a data base history to project future losses. Considering there will be no history available yet, greater judgment will be needed during the first years or even decades.

Some of the actions that may be taken by the insurers during the transition time include[64]:

– Develop more technical underwriting capabilities;
– Establish advanced analytics capabilities; and

[60]Dated 16 September 2009, relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability.

[61]The amendment focuses on two aspects: Insufficient protection of victims of motor vehicle accidents and differential treatment and freeriding behavior negatively affecting policyholders.

[62]Deloitte (2016), p. 7.

[63]Deloitte (2016), p. 8.

[64]Deloitte (2016), p. 8.

– Plan for product and business-line shifts—including offering driverless car insurance.

On the underwriting perspective the profile questionnaire that is known for motor third party liability insurance in most of the countries may give space to a deep analysis of the manufacturer that produced the vehicle, including the indication of the supplier for vehicle parts. Nowadays it is known that underwriters classify vehicle parts into either "critical" or "non-critical" depending on their function in the vehicle.[65] Brakes for example are considered a "critical" part, since any problem can lead to serious injuries to the vehicle occupants; on the other hand, interior lights are harmful and therefore classified as a "non-critical" part. In the future, the software will be likely included on the list of critical parts. It will also be part of the underwriter work to fully understand the conditions that affect the normal vehicle operation and to identify maintenance issues that can have an impact on the product and that must be observed by the owner of the vehicle. All this process may be an issue in the beginning but with time and after the construction of a database, underwriters will be able to adapt the new risk profiles and adjust their pricing and ratemaking.

For insurance matters, with automated vehicles it will be necessary to identify whether the car or the driver was in charge of the control at the time of the accident, and therefore from a risk management perspective, some measures can be taken by the manufacturer[66]: (i) Create simple and conclusive schemes to record when the driver overrides the automated vehicle computer (like black boxes); (ii) Clearly defining maintenance procedures to be followed by the operator; (iii) Consider the creation of an insurance product that includes both the manufacturer and the operator on the policy; and (iv) Create a disabling function as a response to any attempt of altering or enhancing the software. Those are examples of some methods that can help protect manufacturers from liability, but of course, an adequate legislation to be adopted by the countries can be clearer in ways of defining liability. At the end, it is expected that a future environment with autonomous cars will not only present fewer claims and less fraud for the insurance industry, but also a lower amount of insurance premium income assuming that the risk will be classified as "better" and the likelihood of accidents is considerably lower than what human drivers could cause.

5 Conclusions

In summary, it was possible to notice that when it comes to accidents caused by motor vehicles, the attribution of liability was until now generally made to the driver or the owner of the vehicle and this opened a wide market for insurance companies to

[65]Munich Re (2016), p. 9.

[66]Munich Re (2016), p. 9.

offer products to bear those types of risks. With a profile analysis from the driver, that used to include several different variables from gender to the home address, it was easy for insurance companies to allocate them in different classifications and charge the respective premium according to the risk exposure.

Nevertheless, with all the new technology that is coming on the automobile industry, the figure of physical driver will gradually disappear in the near future and vehicle manufacturers may become the core object of analysis by insurance companies for the development of new insurance products. Service providers such as Uber, Lyft, or Cabify may also be considered for the development of a specific type of insurance coverage. Third party liability insurance policy, the way we know, may have to be amended accordingly or even completely changed to become a product that can offer both coverage, motor third party liability, and product liability, depending on the car to be insured. Another scenario would be where insurance companies chose to adopt a no fault basis system for their auto policies to avoid the liability discussion.

I believe that within the next years and depending on how fast autonomous vehicles will gain the streets, the liability attribution discussion will gain more attention and solutions among the market, not only from a legal perspective but also for insurance matters. In the meantime, and during this transition phase where the number of automated and autonomous cars circulating is still a minority, I am in the opinion that a no fault basis system is an interesting solution for insurance companies to adopt. Considering there are countries such as Canada, Australia, and New Zeeland that already use this system, it will be only a manner of adapting an already existing model and defining who will be the insured named in the policy. It is also important to define whether to use a pure no fault system or partial no fault laws, such as those adopted in some states of the U.S. where the right to sue the one that caused the accident still exists for death and severe injuries cases. When adopting the no fault system, the liability coverage is, in a certain matter, transferred to first-party coverage and some of the favorable arguments sustained by countries that already use this type of system include lower premium cost, avoidance of expensive litigation processes and quick payments for injuries or property damages. However, in a mixed scenario where ordinary cars circulate together with automated and autonomous ones, this solution may be questioned by some people that can argue they do not intend to use their insurance to pay for their own damages when the accident was caused by an uncontrolled autonomous car, for example; in this particular case, if proven that the machine had a real technical problem and was really "at fault" at the time of the accident, sub-rogation against the autonomous vehicle insurer could take place and even a legal process against the policyholder, in case of more severe injuries to individuals, following a partial no fault line of coverage.

Concerning the definition of the insured, for automated vehicles, it may still be the "driver" or the owner, but for an autonomous car this may shift to the manufacturer or even a service provider, like Uber. With the no fault basis system, it will be possible to assume that the one who puts the car into circulation is the one who must have an insurance policy, no matter if he/she is the provider of a certain locomotion

service, a delivery agency or even a manufacturer that is still testing its new autonomous vehicles in the streets.

As it was possible to observe, currently countries are more focused in granting the necessary permission and ambiance for autonomous cars to be adequately tested, in that way, liability and insurance subjects will most likely be their next concern. Clearly, such changes will be gradual as we monitor the evolution of new technologies, but insurers must keep an eye in the future and already start designing their new products that will soon substitute the traditional third party liability policy and will have the obligation to meet or exceed the premium income currently generated by this line of business. Actuaries will also have the important task to initially work on risk models without a large (or any) historical data on losses involving automated and autonomous cars and therefore any kind of extra information on the policyholder may be helpful, no matter if it will be a real person or a legal entity. The end of the traditional model the way we have known for decades may be only a sign of the beginning of a new era. Welcome to the future.

References

Automotive News Europe, August 15th, 2018, Spain works toward framework for autonomous driving. http://europe.autonews.com/article/20180815/ANE/180809786/spain-works-toward-framework-for-autonomous-driving

Autovista Group, April 3rd, 2018, France to amend legislation for autonomous vehicle trials. https://www.autovistagroup.com/news-and-insights/france-amend-legislation-autonomous-vehicle-trials

Bertoncello M, Wee D (2015) Ten ways autonomous driving could redefine the automotive world. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/ten-ways-autonomous-driving-could-redefine-the-automotive-world

Bose U (2015) The black box solution to autonomous liability. Wash Univ Law Rev 92:1325

Daimler, Company History. https://www.daimler.com/company/tradition/company-history/1885-1886.html

Davi Connekt. www.davi.connekt.nl

Deloitte (2016) Quantifying an uncertain future: insurance in the new mobility ecosystem. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-insurance-in-the-new-mobility-ecosystem.pdf

Department for Transport, The pathway to driverless cars: summary report and action plan. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf

Funkhouser K (2013) Paving the road ahead: autonomous vehicles, products liability, and the need for a new approach. Utah Law Rev:437

Global Legal Monitor. Netherlands: legislation to allow more testing of driverless vehicles. http://www.loc.gov/law/foreign-news/article/netherlands-legislation-to-allow-more-testing-of-driverless-vehicles/

Gurney JK (2013) Sue my car not me: products liability and accidents involving autonomous vehicles. Univ Ill J Law Technol Policy:247

Hall Z (2018) Apple ramping self-driving car testing, more CA permits than Tesla and Uber. Electrek. Retrieved 21 March 2018

Hugh Durrant-Whyte, Fellow, IEEE, and Tim Bailey, "Simultaneous Localisation and Mapping (SLAM): Part I The Essential Algorithms"

Informal document No. 2, Economic Commission for Europe, Inland Transport Committee, Global Forum for Road Traffic Safety. https://www.unece.org/fileadmin/DAM/trans/doc/2017/wp1/ECE-TRANS-WP1-2017-Informal-2e.pdf
Kohler WJ, Colbert-Taylor A (2014) Current law and potential legal issues pertaining to automated, autonomous and connected vehicles. Santa Clara Comput High Technol Law J 31:99
KPMG (2018) Autonomous Vehicles Readiness Index. Accessing countries openness and preparedness for autonomous vehicles. https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2018/sector/automotive/autonomous-vehicles-readiness-index.pdf
Luperto I, Porrini D (2005) Dynamic risk classification in a law and economics perspective: the Italian perspective. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=828824
Marchant GE, Lindor RA (2012) The coming collision between autonomous vehicles and the liability system. Santa Clara Law Rev 52:1321
Munich Re (2016) Autonomous vehicles. considerations for personal and commercial lines insurers. https://www.munichre.com/site/mram-mobile/get/documents_E706434935/mram/assetpool.mr_america/PDFs/3_Publications/Autonomous_Vehicles.pdf
National Conference of State Legislatures, Autonomous vehicles self-driving vehicles enacted legislation. http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx#enacted
New Atlas, June 8th, 2016, UK company launches insurance policy for autonomous cars. https://newatlas.com/adrian-flux-driverless-car-insurance/43739/
Schreurs MA, Steuwer SD (2016) Autonomous driving – political, legal, social, and sustainability dimensions. In: Maurer M, Gerdes JC, Lenz B, Winner H (eds) Autonomous driving, technical, legal and social aspects. Springer Open
Smith BW (2014) Automated vehicles are probably legal in the United States. Tex A&M Law Rev 1:411
Surden H, Williams M-A (2016) Technological opacity, predictability, and self-driving cars. Cardozo Law Rev 38:121
Technology News, August 23rd, 2017, Germany draws up rules of the road for driverless cars. https://www.reuters.com/article/us-autos-autonomous-germany/germany-draws-up-rules-of-the-road-for-driverless-cars-idUSKCN1B31MT
The Drive, May 12th, 2017, German green-lights self-driving cars with new law. http://www.thedrive.com/tech/10215/germany-green-lights-self-driving-cars-with-new-law
The New York Times, March 19th, 2018, Self-driving Uber car kills pedestrian in Arizona, where robots roam. https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html
UK Connected & Autonomous Vehicle Research & Development Projects 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/737778/ccav-research-and-development-projects.pdf
Website of National Highway Traffic Safety Administration in. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety
Wood SP, Chang J, Healy T, Wood J (2012) The potential regulatory challenges of increasingly autonomous motor vehicles. Santa Clara Law Rev 52:1423

Legislative Instruments

1968 Vienna Convention on Road Traffic dated November 8, 1968
Law no. 58-208 dated February 27, 1958, France
Law no. 85-677 dated July 5, 1985, France ("*Badinter Law*")
Road Traffic Act 1988, Parliament of the United Kingdom
Road Traffic Act, 1930, Parliament of the United Kingdom
Royal Legislative Decree 8/2004 dated October 29, 2004, which approves the revised text of the Act on civil liability and insurance in the circulation of motor vehicles

Ethical Issues, Cybersecurity and Automated Vehicles

Sara Landini

1 Definition of Automation

The Oxford English Dictionary (1989) defines automation as: "1) Automatic control of the manufacture of a product through a number of successive stages; 2) the application of automatic control to any branch of industry or science; 3) by extension, the use of electronic or mechanical devices to replace human labor."

Etymologically, the term automation roots back to the Greek word "automatos". Thus, the complete substitution of humans by machines (i.e., full automation) might be derived and used to denote the meaning of the term automation. Nof (2009), argues: "automation, in general, implies operating or acting or self-regulating, independently, without human intervention". Whereas, automation, generally speaking, can be regarded within a spectrum of no automation (manual) to full automatic (automate). In the middle, it is possible to have different situations (partial automation or semi-automation) in which many tasks are performed in a collaboration of humans and automation systems.[1]

[1] Nof (2009), pp. 13–52: The meaning of the term automation is reviewed through its definition and related definitions, historical evolution, technological progress, benefits and risks, and domains and levels of applications. A survey of 331 people around the world adds insights to the current meaning of automation to people, with regard to: What is your definition of automation?; Where did you first encounter automation in your life?; and What is the most important contribution of automation to society? The survey respondents include 12 main aspects of the definition in their responses; 62 main types of first automation encounter; and 37 types of impacts, mostly benefits but also two benefit–risks combinations: replacing humans, and humans' inability to complete tasks by themselves. The most exciting contribution of automation found in the survey was to encourage/inspire creative work; inspire newer solutions. Minor variations were found in different regions of

S. Landini (✉)
Department of Law, University of Florence, Florence, Italy
e-mail: sara.landini@unifi.it

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_14

The Nobel Prize winner namely Simon (1979)[2] has contested and supported the argument that it is not possible to predict choices through models of optimal choice, arguing that any human decision-making enters necessarily in contact with psychological processes. He goes on to argue that only where there is a full automated choice, there is no human decision. Hence, it is argued that we have a case of a real automated choice in case where there is full automation, that is in case where we have the existence of the technology by which a process or procedure is performed without human assistance; nevertheless, automation usually implies the use of various control systems for operating with minimal or reduced human intervention, although some processes have been completely automated. Furthermore, Herbert Simon[3] prompts us to think of the cases of steering and stabilization of ships, aircraft, and other applications and vehicles where different levels of automation are possible.[4]

In addition, the On-Road Automated Vehicle Standards Committee, which has been established by the International Society of Automotive Engineers (SAE), along with experts from industry and government, has *inter alia* released an information report defining the key concepts, which are related to the increasing automation of on-road vehicles. Central to their lengthy report is the elaboration of the six levels of driving automation, as follows: 0 (no automation), 1 (driver assistance), 2 (partial automation), 3 (conditional automation), 4 (high automation), and 5 (full automation).[5] To define the cause of action in case of an automated choice, it is important to consider the above mentioned levels of automation.

---

the world. Responses about the first automation encounter are somewhat related to the age of the respondent, e.g., pneumatic versus digital control, and to urban versus farming childhood environment. The chapter concludes with several emerging trends in bioinspired automation, collaborative control and automation, and risks to anticipate and eliminate.

[2]See Simon (1979). Simon was one of the pioneers of modern-day scientific domains like artificial intelligence, information processing, decision-making, problem-solving, organization theory, and complex systems. He was among the earliest to analyze the architecture of complexity and to propose a preferential attachment mechanism to explain power law distributions. With Allen Newell, he creates the Logic Theory Machine (1956) and the General Problem Solver (GPS) (1957) programs. GPS is the first method developed for separating problem solving strategy from information about particular problems.

[3]*Id.*

[4]The table on automated vehicles is in Pierini (2018) and Pillath (2016).

[5]Smith (2013). Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is now-and has been for nearly a century-among the organization's primary provisions to those mobility industries it serves: aerospace, automotive, and commercial vehicle. Today's SAE standards product line includes almost 10,000 documents created through consensus standards development by more than 240 SAE Technical Committees with 450+ subcommittees and task groups. These works are authorized, revised, and maintained by the volunteer efforts of more than 9000 engineers, and other qualified professionals from around the world. Additionally, SAE has 60 US Technical Advisory Group (USTAG's) to ISO Committees. For additional information on the SAE Technical Standards Development Program, go to http://www.sae.org/standardsdev/.

Generally speaking, and not only concerning vehicles, we can distinguish the levels of automation as follows:

- at Level 1, the human operator acts and turns to the computer to implement;
- at Level 2, the computer helps the human operator by determining the available options;
- at Level 3, the computer suggests options and the human operator can choose to follow the recommendation;
- at Level 4, the computer selects the action and the human operator decides if it should be done or not;
- at Level 5, the computer selects the action and implements it, only if the human operator approves the selected action;
- at Level 6, the computer selects the action and informs the human operator who can cancel the action;
- at Level 7, the computer performs the action and informs the human operator;
- at Level 8, the computer performs the action and informs the human only if the human operator asks;
- at Level 9, the computer performs the action and informs the human operator only if the computer decides that the operator should be informed;
- at Level 10, the computer performs the action if it decides that it should be done. The computer informs the human operator only if it decides that the operator should be informed.

The definition of automation is strictly connected with the ethical and data protection profiles that we will deal with later. Now, it is clarified that the machine is able to make decisions that are autonomous from the actions and human omissions on the machine itself, and that break the causal link connecting human entities to possible damages committed by the machine. This affects the liability profile in case of violation of human rights, violation of rules of cybersecurity, etc.

The chapter therefore aims to consider the pros and cons of automation and the answers that the European legislator has given on two of the main threats of automation: ethical issues and data protection. It will be verified how these responses can be responsive to the concept of automation and to the different levels of artificial intelligence.

Therefore, conclusions will be made with respect to the current normative rules, considering that with the term "normative" is meant rules, guidelines, principles, and values. The variety of sources in this field and the presence of sources of the so-called Hard Law and of the so-called Soft Law are explained by the need to order a constantly evolving phenomenon that can hardly find orderly responses in strict application of law. The need for flexibility of legal solutions and resilience goes forward with respect to the demands of certainty. The uncertainty that is generated should find, on the other hand, a form of compensation in a "soft sanctioning system" aimed at ordering the elimination of the illicit conduct rather than striking the responsible subject. The output of a violation should not be a sanction but a

"cease and desist order" or a request for clarification, "complaint or explain", coming from the Public Authority.[6]

2 Information Processing and Automation

Parasuraman, Sheridan, and Wickens distinguish[7] different models of human information processing, as follows:

- sensory processing that refers to the acquisition and registration of multiple sources of information and includes the positioning and orienting of sensory receptors,
- sensory processing,
- initial pre-processing of data before full perception,
- selective attention.

This model can be translated in the function of information acquisition:

- Perception and/or working memory that regards conscious perception and manipulation of processed and retrieved information in working memory. It includes cognitive operations such as rehearsal, integration, and inference, but these operations occur before the decision. This model can be translated in the function of information analysis.
- Decision-making. It means a decision based on such cognitive processing. This model can be translated in the function of decision and action selection.
- Response selection that involves the implementation of a response or action consistent with the decision choice. This model can be translated in the function of decision and action implementation.

[6]Bauman (2006), p. 55 ff.

The book deals with the passage from 'solid' to 'liquid' modernity has created a new and unprecedented setting for individual life pursuits, confronting individuals with a series of challenges never before encountered. Social forms and institutions no longer have enough time to solidify and cannot serve as frames of reference for human actions and long-term life plans, so individuals have to find other ways to organize their lives. They have to splice together an unending series of short-term projects and episodes that do not add up to the kind of sequence to which concepts like 'career' and 'progress' could meaningfully be applied. Such fragmented lives require individuals to be flexible and adaptable—to be constantly ready and willing to change tactics at short notice, to abandon commitments and loyalties without regret and to pursue opportunities according to their current availability. In liquid modernity, the individual must act, plan actions, and calculate the likely gains and losses of acting (or failing to act) under conditions of endemic uncertainty.

[7]Parasuraman et al. (2000).

> The model can be used as a starting point for considering what types and levels of automation should be implemented in a particular system. The model also provides a framework within which important issues relevant to automation design may be profitably explored. Ultimately, successful automation design will depend upon the satisfactory resolution of these and other issues.

On the above-mentioned four functions, it is possible to provide an initial categorization for the types of tasks in which automation can support the human operator:

- Information acquisition: automation of information acquisition can be applied to the sensing and registration of input data.
- Information analysis: automation in this function involves cognitive functions such as working memory and inferential processes.
- Decision and action selection. The decision and action selection involve selection from among decision alternatives.
- Action implementation, which refers to the actual execution of the action choice.

According to the opinion of various scholars, automation should be human-centered; automation systems should be comprehensible; automation should ensure operators are not removed from command role; it should support situation awareness; it should never perform or fail silently; management automation should improve system management, and designers should assume that operators would become reliant on reliable automation.[8]

On the contrary, it is admitted that in case of full automation (Level 5), the machine through a self learning proceeding, via the elaboration of data in the cyberspace, can act autonomously. If the action or omission of the machine does not refer to a human action or omission we must say that, regarding the causation proceeding, we are in the presence of an irresistible force that is neither imputable to the user nor to the manufacturer.[9]

[8] Billings (1997), Calefato et al. (2008) and Endsley (1999).

[9] About the problem of "multi-agents" in case of automation see Teubner (2018), p. 155 ff; Teubner (2019). He stressed on the importance to determine a financial entity able to compensate victims.

A problem correlated to the present is the possibility to recognize subjectivity to automated machine. See European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)):

> General principles
>
> T. whereas Asimov's Laws(3) must be regarded as being directed at the designers, producers and operators of robots, including robots assigned with built-in autonomy and self-learning, since those laws cannot be converted into machine code;
>
> U. whereas a series of rules, governing in particular liability, transparency and accountability, are useful, reflecting the intrinsically European and universal humanistic values that characterise Europe's contribution to society, are necessary; whereas those rules must not affect the process of research, innovation and development in robotics;
>
> V. whereas the Union could play an essential role in establishing basic ethical principles to be respected in the development, programming and use of robots and AI and in the incorporation of such principles into Union regulations and codes of conduct, with the aim of shaping the technological revolution so that it serves humanity and so that the benefits of advanced robotics and AI are broadly shared, while as far as possible avoiding potential pitfalls; (...)
>
> Z. whereas, thanks to the impressive technological advances of the last decade, not only are today's robots able to perform activities which used to be typically and exclusively human, but the development of certain autonomous and cognitive features – e.g. the ability

On civil liability for damages caused by the machine, it will be possible that the action or omission does not refer to an act of man unless the act that is the source of responsibility is backdated to a moment before the commission of the illicit fact that is causally referred to the decision of the machine. It could be possible to establish a duty for the machine owner not to operate in full automation or the duty to ensure the ability to regain control of the machine in case there is a high level of alert for possible damage to third parties, or the duty to supervise the self-learning process of the machine. In this case, the liability of human beings is referred to the violation of the above-mentioned duties. A different solution, entails considering liable the owner independently from the presence of a causality nexus between the human action or omission and the damage could deform the function of civil liability: sanctioning a subject for the commission of facts that are not causally attributable to him could weaken the deterrent function of civil liability. Moreover, in the case of the so-called strict liability, the causality nexus is needed. It is only possible that the legislator dispenses the victim from the proof of the intentionality or of the negligence of the actor.[10]

From the point of view of insurance, we will have different effects:

---

to learn from experience and take quasi-independent decisions – has made them more and more similar to agents that interact with their environment and are able to alter it significantly; whereas, in such a context, the legal responsibility arising through a robot's harmful action becomes a crucial issue;

AA. whereas a robot's autonomy can be defined as the ability to take decisions and implement them in the outside world, independently of external control or influence; whereas this autonomy is of a purely technological nature and its degree depends on how sophisticated a robot's interaction with its environment has been designed to be;. . ."

See Borges (2018), p. 977 ff.

[10]Weinrib (1987), p. 407 ff.

The presence of an automated choice affects the process of determining the event and the effect of the choice. As we have seen, the interaction between algorithms and human action present different levels.

According to the theory of probability, the human agent can be held responsible for the action if it is proved that the action was caused with high probability by the human agent.

The problem is that such a vision does not consider the interaction between man and machine in causing the event.

If we take the hypothesis that a subject is acting using a semi-automated mechanism, where the computer selects the action and informs the human operator who can cancel the action and also pretend that the computer chooses an incorrect option and does not warn in time the person who is not able to intervene and avoid damage to third parties. It will not be enough to consider the probability that the computer error has caused the damage, but it will be necessary to verify that the user, in case of correct warning from the computer, would have acted differently.

Thus, we have a double counterfactual judgement: one concerning the human choice and another concerning the automated choice.

If it has been proven that the cause of the accident is the automated choice, it will still be necessary to consider whether the computer error is a production error or if the option chosen by the computer is linked to the combination of algorithms and to an evolution of such combination in a way that is autonomous from its own manufacturer.

- Accidents frequency will decline to where the difference among driving behaviors become negligible and it will be difficult to charge a meaningful premium for insurance;
- Insurance will take the form of commercial product liability instead of personal driver liability as the software will be let to the driving, and accidents could because of defect in the software production.[11]
- Insurance could also take the form of a property insurance instead of a motor insurance, as the cause of accident could not be the driver but the car itself, also in case of lack of defect in the production.
- Car connectivity simplifies the servicing of insurance policies. Using in-car telematics, insurers can offer additional services to motor insurance such as vehicle theft tracking, automated emergency calls, vehicle diagnostics, breakdown notification, fuel efficiency, safe driving tips, and so on.[12]
- Risk exclusions, shaped according to the new risks related to the increase of automation, and additional precautionary duties on policy holders to mitigate new risks.[13]

If the action or omission of the machine does not refer to a human action or omission we must say that, on the causation proceeding, we are in the presence of an irresistible force that is neither imputable to the user nor to the manufacturer.

The term "force majeure" is frequently used to indicate causes that are outside the control of the parties, such as natural disasters, that could not be evaded through the exercise of due care. Force majeure is a circumstance that no human foresight could anticipate or which, if anticipated, is too strong to be controlled. Depending on the legal system, such an event may relieve the parties from the obligation to compensate damage.

The term "force majeure" comes from French but with regard to the present meaning, it is important to remember the German concept of höhere Gewalt. According to German jurisprudence, there is a höhere Gewalt if the event causing the damage has an external effect and the harm caused cannot be averted or rendered harmless by the extremely reasonable care. However, it must be noted that the French force majeure is not identical with the German höhere Gewalt. See Blaschczok (1998) and Jansen (2003). See also the German BGH Urteil vom 21. 8. 2012 – X ZR 146/11.

[11] About this two point see Naylor (2017), pp. 175–185.

[12] *The future of Motor Insurance*, SwissRe Publications https://www.the-digital-insurer.com/wp-content/uploads/2016/05/737-HERE_Swiss-Re_white-paper_final.pdf.

[13] See CASUALTY ACTUARIAL SOCIETY, *Automated Vehicles and the Insurance Industry — A Pathway to Safety: The Case for Collaboration*, Spring 2018 53 https://www.casact.org/pubs/forum/18spforum/01_AVTF_2018_Report.pdf. The paper indicates the following risk:

> C1 - Driver Skill Deterioration: The more the technology is in control, the more out of practice individuals might become. Therefore, certain scenarios that individuals are able to handle today may result in an accident in the future. If the technology's ability increases at a faster rate than the driver's deteriorates, this may not pose much of a problem. However, manufacturers need to recognize the risk is dynamic. The situation needs constant monitoring as the risk minimization actions may change over time.
>
> C2 - Pass-Off Risk: This is the risk that is created when the vehicle goes from technological control back to human control. This scenario could be triggered by the human choosing to take control or by the vehicle passing responsibility to the individual when it encounters a scenario it is unable to handle.

3 Self Learning

To better understand the conclusions derived from the previous paragraph, it is necessary to clarify what is meant by "self learning machine". First, we need to distinguish between machine learning, self-learning, deep learning, and reinforcement learning.[14]

Machine learning is a subclass of artificial intelligence and gives a machine the ability to learn. The machine starts with a pre-programmed set of functions and procedures and can learn on its own, based on the data it acquires from the external environment, without having to be programmed further. Machine learning is based on the scientific study of algorithms and statistical models that computer systems use to effectively perform an activity without using explicit instructions from the human being, relying instead on patterns and inferences. Machine learning algorithms build a mathematical model of sample data ("training data"), which are used by the machine to make predictions or to make decisions without being explicitly

C3 - Other Driver Interaction: How other drivers, pedestrians, and bikers on the road react is also unknown. Drivers' reactions can change based on their age, driving experience, familiarity with the technology, their mood, or almost any other factor.

C4 - Animal Hits: While accidents involving animals are included in the NMVCCS, the dataset appears to be insufficient extrapolation. State Farm estimates that there are over 1.2 million deer-vehicle collisions annually; 33 however, the NMVCCS's extrapolated number of accidents involving animals is only 22,366 — or approximately 1.0 percent of all accidents. This could be due to NHTSA's requirement that a police report be filed to be included in the data, and claimants may be less inclined to call the police in a single vehicle animal hit. The risks animals pose to vehicles varies dramatically by location and time of year. It's also uncertain how the technology interacts with the animals. While it may be able to avoid some accidents, animals may be even more unpredictable than people. Residents in areas with significant animal populations will undoubtedly know someone who has had a deer run into the side of their car while driving. There's nothing that can be done in times like these.

C5 - Hacking: The introduction of more technology in the vehicle may increase the risk that vehicles will be hacked. In the future, the risk of hacking may increase regardless of the vehicle's automation.34 At this point, we do not know what hacking's causes or risk factors may be. Operating in a city may increase the risk by exposing other drivers to the hacked vehicle. It may also decrease part of the risk by reducing the average speed and enabling emergency response teams to respond more quickly. More research will be required to properly evaluate the risk.

C6 - Random Errors: As stated in our assumptions, technological errors will still occur. However, their appearance will be random. Therefore, it is important that when an incident occurs, its severity minimized.

C7 - Unknown: It's important to include a placeholder for unknown events. It's impossible to predict everything that will happen. Therefore, we must accept the fact that there are things that we don't know and cannot predict.

C8 - Incident Severity Risks: There are a number of factors that determine how severe an incident will be. By breaking the drivers into their respective risk components, we can create a risk management structure that minimizes severity of unpreventable incidents.

• Speed: The number one determinant of accident severity is the vehicle's speed.

[14]See Samuel (1959); Koza et al. (1996), pp. 151–170; Mitchell (1997), p. 2; Bishop (2006).

programmed to perform such activities. To give some examples we can remember that machine learning algorithms are used in e-mail filtering applications, in network intrusion detection, and in machine vision. Machine learning is strictly related to computational statistics or the possibility of making predictions using computers.

In-depth learning is a subclass of machine learning and consists of a broad spectrum of data learning algorithms.

Reinforced learning is also a machine learning subclass where human intervention is applied to algorithms. Feedback (reward) is used to teach the machine to optimize its performance. So human-machine interaction is necessary for this type of learning.

At this point, we can distinguish the supervised learning algorithms and those not supervised, where supervision does not necessarily imply a continuous interaction between human being and machine. Supervised learning algorithms build a mathematical model of a set of data that contains both the desired inputs and outputs. The "training data" consist of a series of training examples. Each training example has one or more inputs and a desired output or positive feedback, also known as a supervisory signal. Through iterative optimization of an objective function, supervised learning algorithms learn a function that can be used to predict the output associated with new inputs. An optimal function will allow the algorithm to correctly determine the output for inputs that were not part of the initial training data.

Unsupervised learning algorithms are not without any system of orientation in the correctness of the solutions, but they are algorithms that accept a set of data that contains only input and learn from test data that have not been labeled, classified or categorized. Instead of responding to feedback, non-supervised learning algorithms identify the common characteristics in the data and respond based on the presence or absence of such common elements in each new data.

From what has been said so far, we can see how the answers to the inputs of machines equipped with artificial intelligence systems may not depend on human interventions. Even the initial algorithms included in the programming phase can lead to the processing of unexpected answers because they are the result of independent processes. Decision-making processes vary according to the type of artificial intelligence and are distinct from human intelligence. Even the regulatory response aimed at regulating the conduits associated with the intervention of artificial intelligence must consider this level of autonomy of the machine by man and the ways of processing the responses to the inputs that the machine receives.[15]

[15]Bishop (2006).

4 Positive Impact of Automation

A research based on the SWOT analysis demonstrates the benefits of adopting automation systems in transport. The SWOT analysis (also known as the SWOT matrix) is a strategic planning tool used to evaluate strengths (Strengths), weaknesses (Weaknesses), opportunities (Opportunities) and Threats (T) of a project or in a company, etc. As stated by Acosta (2018), "Regulators and policymakers are increasingly involved in making important decisions about the governance of automated vehicles (AVs). Policymakers need to design comprehensive policies to deliver the benefits of AVs and to foresee and address potential unintended consequences; however, this is not an easy task. Especially given the complexity of the technology, AVs require a sophisticated analysis: beyond the apparent safety and security issues, AVs have significant potential to ECT issues related to privacy, accessibility, the environment, and land management".[16]

Road safety and social costs, as well known human errors, are believed to be responsible for over 90% of these accidents, primarily from causes like distracted driving, speeding, reckless driving, and driving under the influence, among others. Increased mobility and accessibility are considered as positive aspects enhanced via the use of AVs in that AVs can serve as a more convenient mode of transportation from point-to-point, especially for people unable to operate a vehicle manually including youngsters, people with certain disabilities, and the elderly. On environmental sustainability, AVs can help to improve environmental sustainability and could reduce CO2 emissions by 300 million tons per year, also because AVs will reduce traffic congestion.[17] Research conducted (2017) has suggested that AVs may increase worker productivity by 10–15% and save around 1 billion hours every day.[18] Certain technologies, such as Event Data Recorders (EDR), are being used by the NHTSA to investigate crashes and clarify civil liabilities earlier, which may reduce litigation costs.[19] On the other hand, one needs to consider the threats imposed, such as the ethical issues entailed concerning the values that the machine should consider in any decision it will make and the related cybersecurity issues, given that AVs will be connected to a network, and thus more exposed to cybersecurity threats.

The opportunities related to AVs have been considered by European legislator. On 17 May 2018, the European Commission published the Communication

[16]Acosta (2018).

[17]Business insider, The 3 biggest ways self-driving cars will improve our lives, (June 2016), http://www.businessinsider.com/advantages-of-driverless-cars-2016-6/#traffic-and-fuel-efficiency-will-greatly-improve-2.

[18]Digital Transformation Monitor, Autonomous cars: a big opportunity for European Industry, (2017), https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Autonomous%20cars%20v1.pdf, 5.

[19]NHTSA, Event Data Recorder, https://www.nhtsa.gov/research-data/event-data-recorder.

283/2018,[20] with the goal relating to automated mobility. The Commission intends to develop the Galileo services and related vehicle navigation technologies for driverless mobility. Galileo is an asset for precise and secured positioning and for the integrity and reliability of digital maps. A further study has been launched in 2018 to investigate the question of integrity and reliability of digital maps. The Commission therefore intends to propose that the research on cooperative, connected, and automated mobility remains a priority in the next Framework Program for Research and Innovation. The Commission underlined that the current EU support will need to be sustained in the long term as the EU is still some way from deploying fully automated and connected vehicles and the related infrastructure. Hence, it seems that the European Legislator is also willing to consider the above-mentioned threats related to AVs.

5 Ethical Issues and Data Protection

Digitalization offers huge potential for economies and societies, but it is important to consider its impact on human rights and find solutions to permit at the same time the development of automated and connected autonomous vehicles and driving systems (CAVs) and the improvement of human rights protection. As CAVs technologies evolve towards complete automation, governments and commercial organizations make increasing use of big data for diverse purposes, including: regulation of traffic, environmental protection, security and law and order, as well as commercial exploitation. The ethical principles, regulatory standards, rules and guidelines applicable to vehicle manufacturers, software designers, insurers and local and central government authorities will have a wider application.

Laws forbid discrimination based on features such as race, gender, and sexuality. Yet, social media and related applications (e.g., Google maps, etc.) can be used to retrieve information, and hence filter out prospective assureds who will act as users (i.e., drivers and/or passengers) of CAVs, in relation to their driving habits or if a computer algorithm judges them to be socially undesirable. Such regulatory gaps have always existed and will continue to exist because laws are abstract and have not kept up with the advances in technology. The gaps are getting wider as technology advances ever more rapidly in every domain that technology touches. Some argue that is how it must be, because law is, at its best and most legitimate, a form of codified ethics.

Effective laws and standards of ethics are guidelines accepted by members of a society, and that these require the development of a social consensus, hence our laws and ethical practices have evolved over centuries. Today, however, technology is on

[20]COM(2018) 283 final "From the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions- On the road to automated mobility: An EU strategy for mobility of the future".

an exponential curve and is touching practically everyone and everywhere, but may be, we neither realize nor are we fully aware of its actual scope and consequences in our current, mid-term, and long-term life. We have yet to come to a social consensus on how private data can be collected and shared. We have not come to grips with what is ethical, let alone with what the laws should be, in relation to technologies such as social media and related applications (e.g., Google maps, etc.).

Motor insurers will be interested in all the data generated and transmitted via telemetry—the use of small on board computers that gather data and transmit it to insurers via a SIM card. As telematics develops, more data produced by different parts of the vehicle can be fed back to a central server: average speed, rates of acceleration and deceleration; speeds measured against the speed limits in a particular area, so that location-tracking can now determine whether and how often speed limits are being broken, and so on. As more devices are connected to the internet, more data will be generated, aggregated, and analyzed to discern, with ever-increasing precision, their user's risk profile. It has become empirically clear that insurance companies are some of the biggest consumers of Big Data profiling and are increasingly using that data in deciding whether to offer cover to individual potential insureds or not.

The use of AVs must be compliant with ethical constraints related to the importance of the ethics of AI's choices, which need to conform to ethical values. If we think of the following dilemma, i.e., in the case where damage is unavoidable and a choice must be made by the vehicle about choosing who will unavoidably have to be hit or killed by the automated car, i.e., whether the driver or a pedestrian, an adult pedestrian or a child, etc.

The High-Level Expert Group on Artificial Intelligence, which was appointed by the Commission in June 2018, released the first draft of its Ethics Guidelines for the development and use of artificial intelligence (AI). In this document, via the guidelines issued, an independent group of 52 experts coming from academia, business and civil society, sets out how developers and users can make sure AI respects fundamental rights, applicable regulation and core principles, and how the technology can be made technically robust and reliable.[21]

[21] https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai.

As said in the introduction to the Guidelines: "This working document constitutes a draft of the AI Ethics Guidelines produced by the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), of which a final version is due in March 2019.

Artificial Intelligence (AI) is one of the most transformative forces of our time, and is bound to alter the fabric of society. It presents a great opportunity to increase prosperity and growth, which Europe must strive to achieve. Over the last decade, major advances were realised due to the availability of vast amounts of digital data, powerful computing architectures, and advances in AI techniques such as machine learning. Major AI-enabled developments in autonomous vehicles, healthcare, home/service robots, education or cybersecurity are improving the quality of our lives every day. Furthermore, AI is key for addressing many of the grand challenges facing the world, such as global health and wellbeing, climate change, reliable legal and democratic systems and others expressed in the United Nations Sustainable Development Goals.

The Experts focus on the human-centric approach to AI. In essence, what this implies is that the development and use of AI should not be seen as a means in itself, but as having the only goal to increase human well-being. The Experts in their Guidelines talk about "Trustworthy AI", meaning that human beings will only be able to confidently and fully reap the benefits of AI if they can trust the technology.

Trustworthy AI has two components: (1) it should respect fundamental rights, applicable regulation and core principles and values, ensuring an "ethical purpose"; and (2) it should be technically robust and reliable since, even with good intentions, a lack of technological mastery can cause unintentional harm.

The achievement of Trustworthy AI is founded on the field of ethics. The goal of AI ethics is to identify how AI can raise concerns to the good life of individuals, in terms of quality of life, mental autonomy, or freedom to live in a democratic society.[22]

The High-Level Expert Group on AI ("AI HLEG") use the fundamental rights commitment of the EU Treaties and Charter of Fundamental Rights as the polar star to identify abstract ethical principles, and to specify how concrete ethical values can be operationalized in the context of AI. After all, the EU is founded and based on a constitutional commitment to protect the fundamental and indivisible rights of human beings, ensure respect for rule of law, foster democratic freedom and promote the common good. The AI HLEG prefer a rights-based approach to AI ethics because it brings the additional benefit of limiting regulatory uncertainty. Building based on decades of consensual application of fundamental rights in the EU provides clarity, readability, and prospectiveness for users, investors, and innovators.

Having the capability to generate tremendous benefits for individuals and society, AI also gives rise to certain risks that should be properly managed. Given that, on the whole, AI's benefits outweigh its risks, we must ensure to follow the road that maximises the benefits of AI while minimising its risks. To ensure that we stay on the right track, a human-centric approach to AI is needed, forcing us to keep in mind that the development and use of AI should not be seen as a means in itself, but as having the goal to increase human well-being. Trustworthy AI will be our north star, since human beings will only be able to confidently and fully reap the benefits of AI if they can trust the technology.

Trustworthy AI has two components: (1) it should respect fundamental rights, applicable regulation and core principles and values, ensuring an "ethical purpose" and (2) it should be technically robust and reliable since, even with good intentions, a lack of technological mastery can cause unintentional harm.

These Guidelines therefore set out a framework for Trustworthy AI:

- Chapter I deals with ensuring AI's ethical purpose, by setting out the fundamental rights, principles and values that it should comply with.
- From those principles, Chapter II derives guidance on the realisation of Trustworthy AI, tackling both ethical purpose and technical robustness. This is done by listing the requirements for Trustworthy AI and offering an overview of technical and non-technical methods that can be used for its implementation."
- Chapter III subsequently operationalises the requirements by providing a concrete but non-exhaustive assessment list for Trustworthy AI. This list is then adapted to specific use cases.

[22] https://ec.europa.eu/digital-single-market/en/news/have-your-say-european-expert-group-seeks-feedback-draft-ethics-guidelines-trustworthy.

An example illustrated by the AI HLEG is as follows: "To give an example of the relationship between fundamental rights, principles, and values let us consider the fundamental right conceptualized as 'respect for human dignity'. This right involves recognition of the inherent value of humans (i.e. a human being does not need to look a certain way, have a certain job, or live in a certain country to be valuable, we are all valuable by virtue of being human). This leads to the ethical principle of autonomy which prescribes that individuals are free to make choices about their own lives, be it about their physical, emotional or mental wellbeing (i.e. since humans are valuable, they should be free to make choices about their own lives). In turn, informed consent is a value needed to operationalize the principle of autonomy in practice. Informed consent requires that individuals are given enough information to make an educated decision as to whether or not they will develop, use, or invest in an AI system at experimental or commercial stages (i.e. by ensuring that people are given the opportunity to consent to products or services, they can make choices about their lives and thus their value as humans is protected)".[23]

From this example used by AI HLEG, it is evident that the relationship between rights, principles, and values is based on the pillar that the AI fundamental rights provide the basis for the formulation of ethical principles. Those principles are abstract high-level norms that users and regulators should follow to uphold the purpose of human-centric and Trustworthy AI. Such values provide a more concrete guidance, on how to uphold ethical principles, while also underpinning fundamental rights.

Among the human rights affected by AI there are:

- Respect for human dignity based on the idea that every human being has an "intrinsic value" that can never be diminished, compromised, or removed by others. All people are treated with respect because they are individuals, rather than simply as "subjects carrying data". Artificial intelligence can also have a propulsive function of human dignity. Artificial intelligence systems can be developed in a way that protects both the physical and the moral integrity of human beings, the personal and cultural sense of identity, and the satisfaction of their essential needs. This aspect is particularly important in the context of AVs, as these can help the circulation of people who could not drive a vehicle that is not automated because of their disability or old age.
- Freedom of the individual. Human beings should remain free to make decisions about their lives.
- Respect for democracy, justice, and the rule of law. It means that political power is human centric and bounded.
- Equality, non-discrimination, and solidarity including the rights of persons belonging to minorities. In a context of artificial intelligence, equality implies that the same rules should apply to all to access information, data, knowledge,

[23] https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai.

markets, and an equitable distribution of the benefits generated by technologies. Data processing should not allow discrimination from profiling results.
- Citizens' rights in their interaction with the public sector. IA systems have the potential to improve the scale and efficiency of the government in the provision of public goods and services to society. At the same time, citizens should have the right to be informed of any automated processing of their data.

Moreover, for the alignment of AI to the values of the democratic systems, study groups have tried to identify supranational principles that can mitigate the threats of the AVs. In the EU, the European Group on Ethics in Science and New Technologies ("EGE") proposed a set of nine basic principles, based on the fundamental values laid down in the EU Treaties and in the EU Charter of Fundamental Rights. More recently, the AI4 People's project5 has surveyed the aforementioned EGE principles, as well as 36 other ethical principles put forward to date, and subsumed them under four overarching principles. These include:

- beneficence (defined as 'do good'): AI systems should be designed and developed to improve individual and collective wellbeing;
- non-maleficence (defined as 'do no harm'): by design, AI systems should protect the dignity, integrity, liberty, privacy, safety, and security of human beings in society and at work;
- autonomy (defined as 'respect for self-determination and choice of individuals'): Human beings interacting with AI systems must keep full and effective self-determination.
- justice (defined as 'fair and equitable treatment for all'): Developers and implementers need to ensure that individuals and minority groups maintain freedom from bias, stigmatization, and discrimination. Additionally, the positives and negatives resulting from AI should be evenly distributed;
- technological transparency, which implies that AI systems be auditable, comprehensible, and intelligible by human beings at varying levels of comprehension and expertise.[24]

6 ENISA'S Study on Information Security

Another threat of AVs is cybersecurity. The European Commission focuses on the importance of non-personal data sharing while protecting cybersecurity and on the importance of fostering vehicle connectivity for automation. Hence, on 13 September 2017, the Commission adopted a cybersecurity package including a proposal for a voluntary certification framework of information and communication technology (ICT) products and services. The Guidelines have been developed in the framework of the United Nations for the protection of vehicles against cyberattacks and it is the

[24]Beauchamp (2001); Floridi et al. (2018), pp. 689–707.

intention of the Commission to implement these guidelines in the EU vehicle rules. In this contest, the Commission has published guidance on the certificate and security policy needed for secure and trustful communication between vehicles and infrastructure for road safety and traffic management related messages.

On safety on the roads and victims compensation, the European Commission's position is that on the compensation of victims, the Motor Insurance Directive already provides for a quick compensation of victims including where an automated vehicle is involved. The insurer can then take legal action against a vehicle manufacturer under the Product Liability Directive if there is a malfunction/defect of the automated driving system. The European Commission has also evaluated the Product Liability Directive and as a follow-up, intends to issue an interpretative guidance clarifying important concepts in the Directive including in the light of technological developments.

The European Union Agency for Network and Information Security (ENISA) was established in 2004. The Agency provides advice and recommendations, data analysis, and supports awareness raising and cooperation by the EU bodies and Member States in the field of cybersecurity.

The European Union Agency for Network and Information Security (ENISA) has a key role to play. The Commission presents an ambitious reform proposal, including a permanent mandate for the agency to ensure that ENISA can provide support to Member States, EU institutions, and businesses in key areas, including the implementation of the NIS Directive.

The growth of the cybersecurity market in the EU—in terms of products, services, and processes—is held back in a number of ways, also because of lack of a cybersecurity certification scheme recognized across the EU. The Commission is therefore putting forward a proposal to set up an EU certification framework with ENISA at its heart. It is therefore necessary to implement the NIS directive (Directive on security of network and information systems).

In January 2018, ENISA published a study on the "Cyber security and resilience of smart cars".[25] The report identifies good practices and recommendations to ensure the security of smart cars against cyber threats. The report lists the assets present in smart cars, as well as the corresponding threats, risks, attack scenarios, mitigation factors and possible security measures to implement. Smart cars subject matter experts were contacted to reflect the needs of Europe's automotive cyber security stakeholders. The results are further aligned with the C-ITS Platform run by DG MOVE, to synergize efforts and the input from the ENISA Cars and Roads SECurity (CaRSEC) Expert Group to finalize the results.

The study suggests the following recommendations, to increase cyber security in smart cars in Europe:

- Improve information sharing amongst industry actors;
- Achieve consensus on technical standards for good practices;
- Clarify cyber security liability among industry actors.

[25] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/.

ENISA's future work in the field aims in enhancing the security and resilience of road transport in Europe together with all relevant key stakeholders and agencies. In the context of the NIS Directive and smart mobility, ENISA will assist Member States and the European Commission by providing expertise and advice, as well as developing and facilitating the exchange of good practices, with the ultimate goal of enabling higher level of security for Europe's road transport infrastructure.[26]

7 Conclusion

In the studies of the European Commission and ENISA's, it seems that the main objective is that of technological neutrality and of the incentive of technology and automation. These are considered to be fundamental tools to reduce the risk of accidents.

The attention to the security of the cybernetic space is considered taking into account the possible human actions and omissions.

In terms of liability for breaches of personal data security, the focus has been as having regard only to human actions or omissions, in particular in relation to actions or omissions of the owner or user of the vehicle, of the manufacturer of the vehicle and/or of the programmer, in case of defects in the IT system.

The European legislator therefore intervened in redefining the contents of privacy in terms of "data protection" and the precautionary principle. Regulation 679/2016 introduces rules of conduct aimed at avoiding violations of personal data: unauthorized disclosure and processing, destruction of data.The European legislator deals with automation only in the part in which it regulates the possibility of using personal data for profiling and automated choices. Art. 22 of the GDPR stipulates that 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. Such a provision is valid only if: (a) it is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) it is authorized 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) it is based on the data subject's explicit consent.

The European legislator is also concerned with revising the producer responsibility directive to introduce rules that can regulate defects in artificial intelligence systems. In 2019, the Commission will issue guidance on the Product Liability Directive and a report on the broader implications for, potential gaps in and

[26] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/.

orientations for, the liability and safety frameworks for artificial intelligence, the Internet of Things and robotics.[27]

It seems that the European legislator, however, does not sufficiently consider the problem related to the possible "autonomy of automated machines" that can, as said, make autonomous choices by learning and re-elaborating the data available to them. The automated machines through "self learning machine"[28] processes are able to feed their acquaintance with the data they find in the environment and elaborate their knowledge on the basis of which they will make their choices. In our view, the consequences of these choices are difficult to refer to the owner, the driver, or the manufacturer. Generally, they are difficult to refer to human beings unless the legislator introduces rules that refer responsibility to a specific person, for instance, the owner of the machine.

In German law, a new provision, i.e. § 1a StVG (Straßenverkehrsgesetz the German law on motor liability) on "Motor vehicles with highly or fully automated driving function"[29] has been introduced on 16 June 2017. Under German law, the liability of the car owner as in § 7 StVG, in the case of autonomous vehicle, remains unaffected anyway, since the owner is liable for all damage that can be referred to

[27] https://ec.europa.eu/growth/single-market/goods/free-movement-sectors/liability-defective-products_en.

[28] Murphy (2012).

[29] § 1a Motor vehicles with highly or fully automated driving function

(1) The operation of a motor vehicle by means of highly or fully automated driving function is permitted if the function is used as intended.
(2) Motor vehicles with highly or fully automated driving function within the meaning of this Act are those which have technical equipment,
1. To control the driving task - including longitudinal and transverse guidance - the respective motor vehicle after activation control (vehicle control),
2. which is able to comply with traffic regulations directed at vehicle guidance during highly or fully automated vehicle control,
3. which can be manually overridden or deactivated by the driver at any time,
4. can recognize the necessity of the vehicle hand control by the driver,
5. the driver can visually, acoustically, tactually or otherwise perceptibly display the requirement of the autograph vehicle control with sufficient reserve of time before the vehicle control is delivered to the driver, and
6. indicates use contrary to one of the system descriptions.

The manufacturer of such a motor vehicle must declare in the system description that the vehicle complies with the requirements of sentence 1.

(3) The preceding paragraphs shall only be applied to vehicles which are approved in accordance with § 1 (1), which comply with the requirements of paragraph 2 sentence 1 and whose highly or fully automated driving functions
1. are described in, and comply with, international regulations applicable in the scope of this Act; or
2. a type-approval pursuant to Article 20 of Directive 2007/46 / EC of the European Parliament and of the Council of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles (Framework Directive) (OJ L 263, 9.10.2007)

"operation of a motor vehicle". Hence, it is just an additional liability of the motor vehicle driver. For this purpose, the new norm contained in § 1a StVG stipulates that the user must remain receptive to be able to take control immediately.[30]

In fact, under § 1a, an automated vehicle shall be manually overridden or deactivated by the driver at any time; shall recognize the necessity of the vehicle hand control by the driver; shall visually, acoustically, tactually or otherwise discernibly indicate to the vehicle driver the requirement of the vehicle hand control with sufficient time reserve before the vehicle control is delivered to the vehicle driver.[31] German norms refer only to the liability in case of car accidents, but similar problems arise in case of liability for violation of data. Who is liable in case of lack of cybersecurity according to the GDPR? The owner of the machine? The producer in case of machines that are not defective? These are all questions that remain to be legally explored.

On data protection, we have to consider another problem. The machines will be the main holders and data transmitters because automation requires it. We believe that it is appropriate to focus on these aspects and on the ethical issues (to respect human rights, prohibition of discriminations, including the right to privacy and autonomy), and on the possibility that the machines acting independently will have access to enormous number of personal data. They will enable the making of appropriate choices to govern situations better than human beings. Such a scenario may seem futuristic, but perhaps it is time wise much closer than we can imagine.

In our view, this is a good point to include and to emphasize the "dilemma issue". Once ethical standards are established and their form and binding force is clarified, they must have necessarily an impact on deciding and potentially excluding liability. The relationship of traditional civil law notions and principles, such as *vis maior*, etc. to the ethical standards ("codified" answers to the dilemma-situations) must be fixed to achieve the predictability of the law. The legal system cannot send different messages (to motor vehicle manufacturers, software developers, AV owners, etc.) on behavioral standards and on the expectations of society concerning these dilemma-situations.

(4) Driver is also the one who activates a highly or fully automated driving function referred to in paragraph 2 and used for vehicle control, even if he does not control the vehicle in the context of the intended use of this function.

[30]See Greger (2018), p. 1.

[31]Channon (2016), p. 33. He underlines regarding EU law that: "It is submitted that an overall EU wide approach is needed for autonomous vehicles and this should be considered as soon as possible. The Motor Insurance Directives have sought to remove any barriers to trade by harmonizing key aspects of the law of Motor Insurance to protect free movement. Differing laws on autonomous insurance and liability will almost certainly constitute a significant barrier to movement as Member States will almost certainly introduce differing laws and regulations and will almost certainly answer the above questions in relation to liability in different ways".

See also Merkin et al. (2017).

A legislator who wants to order a social reality populated by artificial intelligence capable of acting in full autonomy must find answers not in juridical instruments relative to human reality, but in instruments that consider how the AI learns and decides. The order affected by an illicit fact caused by AI cannot be recovered through the ordinary sanctioning instruments but by intervening on the decisional processes of the AI and preventing possible default when possible, for example, it should intervene with the forms of supervised learning so that the outputs are increasingly conforming to the values.

In these terms, it is important, as underlined in the last part of the Draft of Guidelines of the AI HLEG, the respect of transparency in the algorithms and in the data on which the machine self-learning is built and a continuous evaluation that also leads to improve and (re) build the AI system according to the assessment.[32]

[32]See par. 3. In this term it is useful the last chapter of AI HLEG's guidelines (https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai) ordered to operationalise the implementation and assessment of the requirements of Trustworthy AI set out above, throughout the different stages of AI development and use. The assessment should circular " where the assessment is continuous and no step is conclusive (cfr. Figure 3 above). It will include specific metrics, and for each metric key questions and actions to assure Trustworthy AI will be identified. These metrics are subsequently used to conduct an evaluation in every step of the AI process: from the data gathering, the initial design phase, throughout its development and the training or implementation of the AI system, to its deployment and usage in practice. This is however not a strict, delineated and execute-once-only process: continuous testing, validation, evaluation and justification is needed to improve and (re-)build the AI system according to the assessment".

With regard to the "method of building the algorithmic system:

- In case of a rule-based AI system, the method of programming the AI system should be clarified (i.e. how they build their model)
- In case of a learning-based AI system, the method of training the algorithm should be clarified. This requires information on the data used for this purpose, including: how the data used was gathered; how the data used was selected (for example if any inclusion or exclusion criteria applied); and was personal data used as an input to train the algorithm? Please specify what types of personal data were used.

Method of testing the algorithmic system:

- In case of a rule-based AI system, the scenario-selection or test cases used in order to test and validate their system should be provided
- In case of a learning based model, information about the data used to test the system should be provided, including: how the data used was gathered; how the data used was selected; and was personal data used as an input to train the algorithm? Please specify what types of personal data were used.

Outcomes of the algorithmic system

- The outcome(s) of or decision(s) taken by the algorithm should be provided".

References

Acosta AJ (2018) Smart move? 24 Essentials of a SWOT analysis policymakers need to consider, Policy Paper on Autonomous Vehicles, https://cyber.harvard.edu/publication/2018/smart-move-24-essentials-swot-analysis-policymakers-need-consider

Bauman Z (2006) Liquid times: living in an age of uncertainty. Polity, Cambridge

Beauchamp TL (2001) Childress JF. Principles of biomedical ethics, 5th edn. Oxford University Press, Oxford

Billings CE (1997) Aviation automation: the search for a human-centered approach. Lawrence Erlbaum Associates Publishers, Mahwah

Bishop CM (2006) Pattern recognition and machine learning. Springer, Berlin

Blaschczok A (1998) Gefährdungshaftung und Risikozuweisung. Heymanns, Cologne

Borges G (2018) Rechtliche Rahmenbedingungen für autonome Systeme. NJW 71(14):977 ff

Calefato C, Montanari R, Tesauri F (2008) The adaptive automation design. Human computer interaction: new developments, the human factors and ergonomics society. Web. http://www.hfes-europe.org/wp-content/uploads/2014/06/Save.pdf

Channon M (2016) Autonomous vehicles and legal effects: some considerations on liability issues. DIMAF 1:33

Endsley MR (1999) Level of automation effects on performance, situation awareness and workload in a dynamic control task. Ergonomics 42(3):462–492. North Carolina State University. http://people.engr.ncsu.edu/dbkaber/papers/Endsley_Kaber_Ergo_99.pdf

Floridi L, Cowls J, Beltrametti M, Chatila R, Chazerand P, Dignum V, Luetge C, Madelin R, Pagallo U, Rossi F, Schafer B, Valcke P, Vayena EJM (2018) AI4People —an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. Minds Mach 28(4):689–707

Greger R (2018) Haftungsfragen beim automatisierten Fahren. Zum Arbeitskreis II des Verkehrsgerichtstags. NVZ 33:1

Jansen N (2003) Die Struktur des Haf-tungsrechts. Mohr Siebeck, Heidelberg

Koza JR, Bennett FH, Andre D, Keane MA (1996) Automated design of both the topology and sizing of analog electrical circuits using genetic programming. In: Artificial Intelligence in Design'96. Springer, Berlin, pp 151–170

Merkin R, Noussia K, Bevan N (2017) University of exeter – written evidence (AUV0044), driverless vehicles – where are we going wrong?. In: Connected and Autonomous Vehicles: The future?, House of Lords Report, http://www.maritimeindustries.org/write/Uploads/Resources/Consultations/Connected_and_Autonomous_Vehicles,_The_future_HoL_Report.PDF

Mitchell T (1997) Machine learning. McGraw Hill, New York, p 2

Murphy KP (2012) Machine learning a probabilistic perspective. The MIT Press, Cambridge

Naylor M (2017) Insurance transformed. Technological disruption. Palgrave, Basingstoke, pp 175–185

Nof SY (2009) Automation: what it means to us around the world. In: Nof SY (ed) Springer handbook of automation. Springer, Berlin, pp 13–52

Raja Parasuraman, Sheridan Thomas B, Wickens Christopher D (2000) A model for types and levels of human interaction with automation, https://www.ida.liu.se/~729A71/Literature/Automation/Parasuraman,%20Sheridan,%20Wickens_2000.pdf

Pierini M (2018) Veicoli automatici L'importanza di dare un significato ad un termine ormai noto, in https://cesifin.it/wp-content/uploads/2018/02/Pierini_02-02-18.pdf

Pillath S (2016) Automated vehicles in the EU. European Union, Strasbourg. Available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/573902/EPRS_BRI(2016)573902_EN.pdf, 10. 12. 2018

Samuel AL (1959) Some studies in machine learning using the game of checkers. IBM J Res Dev 44:1.2

Simon HA (1979) Models of thought. Yale University Press, New Haven

Smith BW (2013) SAE levels of driving automation
Teubner G (2018) Digitale Rechtssubjekte? Zum privatrechtlichen Status automoner Softwareagenten. AcP 54:155–205
Teubner G (2019) In: Femia P (ed) Soggetti giuridici digitali? Sullo status privatistico degli agenti software antonomi. Edizioni Scientifiche Italiane, Naples
Weinrib EJ (1987) causation and wrongdoing. Chicago-Kent Law Rev 63:407 ff

A New Era, a New Risk! "A Study on the Impact of the Developments of New Technologies in the Shipping Industry and Marine Insurance Market"

Julia Constantino Chagas Lessa and Belma Bulut

1 Introduction

Current technological developments have brought the shipping industry into the era of digital shipping. Today, it is possible to monitor and control sea traffic, navigate with automated navigation systems (e.g. GPS—Global Positioning System, AIS—Automatic Identification System), ECDIS—Electronic Chart Display and Information System), and track the location of ships and cargoes in real time. As shipping technology has been developing at a fast pace, unmanned and autonomous ships, drones, as well as smart containers, are becoming an ever more feasible reality. Indeed, the industry has never been more technically advanced not only because of the new forms of advanced vessels and offshore unit but throughout the entire shipping logistic chain, from operational offices to port, contractors and commercial partners.

Nevertheless, practical developments often bring new risks attached to them and accordingly the necessity of creating a new regulatory framework to accommodate these. The more sophisticated the industry developments are, the more sophisticated

The author is indebted to the Institute of Maritime Law of the University of Southampton for the opportunity given to her to use its library as a visiting researcher.

J. Constantino Chagas Lessa (✉)
Erasmus University Rotterdam, Rotterdam, Netherlands

Institute of Maritime Law, University of Southampton, Southampton, UK
e-mail: lessa@law.eur.nl

B. Bulut
Department of Maritime Safety and Security, Gendarmerie and Coast Guard Academy, Ankara, Turkey

Institute of Maritime Law, University of Southampton, Southampton, UK
e-mail: bb1d11@southamptonalumni.ac.uk

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_15

policies seem to be necessary. A major cyber attack causing notable loss of or damage to life and property is predicted to occur between now and 2025.[1] Considering the significance of shipping in the world trade and economy, the shipping sector would become the target of such a major cyber attack, and it is questionable if the shipping industry as stands, known for its traditional roots and resilience to untraditional changes, is prepared, both in management and regulatory aspects, to such a risk attached to these recent technological progresses.

Undoubtedly, the increased use of and reliance on technology in trade has made the shipping sector vulnerable to cyber attacks. Indeed, significant weaknesses have been identified in the cybersecurity of critical technology used for navigation at sea. GPS, AIS, and ECDI, as mentioned above, essential aids to navigation, have been identified as potentially vulnerable to attack. Since July 2017, the US Maritime Administration posted various reports of incidents caused by GPS disruptions or interference resulting in either inaccurate positions or no positions at all because of jammed, lost or altered GPS signals.[2]

The recent cyber attack in one of MAERSK' ports clearly demonstrated the devastating effect that these might have, even in one of the largest and most solid shipping company in the world. The attack confirmed that irrespective of how big or small, any shipping stakeholder is susceptible to cyber attacks, which, as it was evidenced by the above example, will likely generate financial loss, business disruption, reputational damages and so forth. The more digitalised the shipping sector, the more it will encounter cyber threats, such as attacks on navigation, communication, propulsion and machinery control systems, cargo management and remote control systems and programmes.

Given the potential risks arising out of cyber attacks and their possible impacts on businesses, shipping stakeholders inarguably need proper cyber risk insurance policies. At the moment, most traditional marine insurance policies are silent on cyber risk whereas others expressly exclude cyber risk from its coverage, such as hull covers by the CI.380 exclusion. There are a limited number of standalone cyber insurance policies available. However, these are unlikely to cover all potential risks arising from cyber attacks as their scopes are generally limited to financial and reputational risks. The fact is that because of lack of understanding on the extent of cyber risks, being this is a new threat with new risks emerging on a regular basis, it is not easy for companies to produce truly efficient plans and procedures for cyber risk managements and much less for insurers to provide efficient coverages, which will not expose unrestrictive liabilities.

Moreover, to steer the issue even further, it can and it has been questioned whether an autonomous/unmanned vessels comes within the current definition of a ship according to the current *lex maritime*, with numerous papers being written in the

[1]P Tucker, 'Major Cyber Attack Will Cause Significant Loss of Life by 2025, Experts Predict' (2014) www.defenseone.com/threats/2014/10/cyber-attack-will-cause-significant-loss-life-2025-experts- predict/97688/ accessed 01/04/2018.

[2]US Department of Transportation, MARAD www.marad.dot.gov/office-of-security/msci/alert/2018/ accessed 15/09/2018.

subject including the publication of a Comite Maritime International (CMI) position paper on unmanned vessels and the establishment of a working group to deal with the topic. Nevertheless, even if it is established that autonomous and unmanned vessels are indeed ships, the question that follows relates to the obligation of owners to provide a seaworthy vessel at the commencement of the voyage. Currently, The Hague-Visby Rules, as well as the Marine Insurance Act 1906 for instance, provided that such obligation includes, amongst other requirements, the maintenance of properly trained crew, a task which is clearly not possible for an autonomous vessel upon a strict interpretation.

This paper aims to address different types of cyber attacks, the effects of these in marine insurance, especially in terms of cargo claims and the current security given to ship industry stakeholders in the face of these type of attacks. Nevertheless, to achieve this, the chapter will start with the basic, but unavoidable discussion, if autonomous and unmanned vessels can be considered ships, followed by a short discussion about general insurance issues raised by the use of such vessels, after which, focuses will be given to the concept of cyber attack; which types of attack fall into the scope of cyber attack and which do not; secondly, assesses the possible extent of cyber risk by analysing the core issues such as risk assessment and management. This paper will present the current position under marine insurance policies and provide some suggestions on how cyber attacks would be properly insured thereunder. Finally, this chapter will concurrently address issues such as liability of the crew in case of autonomous vessel, the cyber attack falling in the category of piracy and if as such could be considered a peril of the sea, among others.

2 Meaning and Scope of the Term "Cyber Attack"

The first challenge in tackling marine insurance problems arising from cyber attack is to understand the meaning and scope of the term "cyber attack". After the use of computer network, internet and communication technologies, the history of cyber attacks began in the late 1980s, yet there is still not an internationally accepted definition for the term "cyber attack".

A dictionary definition states that cyber attack is "an illegal attempt to harm someone's computer system or the information on it, using the internet".[3] A similar definition can be found in the Memorandum of the United States Cyber Command, which defines the term "cyber attack" as "a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions".[4] Furthermore, in the UK's National Cyber

[3]Cambridge Dictionary Online https://dictionary.cambridge.org/dictionary/english/cyberattack accessed 15/09/2018.

[4]JE Cartwright, 'Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations'

Security Strategy 2016–2021, the term "cyber attack" is defined as "deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm".[5] From those definitions it could be stated that an attack could only be treated as cyber attack when it takes place in cyberspace, namely in computer and network systems and when there is an intention to cause harm.

Those definitions focus on the objectives and restrict the scope of the term "cyber attack" only to deliberate actions. However, there might be cases where the attackers do not intent to cause any harm. For instance, without any intention to cause harm, a person may access a ship's computer system or cargo management system by mistake or just for fun or to test its skills and capabilities. Assuming that because of such an access, some data is lost, altered or compromised. Is this action qualified as cyber attack or not? Pursuant to the definitions that focus on the deliberate actions, i.e. intention to harm, such as the abovementioned definitions, it is argued that such an action is not qualified as cyber attack. Even the Morris Worm, which is known as the very first attack, did not meet the criteria of intending to harm.[6] In this cyber incident, Robert Tapan Morris said that he was just trying to assess the size of the internet; he did not have any intention to harm, yet it was estimated that the Morris Worm damaged approximately 6000 computers and costed between $100,000 and $1 million. In cases like those scenarios even the company has a cyber risk policy if the action is not qualified as cyber attack because of the absence of the requirement of intention to harm, then the company may not recover its damages from the insurer.

Although the term "cyber attack" is mostly defined and understood as the malicious hacking, i.e. deliberate action, it was reported that in the shipping sector the majority of cyber incidents, which is estimated as 80%, have occured from accidental acts or omissions caused by human errors.[7] Considering the huge amount of human error in shipping industry, restricting the scope of the term "cyber attack" only to deliberate actions, and leaving accidental acts and omissions from outside of its scope would cause most actions not to be qualified as cyber attack.

However, a wider and comprehensive definition for the term "cyber attack" is provided in the Guidelines on Cyber Security on Board Ships introduced by Baltic and International Maritime Council (BIMCO), together with other leading shipping organisations. In the BIMCO Guidelines, the term "cyber attack" is defined as "any type of offensive manoeuvre that targets IT and OT systems, computer networks and/or personal computer devices attempting to compromise, destroy or access

(2011) www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyber space%20Operations.pdf accessed 19/09/2018.

[5]HM Government, 'UK National Cyber Security Strategy 2016-2021' (2016) https://assets.publish ing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_ cyber_security_strategy_2016.pdf accessed 18/08/2018.

[6]NATO, 'Translation of Cyber- the Good, the Bad and the Bug-free' www.nato.int/docu/review/ 2013/Cyber/timeline/DK/index.htm accessed 30/04/2018.

[7]Allianz Global Corporate & Speciality, 'Safety and Shipping Review 2017, An Annual Review of Trends and Developments in Shipping Losses and Safety' (2017b) www.agcs.allianz.com/assets/ PDFs/Reports/AGCS_Safety_Shipping_Review_2017.pdf accessed 08/09/2018.

company and ships and data".[8] The term IT means information technology systems that focus on implementation and management of computer-based systems such as hardware, software, servers and networking components.[9] On the other hand, the term OT means operational technology systems that focus on the use of data to control and/or monitor physical processes, such as management and control systems, sensors, supervisory control and data acquisition.[10] As seen, the objective to harm is not at the core of the BIMCO definition of "cyber attack"; whatever the attacker has in its mind any type of action, whether intentional or unintentional, attempting to compromise, destroy or access company and ships and data would be deemed as cyber attack. Although the BIMCO definition is wide and would cover both deliberate and accidental actions, it must be kept in mind that any unexpected compromise or data loss resulting from a defective software or hardware programme could not be qualified as cyber attack.

Cyber attacks may come from a range of sources with various kind of motives. States, sponsored organisations, criminals, terrorists, activists, opportunists, even employees who may act intentionally or unintentionally, may exercise cyber attacks. The motives behind cyber attacks would stem from psychological, social or financial roots, such as personal satisfaction of getting through cyber security defences, public or media attention, revenge, sabotage, espionage, blackmailing, financial or political gain, reputational damages, disruption to economies and so forth.[11] In a Cyber Crime Survey Report, it is indicated that motives behind cyber attacks are: 93% financial gain, 68% fraudulent activity, 57% defamation, 53% disruption, 48% cyber terrorism, 32% for fun.[12]

In the early years, cyber attacks were more immature in form such as password guessing or cracking, however with the evolvement of technology, the types of cyber attacks have moved from basic attacks to more sophisticated types of attacks, such as spear phishing, denial of services.[13] Cyber attacks may be in a number of forms and BIMCO Guidelines indicate that according to International Handling Services (IHS) Markit with BIMCO cyber security survey conducted in 2016, the most common types of cyber attacks that shipping industry has experienced are as follows[14]:

- Malware Attack: It means malicious software designed to access or damage a computer. It can perform various functions such as monitoring users' activities, stealing, deleting, altering or encrypting data without permission or even knowledge of the computer users. Malware includes ransomware, which encrypts data

[8]BIMCO et al., 'Guidelines on Cyber Security Onboard Ships, Version 2.0' (2017).

[9]The International Maritime Organization 'Guidelines on Maritime Cyber Risk Management MSC-Fal.1/Circ.3' (2017a); Boyes and Isbell (2017).

[10]Ibid.

[11]BIMCO et al. (2017) and Boyes and Isbell (2017).

[12]KPMG, 'Cyber Crime Survey Report, Insights and Perspectives' (2017) https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf accessed 30/09/2018.

[13]Chouhan (2015), p. 2.

[14]BIMCO et al. (2017).

until the requested ransom is paid, as happened in Maersk cyber attack, spyware, trojan, viruses and worms. According to IHS Markit-BIMCO survey, 77% of cyber attacks were in the form of malware attack.

- Phishing Attack: It involves sending emails and requesting the targeted persons to answer those emails or to download attachments, or directing them to visit fake websites to gather sensitive or confidential information such as passwords. In phishing, the goal is to trick the targeted person to believe that the email is coming from a genuine source. According to IHS Markit-BIMCO survey, 57% of cyber attacks were in the form of phishing attack.
- Spear Phishing Attack: It is similar to phishing but while phishing attacks usually target masses of people, spear phishing attacks target a specific individual or organisation. Therefore, unlike phishing attacks, spear phishing attacks are personalised to their targeted victims. According to IHS Markit-BIMCO survey, 23% of cyber attacks were in the form of spear phishing attack.
- Denial of Service (DoS) Attack: In this type attack, the attackers prevent legitimate and authorised persons from accessing the service. Such types of cyber attacks make the service temporarily or indefinitely unavailable to its intended users. Denial of service attacks are in the category of sophisticated targeted attack and pursuant to IHS Markit-BIMCO survey, 18% of cyber attacks were in this form.
- Brute Force Attack: To obtain information such as passwords or PIN numbers, different password combinations are used in repetitive attempts until the correct information is found. In such types of cyber attacks to generate various password combinations some softwares are usually used. Pursuant to IHS Markit-BIMCO survey, 13% of cyber attacks were in the form of brute force attack.
- Social Engineering: It is a non-technical strategy used to manipulate insider individuals to break security practices. Sensitive information is gathered by convincing or tricking the victim, therefore social engineering does not usually involve exploitation of computer or software systems.

The cyber attacks listed above are the ones shipping companies mostly encounter. There are of course other types of cyber attacks such as water holing or scanning, and with the evolvement in technologies in the future more sophisticated new types of cyber attacks would take place.

Lastly, it must be pointed out that cyber attack is usually not an instant action; it would consist of the following stages: (i) survey, (ii) delivery, and (iii) execution.[15] In the survey stage, information and intelligence about the target, such as determining the design and equipment of the ship, collecting information on itinerary of the ship and its cargo, identifying the authorised users, their emails or social media accounts, etc., is gathered. The survey stage is simply a reconnaissance phase which would take place over a long period. In the delivery stage, the information and intelligence gathered from the survey stage is used to create the method that would

[15]Ibid.

be used for cyber attack. For example, spear phishing or spoofing emails, creating fake website or misleading website to obtain users' account information or creating watering holes, and so forth would be created as cyber weapons and delivered to the target's computer or network systems. After delivery of cyber weapons to the target's computer and network systems, the attackers would wait for the data needed to start rolling in. During delivery stage, the attacker would exploit vulnerabilities, weaknesses and strengths of the company. Depending on the information and intelligence gathered from the first two stages, the final stage i.e. execution stage, takes place. In the execution stage, the attacker can fulfil its objective(s), which would be stealing or deleting data, ransoming stolen data, getting financial gain, getting media and public attention and so forth.

Considering the nature of cyber attack as extending over time, a crucial question may arise on the determination of the exact time when the cyber attack occurs. For instance, in a recent cyber attack where a Malaysian bunker provider lost $1.1 million, attackers used spyware to spy and monitor email exchanges between the bunker provider and supplier, and then they created a fake email and requested payment of monies into a bank account.[16] In this case, when did the cyber attack occur; did the cyber attack occur when the attackers deliver the spyware or when they created a fake email and requested the payment of monies to be made to their bank account or when the payment of monies was actually made?

3 Digitalisation of Shipping Industry

The era of ships sailing without any computer and network systems, and connectivity with shore had already ended. In the digital era of shipping, ships have been rigged with digitalised equipment (such as access control, power management, cargo management, propulsion and machinery systems), and a real-time interconnectivity between shore and ships has been ensured. Further, it seems that the shipping industry will soon enough come to a new era: the era of unmanned and autonomous ships. There is no doubt that the increased use of those new technologies in shipping industry will provide significant benefits for the sector, such incidents resulting from human errors will undoubtedly decrease or the ships will become more energy efficient. However, it should not be forgotten that digitalisation, interconnectivity and automation would bring treats, such as cyber attacks, and cause human injury, loss of life as well as significant financial loss. In the following section, digitalisation of shipping will be tackled from a legal point of view.

[16]Cooper (2018); V Wee, 'Malaysian Bunker Company Cheated of $1.1m in Email Payment Scam' (2017) www.seatrade-maritime.com/news/asia/malaysian-bunker-company-cheated-of-1-1m-in-email-payment-scam.html accessed 20/09/2018.

3.1 *The* Status quo *of Autonomous and Unmanned Ships*

The discussions over the terms ship and vessel seem to always be a topical one. Over the years, legislators have struggled with such definitions heavily affected by international problems. The eminent advent of autonomous and unmanned ships has added even more sparks to such discussion, as it is imperial for stakeholders to surpass such a hurdle before starting to discuss applicable regulations, and more specifically for this chapter, insurance regimes.

International Law

Firstly, it is important to note that most International Conventions do not distinguish between the term ship and vessel. For instance, United Nation Convention on the Law of the Sea (UNCLOS) uses the terms "ship" and "vessel" interchangeably.[17] Nevertheless, some national laws, such as English, may make a distinction between the two terms.[18]

Currently, there is no universal definition of ship or vessel in international law. The terms are used with different meanings in different contexts depending on the aims and purpose of each convention.[19] There are certain characteristics that are usually used to define ships and vessels. These include characteristics such as 'operation in the marine environment',[20] 'seagoing ability',[21] 'navigability',[22] 'mechanical self-propulsion',[23] 'used for the carriage of goods by sea',[24] 'used in

[17]Part XII, Section 5 of the UNCLOS; Art 211 of the UNCLOS.

[18]For instance, Section 742 of The Merchant Shipping Act 1894 stated that:

> Vessel' includes any ship or boat, or any other description of vessel used in navigation:
>
> 'Ship' includes every description of vessel used in navigation not propelled by oars. . .

The words 'not propelled by oars' of the 1894 Act were removed by the Merchant Shipping Act 1994 and these amendments were kept by the Merchant Shipping Act 1995 Section 313. Accordingly, under English law the term "vessel" not only differs from the term "ship" as it is broader. This was confirmed in *Steedman v Scofield* [1992] 2 Lloyd's Rep163, where Sheen J stated that "a vessel is usually a hollow receptacle for carrying goods or people. In common parlance 'vessel' is a word used to refer to craft larger than rowing boats and it includes every description of a watercraft used or capable of being used as a means of transportation on water".

[19]Lazaratos (1969), p. 57.

[20]Art 2(4) of International Convention for the Prevention of Pollution from Ships (MARPOL) 73/78.

[21]Art 1(1) of International Convention on Civil Liability for Bunker Oil Pollution Damage (BUNKER) 2001.

[22]Art 1(b) of International Convention on Salvage 1989.

[23]Annex I, Reg I/3(a)(iii) of International Convention for the Safety of Life at Sea (SOLAS), 1974.

[24]Art 1(d) of International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading (Hague Rules), 1924.

international seaborne trade',[25] 'not being permanently moored'[26] and 'not being permanently attached to the sea-bed'.[27] The first characteristics are the most widely used by international conventions.

Legal scholar Gothard Gauci argues that the least problematic international definition of a "vessel" is probably the one contained in the International Regulations for Preventing Pollution at Sea 1972, commonly known as COLREGS, and perhaps the most important regulation in maritime law and particularly important for the scope of this chapter because of its importance to Marine Insurance, especially concerning Hull & Machinery (H&M) insurance.[28] Rule 3(a) of the COLREGS provides that: "the word 'vessel' includes every description of water craft, including non-displacement craft and seaplanes, used or capable of being used a means of transportation on water." Gauci reasons that because of "the use of the terms 'includes,' 'watercraft,' as well as 'capable of being used' in this definition ensures that the judiciary are unlikely to be stifled if they are minded to apply a purposive interpretation to the legislation."[29] Indeed, COLREGS definition seems to leave limited space for a broader interpretation of the term ship and be in line with some national definitions.[30] Accordingly, it can be assumed that both remote-controlled- and fully autonomous vessels are *"water craft...capable of being used as a means of transportation on water"* within the definition of a "vessel" under the Convention.

In general, scholars seem to agree that there are essential characteristics that define the terms ship: floatability; capability of controlled movement on water; capability in the carriage of persons or goods beyond its own mass; and engagement in maritime (rather than inland water or river) navigation.[31] This means that although some smaller unmanned surfaced craft currently in operation would not fall under this general and accepted understanding of what defines a ship, because of their

[25]Art 2 of United Nations Convention on Conditions for Registration of Ships, 1986.

[26]Art 1(f) of Convention on the International Maritime Satellite Organization (IMSO), 1976.

[27]Art 1(a) of Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), 1988.

[28]Gauci (2016), p. 479.

[29]Ibid 480.

[30]For instance, the general definition set up by the USA Congress is "every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation by water". (1 U.S.C. § 3). In *Steedman v Scofield*, [1992] 2 Lloyds Rep 163. At the time, Mr. Justice Sheen held that the Jet Ski was not a ship for the 2-year time limit applicable to collisions based on the fact that the Jet Ski was not 'used in navigation'. See Arvanitis and Constantino Chagas Lessa (2014), p. 133. Perhaps, more importantly, in *Polpen Shipping Co Ltd v Commercial Union Assurance Co Ltd* [1943] 1 All ER 162, 165, a case concerning a collision, Atkison J stated: I do not want to attempt a definition, but I think a ship or vessel does involve two ideas. If I had to define them, I should say a vessel was any hollow structure intended to be used in navigation, that is, intended to do its real work upon the sea or other waters, and which is capable of free and ordered movement from a place to another'.

[31]Gahlen (2014), p. 252; Bork et al. (2008), pp. 298, 307, 328.

inability to carry persons or conventional cargos,[32] most unmanned and autonomous sea craft would fall under this category.[33]

Although the lack of a consistent international definition and the subsequent lack of soft law can be deemed problematic, it is arguably exactly what allows the term the capability to develop and adapt in line with new regulatory contexts.[34] This flexibility can be said to allow unmanned and autonomous ships to be considered vessels under international law.

It follows that in May 2018, at the 99th Maritime Safety Committee meeting, the International Maritime Organization (IMO) commenced work into Maritime Autonomous Surface Ships (MASS) to access how safe, secure and environmentally sound her operations are and how they may be addressed in IMO instruments. To start the assessment, the organisation has agreed in a preliminary definition of MASS as a "ship, which, to a varying degree, can operate independently of human interaction". The Organization followed the definition by listing (non-hierarchically) the degrees of autonomy

- Ship with automated processes and decision support: Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated.
- Remotely controlled ship with seafarers on board: The ship is controlled and operated from another location, but seafarers are on board.
- Remotely controlled ship without seafarers on board: The ship is controlled and operated from another location. There are no seafarers on board.
- Fully autonomous ship: The operating system of the ship is able to make decisions and determine actions by itself.[35]

Therefore, little doubt rests that according to International Law, autonomous and unmanned sea crafts can be considered ships/vessels. This position being further corroborated by the IMO position when defining Maritime Autonomous Surfaces Ships.

[32]It is important to note that some national jurisdictions, such as England and Wales, do not consider the ability to covey persons or cargo a prerequisite for a craft to be considered a ship. In the case of *R v Goodwin* [2005] EWCA Crim 3184, [27]; [2006] 1 Lloyd's Rep 432, 438, in which Lord Phillips CJ opined that, for a "vessel to be 'used in navigation' under the Merchant Shipping Acts, it is not a necessary requirement that it should be used in transporting persons or property by water to an intended destination."

[33]Veal and Tsimplis (2017), pp. 303, 308.

[34]V Lowe, 'Report on the Interpretation of the Term 'ship' in the 1992 Civil Liability Convention' in *Consideration of the Definition of 'Ship', International Oil Pollution Compensation Funds* (IOPC/OCT11/4/4, 2011) documentservices.iopcfunds.org/meeting-documents/download/docs/3535/lang/en/ accessed 18/08/2018; Van Hooydonk (2014), pp. 403, 408.

[35]The International Maritime Organization Maritime Safety Committee (MSC), 99th session 16–25 May 2018; The International Maritime Organization Briefing, 'IMO Takes First Steps to Address Autonomous Ships' (2018a) www.imo.org/en/mediacentre/pressbriefings/pages/08-msc-99-mass-scoping.aspx accessed 10/06/2018.

National Law Approaches

Because of the scope of this chapter, when analysing national approaches, focus will be given to English and Wales law as it is the predominant choice of law in marine insurance contracts. Norwegian and Danish law will also be briefly analysed because of their advanced research in the area of autonomous shipping and the fact that the first autonomous and electric container ship, *Yara Birkeland*, has been ordered by a Norwegian company.[36]

The current definition of a ship under English law is considered a problematic one. Found in Section 313 of the English Merchant Shipping Act 1995, a ship is "any description of a vessel used in navigation". Arguably, the English legislator has shifted the focus from the physical characteristics of the relevant structure, to its ability to navigate.[37] The definition reliance of "used in navigation" causes problems to the English judiciary.[38]

The most recent case discussing the definition of a ship in England was in 2005, *R. v Goodwin*,[39] when the Court had to analyse if a jet ski could fell under Section 313 of the Merchant Shipping Act 1995. The Criminal Court of Appeal ruled that:

> The words 'used in navigation' exclude from the definition of 'ship or vessel' craft that are simply used for having fun on water without the object of going anywhere, into which jet-skis plainly fall.[40]

Accordingly, at first sight autonomous and unmanned crafts could fall under the English definition of a ship, once they are not used for recreational purposes and have a route to follow. The question to be analysed, nevertheless, as posed by Veal is "whether 'navigation' is a term that which necessarily requires the on board attendance of individuals purporting to 'navigate' the relevant ship"[41] Although, the scholar suggests that there is nothing doctrinally requiring ships to be manned,[42] it is important to highlight that case law may suggest otherwise.

In *R. v Goodwin*, the Court had to decide if a jet ski was a ship under the Merchant Shipping Act 1995 to rule its rider was not a master or seamen within Section 58 of the same Act. In its *obiter dicta*, the Court referred to *Steedman v Scofield*,[43] in particular to the court Ruling that for there to be navigation:

---

[36]Kongsberg, 'Autonomous Ship Project, Key Facts about YARA Birkeland' www.km.kongsberg.com accessed 15/08/2018; The Maritime Executive, 'Shipbuilder Chosen for Yara Birkeland' www.maritime-executive.com/article/shipbuilder-chosen-for-yara-birkeland 15/08/2018.

[37]Veal and Tsimplis (2017), p. 311.

[38]Gauci (2016), p. 482.

[39]EWCA Crim 3184.

[40]Ibid.

[41]Veal and Tsimplis (2017), p. 311.

[42]Ibid 312.

[43][1992] 2 Lloyd's Rep 163.

> The navigator must be able (1) to determine the ship's position and (2) to determine the future course or courses to be steered to reach the intended destination. The word "navigation" is also used to describe [. . .] ordered movement of ships on water.[44]

Thus, case law seems to suggest the need for the ship to be manned to fall within Section 313 of the Merchant Shipping Act 1995. Accordingly, only fully autonomous vessels would not come under the English definition of a ship. It may be argued, however, that even if a fully autonomous vessel does not come within the strict, legal definition of a "ship" under the Merchant Shipping Act, the Secretary of State can easily adapt the definition to include them as she/he has the authority to do under Section 311 of the Merchant Shipping Act, or case law will adapt the understanding of "navigation" to include these type of vessels.

Nevertheless, remarkably, the ability to navigate and a hollow structure were held insufficient on their own to give a craft the character of a ship under a collision liability clause in a marine contract providing for indemnification of the insured owner in respect to liability arising from a collision.[45]

Indeed, in *Polpen Shipping*, the Court had to decide whether a flying boat constituted a vessel when it was damaged in Falmouth Harbour by *the Polperro* which had dragged its anchor, ruled that the policy wording 'ship or vessel' did not include a flying boat as 'ability to navigate' is only 'incidental to its real work' i.e. flying. Accordingly, the court ruling suggests that the primary purpose of a craft should be navigation, the mere ability to navigate does not suffice to constitute a ship, especially for marine insurance.

Perhaps, most importantly, in *Merchants Marine Insurance v North of England P & I*,[46] the Court of Appeal addressed the issue whether a floating crane could be considered a ship or a vessel for an exclusion in a Protection and Indemnity Rulebook. Lord Justice Bankes held that the floating crane was not a ship or vessel, considering its structure as well as its past and future use, considered relevant for such determination.[47]

The approach taken by Courts in such cases will in practice be relevant to determine which insurance policy the obligation of indemnification will fall under, i.e. whether H&M coverage or whether it is the Protection and Indemnity (P & I) Club Rules.[48]

Both cases demonstrate like no other how fragile the English law definition of a ship is. Nevertheless, despite the clear relevance of both cases for marine insurance, neither decision at first glance seems to affect the status of autonomous ship in English law, as the primary purpose of such crafts shall be navigation regardless if fully autonomous or partially manned.

---

[44] *R v Goodwin* [2006] 1 Lloyd's Rep 432, 437.

[45] *Polpen Shipping v Commercial Union* (1943) 74 L1. L. Rep 157.

[46] (1926) 26 Ll L Rep 201.

[47] Ibid 202.

[48] Gauci (2016), p. 489.

Norway does not have a general statutory definition of the term ship. Therefore, a case-by-case approach is adopted to determine if a particular craft/construction can be said to be a ship according to a particular set of rules.[49] In this regard, the Norwegian Maritime Code offers some definitions concerning specific maritime law rules to be applied. For instance, Section 183 of the Norwegian Maritime Code, which deals with the civil liability for oil pollution damage, broadly defines ship as "any seagoing vessel or other floating device on the sea." In the same pace, Section 441 of the Norwegian Maritime Code, dealing with salvage, defines ship as any "ship or vessel and also another construction capable of navigation," hence a more similar definition to the English one. It is in fact argued by scholars[50] that the Norwegian notion of the term is in line with the approach established in *Steedman v Scofield.*[51]

Therefore, it seems Norway could face similar problems as England when dealing with fully autonomous vessels. Nevertheless, the pragmatic approach taken by the country and broadness of the existing definitions might mean that adjudicators might have less problem finding autonomous (even fully) constructions to be ships.

The Danish Merchant Shipping Act in Section 11 (2) delimits the concept of a ship by stating that "floating docks, cable drums, floating containers and other similar equipment are not considered ships," meanwhile Section 11(3) implies that "barges, lighters, dredging machinery, floating cranes and alike are considered ships (...)." Thus, the Danish concept of what constitute a ship seems to be a bit blurred, only having a positive and negative list, not seemingly to be exhaustive, of constructions that can or cannot be considered ships.

Nevertheless, similarly to Norway, Danish maritime legal theory assumes that a vessel has the following characteristics:

- A ship is a floating arrangement, with a buoyancy partly caused by the arrangement being hollow
- A ship must be capable of moving on or through the water.
- The ship is not required to be able to move by its own power. In addition, a lighter, a barge or a floating crane without propulsion machinery are considered ships, cf. section 11(3) of the merchant shipping act.
- The ship must have a certain size. Rowboats, kayaks, etc. fall outside the concept of a ship. Section 10(2) of the merchant shipping act stipulates that ships must have a gross tonnage of at least 5 in order to be registered as ships in the Register of Shipping.[52]

Accordingly, there is nothing in Danish Maritime law preventing autonomous constructions to be considered ships, and hence, subject to Danish regulations and although, English law and similarly Norwegian law, arguably might find some obstacle according to how the navigational requisite has been construed. As seen, this can be easily overcome.

[49]Falkanger et al. (2011), p. 44.

[50]Blaskovic-Schnell (2016), p. 167.

[51][1992] 2 Lloyd's Rep 163.

[52]Danish Maritime Authority, 'Analysis of Regulatory Barriers to the Use of Autonomous Ships Final Report' Ramboll 2017, 38.

4 Seaworthiness

Marine Insurance Law establishes required standards to grant insurers defences in case the vessel is unseaworthy. In England, Section 39 of the Marine Insurance Act 1906 categorises seaworthiness as an implied warranty in a contract of insurance; namely even if the insurance contract does not mention seaworthiness of the ship, it is tacitly understood that the ship must be seaworthy at the start of the voyage, hence being subject to Section 10 of the same Act, which provides that:

(1) Any rule of law that breach of a warranty (express or implied) in a contract of insurance results in the discharge of the insurer's liability under the contract is abolished.
(2) An insurer has no liability under a contract of insurance in respect of any loss occurring, or attributable to something happening, after a warranty (express or implied) in the contract has been breached but before the breach has been remedied.

There is not any universal definition for the term seaworthiness in maritime law. Section 39(4) of Marine Insurance Act 1906 provides that "a ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured". This definition stems from the case of *Dixon v Sadler*[53] in which it was stated that to become seaworthy, the ship "shall be in a fit states as to repairs equipment, and crew and in all respects, to encounter the ordinary perils of the voyage insured, at the time of sailing."

To determine whether cyber attacks would make a ship unseaworthy, two elements of the definition in Section 39(4) of Marine Insurance Act 1906 must be carefully tackled: (i) reasonably fit in all respects, and (ii) encounter the ordinary perils of the seas. The term "reasonably fit in all respects" seems wide enough to embrace the issue of being safe and secure against any kind of cyber attack. That means under the definition in Section 39(4) a ship, which faces any cyber attack, would be deemed as unseaworthy because of its unfitness to the voyage. The required standard is not fitness but reasonable fitness, and to determine what a fit vessel is, there is the need to rely on the general accepted elements of seaworthiness provided by The Hague-Visby Rules.

It is questionable whether cyber attacks could be qualified as ordinary perils of the seas. Marine Insurance Act 1906, First Schedule para 7 provides that the term "perils of the seas" "refers only to fortuitous accidents or casualties of the sea. It does not include the ordinary action of the winds and waves". In *Thompson v Hopper*,[54] it is stated that the word "fortuitous" involves an element of chance or ill luck. English courts state that to be considered as perils of the seas "there must be some causality, something which could not be foreseen as one of the necessary incidents of the

[53](1839) 5 M & W 405.
[54](1856) 6 E & B 937.

adventure"[55] therefore "issues from the conscious working of the human will and not from the haphazard working of natural sources" are not considered as perils of the seas.[56] Furthermore, in a recent case, *The Saldanha*,[57] it was pointed out that "an obviously deliberate and violence attack is not described as an accident, no matter how unexpected it may have been to the victim."

As mentioned above,[58] cyber attacks could be derived from intentional or unintentional actions. Unintentional actions would meet the criteria of being "fortuitous accidents or causalities", therefore would be considered as perils of the seas. However, it could be argued that intentional cyber attacks would not be considered as perils of the seas because of lack of fortuitous accidents or casualties.

On contracts of carriage, the common law classic test of seaworthiness was provided in *McFadden v Blue Star Line*[59] in which it was established that: "The vessel must have that degree of fitness which an ordinary careful and prudent owner would require his vessel to have at the commencement of her voyage having regard to all the probable circumstances of it. To that extent the shipowner, as we have seen, undertakes absolutely that she is fit and ignorance is no excuse. If the defect existed, the question to be put is, would a prudent owner have required that it should be made good before sending his ship to sea had he known of it? If he would, the ship was not seaworthy within the meaning of the undertaking."

A critical problem may arise regarding the time of seaworthiness in cases of cyber attacks. As mentioned above,[60] cyber attack is not an instant action; there could be different stages that may take over a long period. Under English case law, it is required that the ship must be seaworthy at the start of the voyage.[61] However, in cases of cyber attacks, it would not be an easy task to determine whether the cyber attack takes place before the start of the voyage or later. For instance, assuming that computer or network systems of a ship, or a personal computer or mobile phone of the master contains a trojan, spyware or virus before the commencement of the voyage, and the attackers monitor the target for a while but once the voyage starts they fulfill their objective, such as encrypting data and requesting ransom, or interrupting GPS and directing the ship to the route of pirates. In such cases, questions may arise about the time when the vessel become unseaworthy; was it when the cyber attack occurred or before the commencement of the voyage when the cyber weapon was delivered or after the commencement of the voyage when the objective was fulfilled. As it was demonstrated, for insurance it is essential to determine when the vessel became unseaworthy.

[55] *The Xantho* (1887) 12 App Cas 503, 509. See also, Katsivela (2014), pp. 343, 435 *et seq*.

[56] *P Samuel & Co Ltd v Dumas* [1924] AC 431, 461–462.

[57] [2011] 1 Lloyd's Rep 187.

[58] Please refer to Sect. 2 of the chapter, *Meaning and Scope of the Term "Cyber Attack"*.

[59] [1905] 1 KB 697.

[60] Please refer to Sect. 2 of the chapter, *Meaning and Scope of the Term "Cyber Attack"*.

[61] *McFadden v Blue Star Line* [1905] 1 KB 697; *The Madeleine* [1967] 2 Lloyd's Rep 224.

Although there is no universal definition of seaworthiness, there seems to be a general understanding of what a seaworthy vessel will be, it seems that the concept of seaworthiness may have slight variation according to different interests involved.[62] For instance, although Article III Rule 1 of The Hague-Visby Rules does not provide a definition of seaworthiness, it specifies the elements of seaworthiness:

> 1_ The carrier shall be bound before and at the beginning of the voyage to exercise due diligence to: a_ Make the ship seaworthy; b_ Properly man, equip and supply the ship; c_ Make the holds, refrigeration and cool chambers, and all other parts of the ship in which goods are carried, fit and safe for their reception, carriage and preservation.

In *Wedderburn v Bell*,[63] seaworthiness was extended to cover sufficient crew in number and skill to properly navigate the vessel. Furthermore, in *Hong Kong Fir Shipping Co Ltd v Kawasaki Kisen Kaisha Ltd*,[64] Sellers LJ held that a vessel could be deemed seaworthy despite the "numerical deficiency" of the crew so long as the crew was competent.[65]

In Article III Rule 1 of The Hague-Visby Rules, the requirement for a vessel to be *"Properly man, equip and supply the ship"* to be deemed seaworthy under the Marine Insurance Act, which can be deemed problematic when dealing with autonomous vessels.

Furthermore, since the obligation to provide a seaworthy ship is a subjective obligation,[66] there is no reason why the obligation as to crew cannot be deemed such as well. Such interpretation can be further reinforced if it considered the fact that seaworthiness is a time-specific implied warranty,[67] as it requires the insured vessel to be seaworthy at the commencement of the voyage, hence the term *"properly man"* presumably implies adequate manning for the intended ship and voyage and not a general standard of adequacy.

Accordingly, it can be argued that depending on degree of autonomy of a vessel this can be considered seaworthy. Seaworthiness would just likely to be an issue in case of fully autonomous vessel, since a completely unmanned vessel are generally understood to make its own decisions regarding navigation based on pre-programmed instructions or artificial intelligence,[68] being completely unmanned and therefore in the absence of a held covered clause,[69] the insurance policy would be void.

---

[62] Soyer (2017).

[63] (1807) 1 Camp 1; 170 ER 855.

[64] [1962] 2 WLR 474.

[65] Ibid 481.

[66] *President of India v West Coast Steamship Co* [1963] 2 Lloyd's Rep 278, 281 *per* District Judge Kilkenny.

[67] S. 39(1) of Marine Insurance Act 1906.

[68] Van Hooydonk (2014).

[69] Davey (2013), pp. 118, 119.

It can be argued that even a fully autonomous vessel does still have a degree of human interaction, since even in this case there should be an operator monitoring from shore, in case the system fails to determine action.[70] Furthermore, in remotely controlled unmanned vessels, there will be shore-based operators who remotely control the vessels. The question may arise whether shore-based operators are deemed as master and/or seafarers.[71] Under Section 313 of the English Merchant Shipping Act 1995, master is defined as "every person (except a pilot) having command or charge of a ship." Accordingly, being on board a ship is not a requirement to be qualified as master, and in cases of remotely controlled unmanned ships, shore-based remote operators will command the ship and be in charge, therefore they would be deemed as master.[72] If the shore-based operators fall within the definition of master/seafarer, the requirement of properly manned for the seaworthiness of a ship would arguably be satisfied. However, in cases of fully autonomous vessels, the involvement of shore-based operators in command and charge of a ship would be limited to monitoring; pre-programmed code or artificial intelligent would be in charge, therefore it could be argued that shore-based operators would be not deemed as master.

Under both Maritime Labour Convention and The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) 1978, being on board a ship is required to be qualified as a seafarer. Therefore, shore-based operators cannot be qualified as seafarers under those Conventions. The fact that the operator would be ashore will currently unlikely qualify him a seafarer or a master still making the vessel crewless, hence unseaworthy. This problem could be solved by revising current legislations, such as the Maritime Labour Convention and STCW, as a title of example, to the use of autonomous vessels.[73] In fact, considering that historically maritime law framework has been drafted taking into consideration the figure of the master, it seems to be already settled in the mind of stakeholders that new legislation will need to be either revised or especially enacted to guide the specifics demands of autonomous vessels, from technical rules, to navigation regulations, to labour legislation, to liability regimes.[74]

It is important to note, however, that studies conducted by stakeholders acknowledge that remote operation should start with keeping a competent crew on board as "a back up and ready to take control in case of a serious problem".[75] Stakeholders acknowledge that since the transition from traditional shipping to remote and

[70]Danish Maritime Authority (2017), p. 5.

[71]Van Hooydonk (2014), p. 412.

[72]British Maritime Law Association (BMLA), 'Response to CMI Questionnaire on Unmanned Ships' EME_ACTIVE-568475036.1 (2018) www.bmla.org.uk/documents/2018/BMLA-Response-to-CMI-Questionnaire-on-Unmanned-Ships.pdf accessed 08/08/2018.

[73]For a more detailed discussion about how such regulations could be amended please see; Bernauw (2017), p. 359; Daum and Stellplug (2017), p. 363.

[74]Mellilo (2016).

[75]E Jokioinen et al., 'Advanced Autonomous Waterborne Applications (AAWA) Position Paper, Remote and Autonomous Ships: The Next Steps (Rolls Royce)' (2016) www.rolls-royce.com/~/

autonomous operation cannot be achieved over night, a master and a crew are likely to be responsible for vessel operations for years to come.[76] Therefore, it is unlikely that for the next few years any autonomous vessel will be considered unseaworthy for not being properly manned in the current sense, hence having her insurance policy declared void.

In cases where shore-based operators are qualified as crew, the mere absence of the crew on board may not make autonomous ships unseaworthy. However, the incompetence of shore-based operators would cause unseaworthiness. Considering the high technologies autonomous ships contain shore-based operators need to be adequately trained, they must have skills and knowledge to properly operate and manage the ships, otherwise the ship would be considered as unseaworthy. For instance, in *The Star Sea*,[77] it was held that the ship was unseaworthy because the master was incompetent, as he did not know how to operate the ship's CO2 system for extinguishing fires. Likewise, in *The Eurasian Dream*,[78] the ship was considered as unseaworthy because of inadequate training of the crew regarding fire-fighting equipment. Similar decisions could be given in case of autonomous ships if shore-based operators are incompetent to properly operate and manage the ship remotely.

Lastly, it must be pointed out that another leg of the requirements of seaworthiness is to have the required certificates and documents on board. Although a ship is seaworthy in a physical sense, and properly manned with competent crew, it could be considered as unseaworthy if the required certificates and documents are not on board. Under the International Safety Management (ISM) Code, ships are required to have a valid Safety Management Certificate and Document of Compliance. Likewise, under the International Ship and Port Facility Security (ISPS) Code, ships are required to have a valid International Ship Security Certificate. Absence of any of those documents would render the ship to be considered unseaworthy. It must be highlighted that the mere physical existence of the required certificates and documents on board does not make the ship seaworthy if they are not properly adopted and the ship is not actually managed and operated safely.[79]

---

media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf accessed 15/08/2018.

[76]The first autonomous container line vessel is expected to be launched in 2020 and gradually move from manned operation to fully autonomous operation by 2022, leaving a mere more or less three years since the drafting of this chapter for the maritime legislative framework to adapt to this new reality.

[77][2001] 1 Lloyd's Rep 389.

[78][2002] 1 Lloyd's Rep 719. In this case, it was stated that incompetence might result from: (a) an inherent lack of ability; (b) a lack of adequate training or instruction; (c) a lack of knowledge about a particular vessel and/or its systems; (d) disinclination to perform the job properly; (e) physical or mental incapacity.

[79]As happened in *The Star Sea* [2001] 1 Lloyd's Rep 389 in which the ship was carrying safety certificates but in fact they were not properly applied therefore the ship was considered as unseaworthy.

5 Cyber Risks

The expectation surrounding the use of autonomous and unmanned vessels is for a reduction in known or traditional risks.[80] For instance, currently, the industry speculates that human errors are the cause of 75% of marine insurance losses and the advent of autonomous shipping will help reduce the risks of such accidents[81] while allowing owners to extract further savings through operational efficiency.[82]

Nevertheless, while traditional risks are more likely to be reduced, new risks are deemed to arise from autonomous operations: software and data malfunctions, navigational issues and cyber piracy,[83] most commonly referred by stakeholders as 'cyber risks'.

The IMO defined 'maritime cyber risk' as "a measure of the extend to which a technology asset is threatened by the potential circumstance or event which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised".[84] The Organization definition seems to encompass all the risks arising out of cyber-enabled ship such as autonomous and unmanned vessel and as such will be the one adopted in this chapter.

5.1 Cyber Risk Assessment/Management

As it could be noted, regulatory barriers still need to be dealt with for the development of autonomous shipping. In the same pace, insurance policies need to adapt, being also decisive for the use of autonomous vessels. These two circumstances, as seen, mutually affect each other.[85]

Nevertheless, insurers are said to be able to encourage progress by making their own risk assessments and providing policies for responsible operators, being unquestionable that the insurance industry's expertise in risk management will factor

[80]HC Burmeister et al., 'Can unmanned ships improve navigational safety?' (2014) Transport Research Arena http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.846.5385&rep=rep1&type=pdf accessed 09/10/2018.

[81]Allianz Global Corporate & Speciality, 'Ready to launch: Autonomous ships - Smart Sails (2017a) www.allianz.com/en_GB/press/news/business/insurance/170824-autonomous-shipping-smart-sails.html accessed 09/09/2018.

[82]Macfarlane (2017).

[83]IMO Guidelines (2017) include a non-exhaustive list of vulnerabilities created by such risks, including bridge systems, access control systems and communication systems.

[84]Ibid, 1.

[85]For a more comprehensive analysis of the circumstances effecting autonomous shipping see; Danish Maritime Authority (2017), p. 3.

in the adoption of autonomous and unmanned technology.[86] The fact is that insurers insure risks, hence it is critical for them to assess exactly what they are insuring, as well as imperative for companies to be able to manage cyber risks, having a response plan for cyber breach and evaluate the ability to cover these risks through insurance.[87]

The functionality provided by autonomous shipping, as noted, can range from simple remote monitoring with a crew on board to a fully autonomous and therefore crewless vessel. Thus, according to a Lloyd's Register report, since the risks can vary considerably, the assessment of these systems requires a risk based approach to identify the hazards introduced by cyber enablement and to mitigate associate risks.[88]

In 2016 BIMCO, with the support of the International Chamber of Shipping, INTERCARGO, INTERTANKO, CLI and International Union of Marine Insurance (IUMI), presented one of the first more extensive concepts on how to prevent cyber attacks by focusing on risk assessment and the detection of vulnerabilities of the IT systems used and expected responses to a cyber attack, including how to act adequately to limit the damage.[89] It followed that in 2017, after the advent of the IMO Guidelines in Cyber Risk Management, BIMCO introduced renewed guidelines, with a similar approach to the 2016 one, stating that access to risk exposure should be determine by:

- the likelihood of vulnerabilities being exploited by external threats;
- the likelihood of vulnerabilities being exposed by inappropriate use;
- the security and safety impact of any individual or combination of vulnerabilities being exploited.[90]

Similarly, a Recommended Practice Guide on Cyber Security issued by the Classification Society DNV-GL, provides that the first step to access the risks is to describe the different scenarios that caused unwanted consequences, while also evaluating its consequences.[91]

The IMO, following the same lines of BIMCO and DNV-GL, set the following actions that can be taken to support effective cyber risk management:

[86]G Yeomans, 'Autonomous Vehicles- Handing over Control: Opportunities and Risks for Insurance' (2014) www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/autonomous-vehicles accessed 09/10/2018.

[87]P Marllow, 'Cyber Liability in the Marine Industry Report' (2015) https://www.ajg.com/media/1697987/cyber-liability-for-the-marine-industry.pdf accessed 09/10/2018.

[88]Lloyd' s Register, 'Cyber Enabled Ships – Ship Right Procedure Assignment For Cyber Descriptive Notes for Autonomous & Remote Access Ships' (2017) Lloyd's Register Guidance Document, Version 2.0.

[89]BIMCO et al., 'Guidelines on Cyber Security Onboard Ships, Version 1.1' (2016).

[90]BIMCO et al. (2017).

[91]DNV-GL, 'Recommended Practice – Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation' DMVGL-RP-0496, 2016.

- "Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.
- Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.
- Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.
- Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.
- Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event."[92] Furthermore, the IMO Maritime Safety Committee through Resolution MSC. 428(98) on Maritime Cyber Risk Management Systems[93] provided that an approved safety management system should consider cyber risk management in accordance with the objectives and requirements of the International Safety Management (ISM) Code. The Resolution further encourages Members States to ensure cyber risks are addressed in their onboard safety management no later than the first annual verification of a company's Document of Compliance after 1 January 2021, hence before the fully autonomous vessel becomes a reality.[94] Nevertheless, shipowners are strongly advise to act immediately.[95] It is important to note that failure of compliance with the terms of the ISM Code raises liability should any loss or damage result therefrom as it would as it constitutes or support and action in negligence and/ or breach of statutory duty of care.[96] Thus, when such claim is made under an insurance policy, insurers are most likely to raise the breach of the implied warranty of seaworthiness and the defence of privity afforded by Section 39(5) of the Marine Insurance Act 1906.[97]

In September 2017, the UK government published a "Code of Practice – Cyber Security for Ships". The Code sets a high-level guidance for the development and maintenance of an effective cyber security policy for ship and shipowners.[98] Moreover, following the line of other industry stakeholders, the document provides

[92]IMO Guidelines (2017).

[93]The International Maritime Organization Maritime, 'Safety Committee Maritime Cyber Risk Management in Safety Management Systems Resolution MSC. 428(98)' (2017b).

[94]Yara, 'YARA Selects Norwegian Shipbuilder VARD For Zero-Emission Vessel Yara Birkeland' www.yara.com/corporate-releases/yara-selects-norwegian-shipbuilder-vard-for-zero-emission-vessel-yara-birkeland/ accessed 15/08/2018.

[95]Macfarlane (2017).

[96]Donaldson (1999), p. 526.

[97]Anderson (2015).

[98]Boyes and Isbell (2017).

guidance on cyber security assessment and the subsequent development for a Cyber Security Plan.[99]

The efforts made by shipping industry stakeholders, including insurers in accessing and managing cyber risks are, if nothing else, remarkable. They demonstrate that the industry is not sparing efforts to be ready for the advent of new technologies and new threats.

6 The Insurability of Liabilities Arising from Collision

As pointed out by a report conducted by GARD, hacking of e-navigation and other systems could result in a collision that could lead among other things to loss of cargo, pollution and business interruption.[100] In fact, any type of software malfunction, not necessarily caused by a cyber attack, could lead to a collision.

According to Section 41 of the Marine Insurance Act 1906, it is an implied warranty that the adventure insured is lawful and that it shall be carried out in a lawful manner. The section refers to breaches of statutes or regulations.[101] The effect of this is that a lawful adventure from the outset may subsequently become unlawful, hence breaching the implied warranty of legality.[102]

The problematic particularly revolves around the fact that Rules 2 and 5 of the COLREGS assume some human involvement, with Rule 2 requiring the master and the crew to comply with the Rules and Rule 5 requiring that every vessel "shall at all times maintain a proper look-out by sight and hearing".

Rule 2 of the Convention in essence reaffirms the primacy of good seamanship by expressly providing for a duty of care and not only from the owner but as well as the master and the crew. In fact, legal scholars identify seamanship as the foundation of the COLREGS provisions and that such a duty has an important but no less residual applicability filling in the gaps unfulfilled by the wording of the Convention.[103] In this regard, Veal argues that communication systems utilised by a remote controlled unmanned vessels might be sufficiently instantaneous even when provided from afar by a remote controller, and assuming that this has the required training, the seamanship obligation can be discharged efficiently, meaning that potentially remote controlled vessels can comply with the convention.[104] Nevertheless, and considering that one important element of good seamanship is the sufficiency of the ship's crew, fully autonomous vessels are likely to not comply with the COLREGS. Furthermore,

[99] Ibid.

[100] GARD, 'Cyber Security- Managing the Threat' (2017) www.gard.no/Content/21112216/Cyber Security accessed 14/05/2018.

[101] Ibid.

[102] Soyer (2017), p. 147.

[103] Gault et al. (2016) ch.4, para 5.106.

[104] Veal and Tsimplis (2017), p. 325.

it is important to highlight that currently human involvement in the decision making process of the Convention is still considered essential, even if on board attendance is not always.[105]

Following this, studies are currently being conducted to offer an optimised framework for online path planning autonomous vessel to comply with COLREGS, at the same time as collision avoidance, by considering mariners' interpretation of the Convention together with good seamanship input from experienced seafarers.[106]

In terms of a remote-controlled vessel, it can be argued that on-shore "look-out" is sufficient to satisfy Rule 5 in line with Sheen J ruling in *The Nordic Ferry.*[107] However, the same argument does not necessarily fits fully autonomous vessels. Veal submits that "proper" lookout can be substituted for audio- and visual recordings depending on their quality and instantaneousness, and in this sense autonomous vessels could comply with Rule 5.[108] Likewise, analysed by a linguistic perspective, the Rule provides that proper lookout shall also be maintained by "all available means appropriate", hence not necessarily excluding technological advances in the area. Accordingly, autonomous vessels can potentially fall within the rule.

Nevertheless, it should be noted that Rule 5 does not consider that future technology may make (and it aims to do so[109]) ships communicate directly with each other and coordinate their course and speed to avoid collisions.[110]

From an insurance perspective, another issue that arises concerning collisions, and is already a reality in terms of cyber risks, is the case of consequence of a software malfunction that leads to a loss of communications. In which case it can be argued that the vessel breached Rule 5 of COLREGS because of lack of "proper look-out" which would lead to a loss of H&M cover under Section 41 of the Maritime Insurance Act 1906.

Although this may be the case in Australia where Section 41 of the Marine Insurance Act 1906 is quoted verbatim into Section 47 of the Australian Marine Insurance Act 1909,[111] the UK seems to have taken a different approach, as it can be seen in *St John Shipping Corp v Joseph Rank Ltd*[112] when Devlin J ruled the

[105]Reynardson et al. (2017).

[106]Hu et al. (2017), p. 13622.

[107][1991] 2 Lloyd's Rep 591. In this case, Sheen J found, in circumstances where the radars of the vessel were rendered inoperative because of a thick fog that the vessel "could have sought advice from the fog watch pilot on duty in the Harwich Habour Operations Room...this would have been better than without assistance and proceeding down channel on the wrong side".

[108]Veal and Tsimplis (2017), p. 328.

[109]Hu et al. (2017).

[110]Danish Maritime Authority (2017), p. 47.

[111]In *Doak v Weekes & Commercial Union Assurance Co plc* [1986] 82 FLR 334 Ryan J held that leaving port without people on board with the correct certificates was contrary to regulation and the adventure was thus carried out in an unlawful manner. Following the same lines, in *Switzerland Insurance Australia Ltd v Mowie Fisheries Pty Ltd* [1997] FCA 231 when a vessel sailed from port without the complement of officers as required by the relevant act. See also Soyer (2017), p. 148.

[112][1957] 1 QB 267.

adventure to be lawful even if the shipowner overload his ship contrary to statute.[113] Similarly, in *Redmond v Smith*[114] failure to provide a written agreement with the crew under the Merchant Seamen's Act of the time was held to be nevertheless lawful. Consequently, it seems that the UK takes a case-by-case approach in determining the lawfulness of the adventure according to policy considerations.

When dealing with cyber risks in case of collision is also relevant to analyse with navigational software malfunction would fall under the Product Liability Insurance Cover. This development would be advantageous for claimants as these types of claims are not subject to the limitations of liability under the Convention on Limitation of Liability for Maritime Claims 1976 (LLMC).[115] Moreover, considering that software malfunctions are likely to be considered cyber risks, they might fall under CI.380 exclusion, hence not covered by H&M insurance.

For a claim to be successful under a product liability insurance policy, there must be a defect in the product itself that causes damage.[116] Little doubt rests that software would be deemed a product since the European Parliament in advent of the European Product Liability Directive (1985/374) (The Directive), which came into effect in the U.K. via the Consumer Protection Act (CPA) 1987,[117] put an end in the discussion when questioned if computer software would fall under the definition of a product.[118] Furthermore, on "defect" Section 3 of the CPA provides that this is deemed to have occurred in a product if "the safety of the product is not such as persons generally are entitled to expect". Scholars argue that claim under product liability will likely fail under this section as the software will only be adopted once it can be proven that the level of security is, on aggregate, higher than that of human decision-making, with evidence to support such a conclusion invariably always readily available.[119] In this sense, as already pointed out, it is important to call attention to the fact that it is estimated that around 75–80% of marine accidents are caused by human error,[120] and reducing this from the equation would reduce insurable risks.

Nevertheless, is also conceivable that the level of safety of the product will not be judged on aggregate but rather on a case-specific basis.[121] Thus, in the case of autonomous vessels scenario whereby software malfunction leads to a loss of communication, a superior safety management may be deemed not available as it

[113] Soyer (2017), p. 147.

[114] (1844) 7 Man & Gr 457.

[115] Jokioinen et al. (2016), p. 52. It is important to note, because of the scope of this chapter, that the LLMC defines the right to limit by reference to 'shipowners and salvors', hence seemingly applying to autonomous vessels.

[116] Section 2(1) of Consumer Protection Act 1987.

[117] Brooke and Forrester (2005), p. 17.

[118] Rowland and MacDonald (2005), p. 214.

[119] C Reed et al., 'Responsibility, Autonomy and Accountability: Legal Liability for Machine Learning' (2016) Queen Mary University of London, School of Law, Legal Studies Research Paper, No. 243/2016, 6.

[120] Allianz (2017a, b), Khanna (2017), p. 13.

[121] Reed et al. (2016), p. 6.

can be argued that the very presence of personnel on board will allow preventative action to be taken unlike in the autonomous case.[122] Second, on a manned vessel, defined lines of communication between on-shore- and on-board personnel are required by the ISM Code. Therefore, contingency plans concerning scenarios of lost communication will be in place making the manned vessel safer in this instance. Nevertheless, it is important to bear in mind, as already pointed in this chapter that currently a number of shipping industry stakeholders are working in developing risk managements guidelines for autonomous vessels.

Finally, it should be noted that because of the advanced nature of autonomous software, the producer or his insurer, may avail himself of the "state of the art" defence should the product be deemed unsafe.[123] In *Commission v UK*[124] the defence refers to *"the state of scientific and technical knowledge, including the most advanced level of such knowledge, at the time when the product in question was put into circulation"*. Nevertheless, this defence can be easily rebutted just by proving that no reasonable producer would, considering the current state of knowledge, have discovered the defect at hand.[125]

7 Protection and Indemnity (P&I) Cover

A marine insurance policy has distinctive features from regular commercial insurance policies, being divided into two categories; the first being dedicated to the insurance of cargo wholly or in part by sea and in the second, the subject of insurance is the ship itself. Protection & Indemnity (P&I) insurance falls within the latter category.[126] Thus, when dealing with marine insurance, it is impossible not to discuss P&I Clubs, even if briefly, as they cover a wide range of liabilities including personal injury to crew, passengers and others on board, cargo loss and damage, oil pollution, wreck removal and dock damage.[127]

As cyber attacks, as already exposed, can lead to collision, personal injury, property damage, pollution or even shipwreck, and as a rule, most cyber risks will be covered under P&I Rules[128] with the International Group Pooling Agreement not being subject to cyber risk exclusion.[129]

[122] Bernauw (2017), p. 390.

[123] Section 4(1)(e) of Consumer Protection Act 1987; Reed et al. (2016), p. 6.

[124] (C-300/95) [1997] 3 CMLR 923.

[125] Section 4(60)(e) of Consumer Protection Act 1987.

[126] Gold (2002).

[127] I G P&I website, online at: www.igpandi.org/.

[128] Rules of the UK P&I Club Rule Book.

[129] UK P&I Club, 'Q&A, Cyber Risks and P&I Insurance' (2018) www.ukpandi.com/fileadmin/uploads/uk-pi/Documents/2018/Brochure/Cyber_Risks_and_PandI_Insurance.pdf accessed 09/09/2018.

Although some cyber risks might be excluded from coverage by virtue of exclusions relating to paperless trading[130] or P&I war risks, which include terrorist acts,[131] these seem to be included in the UK War Risk Clubs up to U$50 million in the aggregate or U$150 million for the Hellenic War Risks' membership as a whole.[132] Accordingly, claims excluded under traditional P&I pooling agreement would be settled by those clubs in a pro rata bases dependable on the losses in the policy year were to exceed the aggregate limit.[133]

Therefore, P&I Clubs are not only investing in helping the industry by issuing risk management guidelines,[134] as well as providing coverage, that seems to be sufficient so far, to cyber threats.

8 Conclusion

This chapter has demonstrated that with the advance of technology, the shipping industry was not only confronted with new risks arising from it, but currently faces the possible increase of liability with insurable interests potentially being left outside insurance policies. The need of current international and national regulations is eminent to keep the industry with its usual array of insurance protection.

Nevertheless, as it was shown, with the increase of new risks there is also the reduction of old risks. The expectation is that with the advent of new technology, the number of most common insurable claims will reduce.[135]

Part 1, Section 2 of the UK Automated and Electric Vehicles Act 2018, dealing with liability of insurers for automated vehicles, demonstrates that industry stakeholders can act fast and efficiently when their interests are at stake. Indeed, shipping industry stakeholders are working conspicuously to assess, manage and mitigate new risks. At the same pace, studies are being conducted to adapt current legislation with the use of new technology and creating more efficient systems.

Acknowledgements The authors thank the Scientific Committee of Association Internationale de Droit des Assurances (AIDA) Europe for awarding this paper with the AIDA Europe Academic Prize 2018.

[130]UK P&I Club Rule Book, Addendum for Owners.

[131]Rule 5E of the UK P&I Club Rule Book.

[132]Hellenic War Risks'C1- 2015 Cyber Losses/Computer Virus Risks www.hellenicwarrisks.com/fileadmin/uploads/hellenic/Docs/PDFs/HWRB_C1-2015_-_Cyber.pdf accessed 09/09/2018.

[133]UK P&I Club (2018).

[134]GARD (2017); North P&I Club, 'North P&I Club Highlights the Need for Increased Cyber Security (2016) www.nepia.com/news/press-releases-area/north-pi-club-highlights-the-need-for-increased-cyber-security/ accessed 30/08/2018.

[135]GARD (2017).

References

1 United State Code § 3
Allianz Global Corporate & Speciality (2017a) Ready to launch: Autonomous ships - Smart Sails. www.allianz.com/en_GB/press/news/business/insurance/170824-autonomous-shipping-smart-sails.html. Accessed 9 Sept 2018
Allianz Global Corporate & Speciality (2017b) Safety and Shipping Review 2017, An Annual Review of Trends and Developments in Shipping Losses and Safety. www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Safety_Shipping_Review_2017.pdf. Accessed 8 Sept 2018
Anderson P (2015) The ISM Code: a practical guide to the legal and insurance implications, 3rd edn. Informa
Arvanitis D, Constantino Chagas Lessa J (2014) Offshore platforms' seafarers: an excluded group within an overlooked sector? Eur Transp Law J 3:133–151
Bernauw K (2017) The insurance of driverless vehicles, pilotless aircraft and unmanned vessels. Eur Transp Law J LII(4):359–391
BIMCO et al (2016) Guidelines on Cyber Security Onboard Ships, Version 1.1
BIMCO et al (2017) Guidelines on Cyber Security Onboard Ships, Version 2.0
Blaskovic-Schnell I (2016) Mobile offshore units and notion of ship in the Norwegian maritime law: implications and challenges. In: Musi M (eds) The ship: an example of legal pluri-qualification. Il Diritto Marittimo – Quaderni, Bonono, pp 167–169
Bork K et al (2008) The legal regulation of floats and gliders—in quest of a new regime? Ocean Dev Int Law 39:298–328
Boyes H, Isbell R (2017) UK code of practice, cyber security for ships. UK Department of Transport
British Maritime Law Association (BMLA) (2018) Response to CMI Questionnaire on Unmanned Ships, EME_ACTIVE-568475036.1. https://www.bmla.org.uk/documents/2018/BMLA-Response-to-CMI-Questionnaire-on-Unmanned-Ships.pdf. Accessed 8 Aug 2018
Brooke M, Forrester I (2005) The use of comparative law in A & Others v National Blood Authority. In: Fairgrieve D (eds) Product liability in comparative perspective. Cambridge University Press
Burmeister HC et al (2014) Can unmanned ships improve navigational safety?. Transport Research Arena, Paris. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.846.5385&rep=rep1&type=pdf. Accessed 9 Oct 2018
Cambridge Dictionary Online (2018). https://dictionary.cambridge.org/dictionary/english/cyberattack
Cartwright JE (2011) Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations. http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf. Accessed 19 Sept 2018
Chouhan R (2015) Cyber crime escalation vs solutions: a literature snapshot. IJCTM 1:2. http://www.gyanvihar.org/researchjournals/cmt_vol_2_2.pdf. Accessed 14 Oct 2018
Commission v UK (C-300/95) [1997] 3 CMLR 923
Consumer Protection Act 1987 (UK)
Convention on the International Maritime Satellite Organization (IMSO), 1976
Cooper S (2018) Cyber risks, liabilities and insurance in the marine sector. In: Soyer B, Tettenborn A (eds) Maritime liabilities in a global and regional context, 1st edn. Routledge, London, pp 103–118
Danish Maritime Authority (2017) Analysis of Regulatory Barriers to the Use of Autonomous Ships Final Report. Ramboll
Danish Merchant Shipping Act
Daum O, Stellplug T (2017) The implications of international law on unmanned merchant vessels. J Int Marit Law 5:363–374

Davey J (2013) The reform of insurance warranties: a behavioural economics perspective. J Bus Law 1:118–137
Dixon v Sadler (1839) 5 M & W 405
DNV-GL (2016) Recommended Practice – Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation. DMVGL-RP-0496
Doak v Weekes & Commercial Union Assurance Co plc [1986] 82 FLR 334
Donaldson JL (1999) The ISM Code: the road to discovery? LMCLQ 4:526–535
European Product Liability Directive (1985/374)
Falkanger T et al (2011) Scandinavian maritime law – the Norwegian perspective, 3rd edn. Universitetsforlaget, Oslo
Gahlen S (2014) Ships revisited: a comparative study. J Int Marit Law 20:252–269
GARD (2017) Cyber Security- Managing the Threat. http://www.gard.no/Content/21112216/Cyber Security. Accessed 14 May 2018
Gauci GM (2016) Is it a vessel, a ship or a boat, is it just a craft, or is it merely a contrivance. J Marit Law Commer 47:479–499
Gault S et al (2016) Marsden and Gault on collisions at sea. Sweet & Maxwell, London
Gold E (2002) Gard handbook on P&I insurance. Gard, Norway
Hellenic War Risks'C1- 2015 Cyber Losses / Computer Virus Risks. https://www.hellenicwarrisks.com/fileadmin/uploads/hellenic/Docs/PDFs/HWRB_C1-2015_-_Cyber.pdf. Accessed 9 Sept 2018
HM Government-UK (2016) National Cyber Security Strategy 2016–2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. Accessed 18 Aug 2018
Hong Kong Fir Shipping Co Ltd v Kawasaki Kisen Kaisha Ltd [1962] 2 WLR 474
Hu L et al (2017) COLREGS – compliant path planning for autonomous surface vehicles: a mutiobjective optimization approach. IFAC PapersOnLIne 50(1):13622–13677
I G P&I website, online at: www.igpandi.org/
Jokioinen E et al (2016) Advanced Autonomous Waterborne Applications (AAWA) Position Paper, Remote and Autonomous Ships: The Next Steps (Rolls Royce). Available at www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf. Accessed 15 Aug 2018
Katsivela M (2014) Perils of the Sea under English, French and Greek Law; a perilous Venture? J Int Marit Law 20(5):343–355
Khanna R (2017) Heavier weather, increased safety concerns, emerging risks threaten shipping industry. Marit Risk Int 31(1):13
Kongsberg (2018) Autonomous Ship Project, Key Facts about YARA Birkeland. www.km.kongsberg.com. Accessed 15 Aug 2018
KPMG (2017) Cyber Crime Survey Report, Insights and Perspectives. https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf. Accessed 30 Sept 2018
Lazaratos G (1969) The definition of ship in national and international law. RHDI 22:57
Lloyd's Register (2017) Cyber Enabled Ships – Ship Right Procedure Assignment For Cyber Descriptive Notes for Autonomous & Remote Access Ships. Lloyd's Register Guidance Document, Version 2.0
Lowe V (2011) Report on the Interpretation of the Term 'ship' in the 1992 Civil Liability Convention. In Consideration of the Definition of 'Ship', International Oil Pollution Compensation Funds (IOPC/OCT11/4/4). documentservices.iopcfunds.org/meeting-documents/download/docs/3535/lang/en/. Accessed 18 Aug 2018
Macfarlane R (2017) How to Mitigate Your Risk. Maritime Risk International (18/10/2017)
Marine Insurance Act 1906 (UK)
Marine Insurance Act 1909 (Australian)
Marllow P (2015) Cyber Liability in the Marine Industry Report. https://www.ajg.com/media/1697987/cyber-liability-for-the-marine-industry.pdf. Accessed 9 Oct 2018
McFadden v Blue Star Line [1905] 1 KB 697

Mellilo F (2016) The human element in the autonomous shipping era – essential to avoid gaps. Maritime Risk International, 21/11/2016
Merchant Shipping Act 1894 (UK)
Merchant Shipping Act 1995 (UK)
Merchants Marine Insurance v North of England P & I (1926) 26 Ll L Rep 201
NATO, Translation of Cyber - the Good, the Bad and the Bug-free https://www.nato.int/docu/review/2013/Cyber/timeline/DK/index.htm. Accessed 30 Apr 2018
North P&I Club (2016) North P&I Club Highlights the Need for Increased Cyber Security. http://www.nepia.com/news/press-releases-area/north-pi-club-highlights-the-need-for-increased-cyber-security/. Accessed 30 Aug 2018
P Samuel & Co Ltd v Dumas [1924] AC 431
Polpen Shipping Co Ltd v Commercial Union Assurance Co Ltd [1943] 1 All ER 162; 74 Ll L Rep 157
President of India v West Coast Steamship Co [1963] 2 Lloyd's Rep 278
Protocol to Amend the International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading ("Visby Rules") 1968
R v Goodwin [2005] EWCA Crim 3184; [2006] 1 Lloyd's Rep 432
Redmond v Smith (1844) 7 Man & Gr 457
Reed C et al (2016) Responsibility, autonomy and accountability: legal liability for machine learning. Queen Mary University of London, School of Law, Legal Studies Research Paper, No. 243/2016
Reynardson B et al (2017) CMI International Working Group Position Paper on Unmanned Ships and the International Regulatory Framework
Rowland D, MacDonald E (2005) Information technology law, 3rd edn. Cavendish Publishing
Soyer B (2017) Warranties in marine insurance. Routledge, Oxon
St John Shipping Corp v Joseph Rank Ltd [1957] 1 QB 267
Steedman v Scofield [1992] 2Lloyd's Rep 163
Switzerland Insurance Australia Ltd v Mowie Fisheries Pty Ltd[1997] FCA 231
The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention), 1988
The Convention on Limitation of Liability for Maritime Claims (LLMC), 1976
The Eurasian Dream [2002] 1 Lloyd's Rep 719
The International Convention for the Prevention of Pollution from Ships (MARPOL), 73/78
The International Convention for the Safety of Life at Sea (SOLAS), 1974
The International Convention for the Unification of Certain Rules of Law Relating to Bills of Lading (Hague Rules), 1924
The International Convention on Civil Liability for Bunker Oil Pollution Damage (BUNKER), 2001
The International Convention on Salvage, 1989
The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978
The International Maritime Organization (2017a) Guidelines on Maritime Cyber Risk Management MSC-Fal.1/Circ.3
The International Maritime Organization (2017b) Maritime Safety Committee Maritime Cyber Risk Management in Safety Management Systems Resolution MSC. 428(98)
The International Maritime Organization (2018a) Briefing: IMO Takes First Steps to Address Autonomous Ships. http://www.imo.org/en/mediacentre/pressbriefings/pages/08-msc-99-mass-scoping.aspx. Accessed 10 June 2018
The International Maritime Organization (2018b) Maritime Safety Committee (MSC), 99th session 16–25 May 2018
The International Maritime Safety Management (ISM) Code
The International Regulations for Preventing Collisions at Sea (COLREGS Convention), 1972
The International Ship and Port Facility Security (ISPS) Code

The Madeleine [1967] 2 Lloyd's Rep 224
The Maritime Executive (MAREX) (2018) Shipbuilder Chosen for Yara Birkeland. https://www.maritime-executive.com/article/shipbuilder-chosen-for-yara-birkeland. Accessed 15 Aug 2018
The Maritime Labour Convention, 2006
The Nordic Ferry [1991] 2 Lloyd's Rep 591
The Norwegian Maritime Code (Act No. 39 of 1994)
The Saldanha [2011] 1 Lloyd's Rep 187
The Star Sea [2001] 1 Lloyd's Rep 389
The United Nations Convention on the Law of the Sea (UNCLOS), 1980
The Xantho (1887) 12 App Cas 503
Thompson v Hopper (1856) 6 E & B 937
Tucker P (2014) Major Cyber Attack Will Cause Significant Loss of Life by 2025, Experts Predict. http://www.defenseone.com/threats/2014/10/cyber-attack-will-cause-significant-loss-life-2025-experts- predict/97688/. Accessed 1 Apr 2018
UK Automated and Electric Vehicles Act 2018
UK P&I Club (2018) Q&A, Cyber Risks and P&I Insurance. https://www.ukpandi.com/fileadmin/uploads/uk-pi/Documents/2018/Brochure/Cyber_Risks_and_PandI_Insurance.pdf. Accessed 9 Sept 2018
UK P&I Club Rule Book
United Nations Convention on Conditions for Registration of Ships, 1986
US Department of transportation, MARAD (2018). https://www.marad.dot.gov/office-of-security/msci/alert/2018/. Accessed 15 Sept 2018
Van Hooydonk E (2014) The law of unmanned merchant shipping—an exploration. J Int Marit Law 20:403–423
Veal R, Tsimplis M (2017) The integration of unmanned ships into the Lex Maritima. Lloyd's Marit Commer Law Q 2:303–336
Wedderburn v Bell (1807) 1 Camp 1; 170 ER 855
Wee V (2017) Malaysian Bunker Company Cheated of $1.1m in Email Payment Scam. http://www.seatrade-maritime.com/news/asia/malaysian-bunker-company-cheated-of-1-1m-in-email-payment-scam.html. Accessed 20 Sept 2018
Yara (2018) YARA Selects Norwegian Shipbuilder VARD For Zero-Emission Vessel Yara Birkeland. https://www.yara.com/corporate-releases/yara-selects-norwegian-shipbuilder-vard-for-zero-emission-vessel-yara-birkeland/. Accessed 15 Aug 2018.
Yeomans G (2014) Autonomous Vehicles- Handing over Control: Opportunities and Risks for Insurance. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/autonomous-vehicles. Accessed 9 Oct 2018

Probing Civil Liability Insurance for Unmanned/Autonomous Merchant Ships

Ling Zhu and Richard W. W. Xing

1 Introduction

Shipping plays an essential role in international trade, since around 90% of world trade is transported by the international shipping industry.[1] From the origin of ships about 6000 years ago,[2] through iron and steam vessels, and down to modern times,[3] evolution of the merchant ship enables itself to now navigate longer, further, safer, with fewer risks, and less labour. Currently, it is not just ship designers who are thinking ahead and anticipating the future of unmanned/autonomous ships—several

The writing of this paper was financially supported by a research grant awarded by the Department of Logistics and Maritime Studies, The Hong Kong Polytechnic University (Account Code: G-UADQ).

[1]Available at: http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade.

[2]Forde (2015), p. 13.

[3]Chatterton (1915), p. 273.

L. Zhu (✉)
Shipping Insurance and Law, Department of Logistics and Maritime Studies, Faculty of Business, The Hong Kong Polytechnic University, Hung Hom, Hong Kong
e-mail: ling.zhu@polyu.edu.hk

R. W. W. Xing
Department of Logistics and Maritime Studies, Faculty of Business, The Hong Kong Polytechnic University, Hung Hom, Hong Kong

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_16

governments are also motivated by this trend, such as Norway,[4] Finland,[5] and Australia,[6] which have already opened marine water areas for testing unmanned/autonomous ships.

The introduction of unmanned/autonomous merchant ships may on the one hand eliminate risks caused by human faults during a marine adventure, and thus enhance navigational safety[7]; on the other hand, it will create changes in shipping practice, leading to new risks. Although the development of technology has increasingly enhanced the security and safety of ships, marine navigation is a high-risk adventure, and hence needs the safeguard provided by insurance.

Marine Insurance, the oldest of the many forms of protection against losses,[8] is a response to the expansion of sea trade,[9] and provides cover against losses incidental to marine adventure.[10] As with traditional merchant ships, unmanned ships may also trigger many different civil liabilities, such as collision liability, cargo liability and pollution liability, to name a few. In addition, the relevant autonomy level of the unmanned ship will impact profoundly on this question.[11]

Against this background, this article aims to probe civil liability insurance for unmanned/autonomous merchant ships. Accordingly, after this introduction, it will first discuss the various kinds of civil liability that ships incur, and their corresponding insurance arrangements. The article then examines the conceptual difficulties of unmanned/autonomous ships, along with the changes and risks they will create. Finally, the article focuses on key issues related to the insurance of unmanned/autonomous ships, including who is eligible to take out the insurance and who may be the insurer.

[4]Norway opened its first test area in the world for unmanned ships in 2016, and now it has three test areas for unmanned ships, namely, Trondheim fjord, Sunnmøre region, and Oslofjord. Available at: https://worldmaritimenews.com/archives/237297/norway-opens-new-test-area-for-autonomous-ships/.

[5]Finland opened its first test area for autonomous ships in August 2017. Available at: https://worldmaritimenews.com/archives/227275/first-test-area-for-autonomous-ships-opened-in-finland/.

[6]The Australian Maritime Safety Authority granted a request for the operation of remotely operated unmanned ships in Australian waters in August 2017, see Working Boats issue 11 by AMSA 299 on 8 February 2018, p. 15, available at: https://www.amsa.gov.au/news-community/newsletters/working-boats-issue-11.

[7]Burmeister et al. (2014), pp. 1–13; Wahlström et al. (2015), pp. 1038–1045.

[8]Noussia (2007), p. 1.

[9]Gurses (2016), p. 2.

[10]English Marine Insurance Act 1906, Sec. 1.

[11]*CMI International Working Group Position Paper on Unmanned Ships and the International Regulatory Framework,* p. 19, available at: http://comitemaritime.org/Maritime-Law-for-Unmanned-Craft/0,27153,115332,00.html.

2 The Ship's Liability and Civil Liability Insurance

2.1 The Ship's Expanding Liabilities

Basically, there are two types of ship's civil liability: contractual liability and third-party liability[12]; the divergence of these relies on whether the liability is incurred within the contract clauses or if the liability is incurred because of private wrongs causing damage or losses to a third-party. At the same time, the basis of liability may also be classified into two types: one is fault-based liability, where fault/negligence, including breaches of legal rules, causes liability[13]; and the other is strict liability, where liability is incurred without requiring fault/negligence but where merely causing the relevant harm is sufficient to incur liability.

Generally, the civil liability of shipping is regulated nationally, where the relevant rules may vary from one jurisdiction to another.[14] With the development of international regulations on shipping, an increasing number of civil liabilities are covered by maritime conventions, including but not limited to: (1) the International Convention on Civil Liability for Oil Pollution Damage (CLC),[15] (2) the 1992 Protocol to the International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (FUND 1992),[16] (3) the Convention relating to Civil Liability in the Field of Maritime Carriage of Nuclear Material (NUCLEAR),[17] (4) the Athens Convention relating to the Carriage of Passengers and their Luggage by Sea (PAL),[18] (5) the Convention on Limitation of Liability for Maritime Claims (LLMC),[19] (6) the International Convention on Liability and Compensation for Damage in Connection with the Carriage of Hazardous and Noxious Substances by Sea (HNS),[20] (7) the International Convention on Civil Liability for Bunker Oil Pollution Damage (BUNKER),[21] (8) the Nairobi

[12]Zhu (2014), p. 64.

[13]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 84.

[14]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 84.

[15]Adoption: 29 November 1969; Entry into force: 19 June 1975; Being replaced by 1992 Protocol: Adoption: 27 November 1992; Entry into force: 30 May 1996.

[16]Adoption: 18 December 1971; Entry into force: 16 October 1978; superseded by 1992 Protocol: Adoption: 27 November 1992; Entry into force: 30 May 1996.

[17]Adoption: 17 December 1971; Entry into force: 15 July 1975.

[18]Adoption: 13 December 1974; Entry into force: 28 April 1987; 2002 Protocol: Adoption: 1 November 2002; Entry into force: 23 April 2014.

[19]Adoption: 19 November 1976; Entry into force: 1 December 1986; Protocol of 1996: Adoption: 2 May 1996; Entry into force: 13 May 2004.

[20]Adoption: 3 May 1996; Not in force; superseded by 2010 Protocol: Adoption: 30 April 2010; Not yet in force.

[21]Adoption: 23 March 2001; Entry into force: 21 November 2008.

International Convention on the Removal of Wrecks (the Nairobi Wreck Removal Convention),[22] and (9) the Maritime Labour Convention (MLC).[23]

As for the basis of liability, fault-based liability is prescribed for some liabilities, for example: The 1910 Collision Convention[24] regulates the liability for collisions based on the fault of ships[25]; and it states that if the collision is caused by the fault of one of the vessels, liability to make good the damages attaches to the one which has committed the fault.[26] On the other hand, strict liability is associated with certain other liabilities: for instance, shipwreck removal liability under Article 10 of the Nairobi Wreck Removal Convention[27] and oil pollution liability under Article III of CLC, 1992.[28]

2.2 *Marine Insurances for a Ship's Civil Liability*

Marine insurance insures against the losses incidental to marine adventure. There are different types of marine insurance. Cargo insurance, freight insurance, and H&M insurance (which covers some of the liabilities related to ships) are regarded as a form of property insurance for covering the loss of or damages to property (e.g. the ship itself, or a consignment of goods). In addition to these, P&I insurance covers a ship's third-party liability insurance. It seems that among these H&M insurance and P&I insurance thus provide insurance for ships' civil liability.

Although H&M insurance provides cover for the loss of or damage to the insured vessels, the collision clause in many H&M policies appears to be a "3/4ths Collision Liability" Clause, which indicates that the H&M underwriters agree to indemnify the assured for three-fourths of any sum or sums paid by the assured to others in consequence of the insured vessel coming into collision with any other vessel.[29] This incomplete cover provided by the 3/4ths Collision Liability Clause was intended as a way of motivating the assured to assume part of the risks, thus prompting them to take greater care in navigating. To cover this extra 1/4th collision

[22]Adoption: 18 May 2007; Entry into force: 14 April 2015.

[23]Adopted by the International Labour Conference at its 94th (Maritime) Session (2006). Amendments approved by the International Labour Conference at its 103rd Session (2014).

[24]Convention for the Unification of Certain Rules of Law with respect to Collisions between Vessels (Brussels, 23 September 1910) is the most successful private law harmonisation Convention of the Comité Maritime International (CMI).

[25]Van Hooydonk (2014), p. 421.

[26]1910 Collision Convention, Article 3.

[27]See Nairobi Wreck Removal Convention, Article 10, "the registered owner shall be liable for the costs of locating, marking and removing [a] wreck".

[28]See CLC, 1992, Article III, "the owner of a ship at the time of an incident. . .shall be liable for any pollution damage caused by the ship as a result of the incident".

[29]Institute Time Clauses - Hulls 1.10.83, Article 8. INTERNATIONAL HULL CLAUSES (01/11/03), Article 6.

liability, the assureds can either agree to an optional additional clause within the hull insurance,[30] or alternatively they may resort to additional P&I club insurance.

The P&I insurance provided by the Clubs is a primary means for shipowners to protect themselves against third-party civil liability claims.[31] The risks listed in the Club Rulebooks are expanding. However, it is not compulsory for a shipowner to select all risks, since he can choose and even negotiate the perils to be covered.[32] Although different P&I Clubs offer differing degrees of cover for such marine risks, most of the P&I rules include but do not limit themselves to the following liabilities: liabilities in respect of crew and passengers, liability for other persons carried on/off board, stowaways, refugees or persons saved at sea, life salvage, collision with other ships, damage to fixed or floating objects, pollution, liability for obstruction and wreck removal, general average, and salvage.[33]

2.3 Other Insurances Covering a Ship's Liability

Some non-marine liabilities may also be invoked in association with the operation or navigation of the ship. There are the Kidnap and Ransom insurance (K&R) and Mortgagees Interest Insurance (MII). K&R insurance, which is designed to protect individuals and corporations operating in high-risk areas around the world, may cover the crew in case of piracy and maritime crimes. MII insurance will protect a bank or lender's mortgage if the insurers of the borrower or shipowner do not respond.[34]

Certain other non-marine insurances may also be related to a ship's liability, such as cybersecurity insurance. It has been excluded by the Institute Cyber Attack Exclusion Clause CL380,[35] since the risk of being cyberattacked is not particularly a marine risk. In addition, product liability insurance is usually taken out by ship builders and software designers to protect against any possible blame for their

[30]INTERNATIONAL HULL CLAUSES (01/11/03), Article 38.

[31]Hurd (1952), pp. 147–148.

[32]Zhu (2007), p. 60.

[33]See Gard Rules 2016.

[34]The Swedish Club - Mortgagees Interest Insurance (MII), available at: https://www.swedishclub.com/insurance/marine/mortgagee-interest-insurance-mii/.

[35]Institute Cyber Attack Exclusion Clause CL3801.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.2.1 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

product's defects. However, in the case of unmanned/autonomous ships, cybersecurity and manufacturing reliability are of prime concern, so these two kinds of insurance thus deserve additional consideration elsewhere in this article.

3 The Unmanned/Autonomous Merchant Ship

Unmanned/autonomous ships have already been operated by some States, but used exclusively on government non-commercial services.[36] Introducing unmanned ships to commercial shipping is a development trend, and it will certainly bring changes and challenges to the shipping industry. The foremost challenge is its defining scope and issues related to its seaworthiness and legality.

3.1 Definition and Classification

As the name suggests, it is obvious that an unmanned ship is a ship that can navigate in the sea without any crew on board. In contrast, an autonomous ship can either have no crew or less crew on board during navigation. Similarly, there are several other expressions that may fall into the category of the unmanned/autonomous ship; for example, a ship with an E-navigation plan by the IMO[37] could be implemented by enhancing the autonomy level for ships. The definition is still under debate, as is the idea of a smart ship, which is even harder to define. Therefore, for the purpose of this article, we use the title unmanned/autonomous ship to identify this new kind of ship. The most recent progress on the international regulatory framework for unmanned/autonomous ships is on IMO's ninety-eighth session 2018 of the Maritime Safety Committee, where the IMO endorsed a definition for the Maritime Autonomous Surface Ship (MASS) as a ship that, to varying degrees, can operate independently of human interaction.[38]

It is necessary to consider whether or not the unmanned/autonomous ship can fall within the definition of "ship" in the existing regulatory framework. Under

[36]McLaughlin (2011), p. 100.

[37]E-navigation is defined by the IMO as "...the harmonized collection, integration, exchange, presentation and analysis of marine information on board and ashore by electronic means to enhance berth to berth navigation and related services for safety and security at sea and protection of the marine environment." Available at: http://www.imo.org/en/OurWork/safety/navigation/pages/enavigation.aspx.

[38]IMO takes first steps to address autonomous ships, available at: http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx.

international law, the United Nations Convention on the Law of the Sea (UNCLOS), which provides a general legal framework relating to ocean governance, leaves the question to the flag State to establish the conditions for giving ships their nationality.[39] Van Hooydonk E. categorises the legal definitions of 'ship' and 'vessel' in numerous international public law maritime conventions, private maritime law conventions, and national maritime laws, and a heterogeneous picture on ship definition has been found.[40] It has thus been concluded with a considerable degree of certainty that no significant hurdle has been found that would prevent unmanned/autonomous ships from falling within the various similar definitions in international conventions.[41] Having a crew on board, including a master is not generally regarded as an essential part of the notion of a ship under international law.[42] The IMO has shown its attitude towards this question by examining how safe, secure and environmentally sound MASS operations may be addressed in IMO instruments. The list of instruments to be covered in the MSC's scoping exercise for MASS operations includes those covering safety; collision regulations; loading and stability; training of seafarers and fishers; search and rescue; tonnage measurement; and special trade passenger ship instruments.[43] At least it is known that, in these IMO conventions, the unmanned/autonomous ship will be regulated as a "ship" defined for the purpose of these conventions to exercise international regulatory scoping.

One more question that arises is whether or not the classification societies will accept the unmanned/autonomous ship? A classification society is a non-governmental organisation that establishes and maintains technical standards for the construction and operation of ships. The original role of a classification society was to supply reliable information about the conditions of ships for underwriters and cargo owners[44]; for example, a classification certificate issued by a classification society is required for a ship's owner to be able to obtain marine insurance for the ship.[45] Today, the role of classification societies is evolving towards a global function that integrates many aspects of ship safety: construction and operation standards, technical requirements, and human factors.[46] Regarding unmanned/autonomous ships, the Lloyd's Register—the oldest classification society, which was found in 1760—launched a goal-based code that takes a structured approach to the assessment of unmanned marine systems (UMS) against a set of

[39]UNCLOS, Article 91.

[40]Van Hooydonk (2014), p. 406.

[41]The Nairobi International Convention on the Removal of Wrecks, 2007; the International Convention on Salvage, 1989; the 1992 Protocol to the Convention on Civil Liability for Oil Pollution Damage, 1969.

[42]Van Hooydonk (2014), p. 406. See also: Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 37.

[43]IMO takes first steps to address autonomous ships, available at: http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx.

[44]Boisson (1994), pp. 363–377.

[45]Classification society, available at: https://en.wikipedia.org/wiki/Classification_society.

[46]Boisson (1994), pp. 363–377.

safety and operational performance requirements.[47] In the Design Code for Unmanned Marine Systems by the Lloyd's Register, the unmanned/autonomous ship has been categorised based on the autonomy level (AL) from AL0 (no autonomous function) to AL6 (fully autonomous), which indicates unsupervised operation where decisions are entirely made and actioned by the system during the mission.[48] Although the Code launched by the Lloyd's Register is still a goal-based one to provide a set of Performance Requirements that support design innovation,[49] if the emerging unmanned/autonomous ship can meet the requirements set by the Lloyd's Register, then it seems that the classification societies will accept the unmanned/autonomous ship.

3.2 Seaworthiness and Legality

Although the European Commission co-funded project MUNIN[50] and certain other scientific researchers[51] have established that the application of unmanned/autonomous ships will hopefully decrease the number of accidents caused by human faults, the safety and security of unmanned/autonomous ships is still in doubt.[52] Unmanned/autonomous ships will inevitably rely upon computer technology and autonomous systems,[53] which thus raises concerns about both the safety of navigation and seaworthiness of the ship. Under such debates on security, whether or not the navigation of unmanned/autonomous ships will be accepted by both international law and domestic law is becoming an important question to examine.

[47]New code to certify unmanned vessels announced, available at: https://www.lr.org/en/latest-news/new-code-to-certify-unmanned-vessels-announced/.

[48]Lloyd's Register. Design Code for Unmanned Marine Systems, February 2017, Section 4.1.2, available at: https://www.lr.org/en/latest-news/new-code-to-certify-unmanned-vessels-announced/.

[49]Ibid, Section 2.1.3.

[50]The project MUNIN—Maritime Unmanned Navigation through Intelligence in Networks—as a collaborative research project, co-funded by the European Commission under its Seventh Framework Programme, has found the following result:Unmanned vessels can contribute to the aim of a more sustainable maritime transport industry. . . . .The autonomous ship represents a long-term, but comprehensive solution to meet these challenges, as it bears the potential to: 1) Reduce operational expenses; 2) Reduce environmental impact; and 3) Attract seagoing professionals. Available at: http://www.unmanned-ship.org/munin/about/munin-results-2/.

[51]Burmeister et al. (2014), pp. 1–13.
Wahlström et al. (2015), pp. 1038–1045.

[52]Wróbel et al. (2017), pp. 155–169.

[53]"Future Proofed? What Maritime Professionals Think about Autonomous Shipping?" Report by NAUTILUS Federation, A Federation of Maritime Professionals.

Seaworthiness

The concept of seaworthiness has its origin in common law, where it has been developed through several centuries of case law.[54] The criteria laid down in the Hague/Visby Rules for seaworthiness in association with sea carriage are normally regarded as the most acceptable ones, which require the carrier to exercise due diligence to properly man, equip and supply the ship.[55] When discussing seaworthiness of a vessel, many factors may be considered: design and construction[56]; machinery, equipment and navigational aids[57]; sufficiency and competence of the crew,[58] sufficiency and quality of fuel[59]; and the stowage of cargo and its stability.[60] The seaworthiness in insurance law contains similar elements.[61] A ship is deemed to be seaworthy when it is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured.[62]

Seaworthiness of unmanned/autonomous ships shall be examined and proved at the time when their civil liability insurance is being considered. P&I clubs could avoid liability under claims by virtue of the unseaworthiness of the vessel where the member was privy in advance of the incident to such unseaworthiness.[63] In the case

[54]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 81.

[55]Hague-Visby Rules, Art. III.

[56]*Anglis and Co v P and O Steam Navigation Co* [1927] 2 KB 456; *The Marine Sulphur Queen* [1973] 1 Lloyd's Rep 88, US CA; *The Torenia* [1983] 1 Lloyd's Rep 210; and *Coltman v Bibby Tankers Ltd, 'Derbyshire'* [1986] 1 WLR 751. See Hodges (2012), p. 308.

[57]*The President of India* [1963] 1 Lloyd's Rep 1; *The Antigoni* [1991] 1 Lloyd's Rep 209; *The Yamatogawa* [1990] 2 Lloyd's Rep 39; *The Theodegmon* [1990] 1 Lloyd's Rep 52; *The Subro Valour* [1995] 1 Lloyd's Rep 509; *The Maria* (1937) 91 Fed Rep (2d) 819; and *The Irish Spruce* [1976] 1 Lloyd's Rep 63. See Hodges (2012), p. 308.

[58]*Wedderburn and Others v Bell* (1807) 1 Camp 1; *The Makedonia* [1962] 1 Lloyd's Rep 316; *Standard Oil Co of New York v Clan Line Steamers Ltd* [1924] AC 100; and *Hong Kong Fir Shipping Co v Kawasaki Kisen Kaisha* [1962] 2 QB 26; [1961] 2 Lloyd's Rep 478. See Hodges (2012), p. 308.

[59]*Louis Dreyfus and Co v Tempus Shipping Co* [1931] AC 726, HL; *Fiumana Società di Navigazione v Bunge and Co Ltd* [1930] 2 KB 47; *Thin v Richards* [1892] 2 QB 141; *McIver and Co v Tate Steamers Ltd* [1903] 1 KB 362; and *Northumbrian Shipping Co v Timm and Son Ltd* [1939] AC 397. See Hodges (2012), p. 308.

[60]*The Aquacharm* [1982] 1 Lloyd's Rep 7; *The Friso* [1980] 1 Lloyd's Rep 469; *Elder Dempster and Co Ltd v Paterson, Zochonis and Co* [1924] AC 522; and *Smith Hogg and Co v Black Sea and Baltic Insurance Co* [1940] AC 997. See Hodges (2012), p. 308.

[61]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 92.

[62]English Marine Insurance Act 1906, Sec. 39(4).

[63]Hazelwood and Semark (2010), para. 11.22. In the China Shipowners Mutual Assurance Association (CPI) 2017/2018 Rules, unseaworthiness is associated with the wilful misconduct of a Member in RULE 8, which states that the CPI shall not be liable for any liabilities, losses, damages, costs or expenses which result from the Member's knowingly sending the entered ship to sea in an unseaworthy condition.

of unmanned/autonomous ships, the lack of any human physical presence on board the ship, and doubts as to its technical reliability, are deemed to be the two biggest challenges for it to meet the requirement of seaworthiness.

The need to be "properly manned" is the most controversial point for unmanned/autonomous ships to prove their seaworthiness,[64] since unmanned/autonomous ships may have no crew on board or even no one who can intervene during the navigation. However, as discussed earlier, the requirement of seaworthiness does not require every ship to be manned, and the word "properly" allows for an interpretation by which manning would be appropriate for each individual ship considering the specific type and voyage[65]; and therefore both "no manning" and "low manning" could be appropriate. As for the technical reliability of unmanned/autonomous ships, although scientific uncertainties still exist, international regulators[66] as well as several States[67] are trying to introduce some standard guidelines and technical codes for the construction of unmanned/autonomous ships. Accordingly, homogeneous technical standards and regulations, as well as their acceptance by classification societies, will be an important way forward to ensuring a functioning insurance market for unmanned/autonomous ships.[68]

Legality

For the unmanned/autonomous ship, two aspects of legality shall be discussed: the legality of the ship itself and the legality of navigation. The answer to the legality of the ship is closely related to the issue as to whether or not the unmanned/autonomous ship can be treated as a "ship". As discussed above, it seems that there are no

[64]Carey L J. "All Hands off Deck? The Legal Barriers to Autonomous Ships". *NUS Centre for Maritime Law Working Paper*, 2017.

[65]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 92.

[66]The Maritime Safety Committee has begun to undertake a regulatory scoping exercise to determine how the safe, secure and environmentally sound operation of Maritime Autonomous Surface Ships (MASS) might be introduced in IMO instruments. See IMO, Report of the Maritime Safety Committee on Its Ninety-Eighth Session, MSC 98/23, pp. 78–79. CMI and other organisations had already commenced a gap analysis relating to the regulatory work for the introduction of unmanned/autonomous ships. See *CMI International Working Group Position Paper on Unmanned Ships and the International Regulatory Framework*, available at: http://comitemaritime.org/Maritime-Law-for-Unmanned-Craft/0,27153,115332,00.html.

[67]UK's maritime sector body Maritime UK has launched a new Industry Code of Practice for the design, construction and operation of autonomous maritime systems. Available at: https://www.maritimeuk.org/media-centre/news/uk-launches-industry-code-practice-autonomous-vessels/. The Code of Practice can be found at: www.maritimeuk.org/mas-cop. The Danish Maritime Authority has also published a report on analysis of regulatory barriers to autonomous ships in December 2017. See Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017.

[68]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 93.

significant legal barriers for an unmanned/autonomous ship to be recognised as a ship under international law; however, legal uncertainties still exist, since various domestic jurisdictions may have different legislations on this question.

As for the legality of navigation, the issue could be more complicated. Based upon the law of the sea, the sea may be delimitated into different jurisdictions, and the answers to legality of navigation would be different in each:

(1) Navigation is conducted within one national water: Under this circumstance, the legality of the ship determines the legality of navigation. This means that an unmanned/autonomous ship can lawfully navigate in the waters of a nation as long as that nation has recognised the legality of such unmanned/autonomous ship.
(2) Navigation is carried out solely in international waters: This is a rather theoretical issue, since in reality it is not possible for a ship to navigate solely in international waters and never come into a port. If the ship only navigates in international waters, the UNCLOS will be applicable or referable. Based upon the provisions in the UNCLOS, for ships' navigation on the high seas, the flag states have the obligation to take measures for ships flying its flag and ensure safety at sea with regard, inter alia, to: (a) the construction, equipment and seaworthiness of ships; and (b) the manning of ships, labour conditions and the training of crews, considering the applicable international instruments.[69] Accordingly, seaworthiness and manning will be the main issues for the flag states to consider when introducing unmanned merchant ships. However, UNCLOS also require the states to implement the relevant international rules and standards[70] developed by or through the "competent international organization", which means the IMO.[71] Therefore, if the IMO instruments are amended to introduce unmanned ships,[72] such obligations established under UNCLOS may not be interpreted and implemented without referring to them. In other words, the requirements for seaworthiness and manning, which currently apply to traditional merchant ships, may have to be amended for a better fit with unmanned/autonomous ships to satisfy the navigation legality.

[69]UNCLOS, Article 94 (3).

[70]UNCLOS, Article 94 (3) (b).

[71]"The competent international organization," as used in UNCLOS Articles 22, 41, 53 and 60, means the International Maritime Organization (IMO) or its successor. Walker (2012), p. 138. Kingham and McRae (1979), pp. 106–132. Mihneva-Natova A. The Relationship Between United Nations Convention on the Law of the Sea and the IMO Conventions, the United Nations and the Nippon Foundation of Japan Fellow, 2005. Available at: http://www.un.org/depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/natova_0506_bulgaria.pdf.

Secretariat IMO. Implications of the United Nations Convention on the Law of the Sea for the International Maritime Organization[J]. Study by the Secretariat of the International Maritime Organization (IMO) ||, LEG/MISC, 2008, 6(10). Available at: http://www.imo.org/en/OurWork/Legal/Documents/LEG%20MISC%208.pdf.

[72]IMO takes first steps to address autonomous ships, available at: http://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx.

(3) Navigation among jurisdictional waters of different states as well as international waters: A ship often needs to navigate across the ocean and from one national waters to another, so the legality of an unmanned/autonomous ship's navigation in such a situation thus needs to be considered by taking account of both the international laws and the various domestic rules. If there were an incident, questions over the legality of navigation would be more complicated, since all legal elements involved in the incident need to be considered, such as: which national waters the ship in question was in; the flag State(s) of the involved ships; and other issues.[73]

So it seems necessary to further clarify the legality issues under both international and domestic law. The Danish Maritime Authority in its report suggested that it would be necessary to amend Article 94 of UNCLOS to expressly allow for unmanned ships.[74] However, for a convention with 148 national parties, it will not be easy to amend it without clear mechanisms for amendment.[75] Maybe it is, therefore, more feasible for national legislations and IMO instruments to provide interpretations on the legality of unmanned/autonomous ships.

Changes and New Risks

As previously mentioned, it is argued that introducing unmanned/autonomous ships into practice may increase the efficiency of shipping operations and enhance the sustainability of maritime transport as a whole.[76] However, the changes and potential risks that will be brought about by the introduction of unmanned/autonomous ships must also be fully explored.

The first obvious change is the application of computer and communication technologies, which require a combination of remote, automatic and autonomous control systems. An unmanned/autonomous ship needs wireless monitoring and control functions both on and off board, which then raises concerns about the safety of navigation. In a survey report provided by NAUTILUS Federation, eleven safety risks are highlighted, these being mainly related to the safety of software maintenance and navigational safety.[77] This change raises three major potential risks:

[73]The Danish Maritime Authority's report lists these four elements. See Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 84.

[74]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 58.

[75]Boyle (2005), pp. 563–584.

[76]Rødseth Ø J, Burmeister H C. "Developments toward the Unmanned Ship", Proceedings of International Symposium Information on Ships–ISIS. 2012, 201, p. 7. Available at: http://www.unmanned-ship.org/munin/wp-content/uploads/2012/08/R%C3%B8dseth-Burmeister-2012-Developments-toward-the-unmanned-ship.pdf.

[77]"Future Proofed? What Maritime Professionals Think about Autonomous Shipping?" Report by NAUTILUS Federation, A Federation of Maritime Professionals.

(1) The reliability of new technology is questionable, since certain technical problems related to sensor and decision-making technology still need to be solved[78]; and (2) piracy issues are still outstanding. Both sides argue their point: the IT systems of an unmanned/autonomous ship could be easier to hack, putting an unmanned vessel at sea at higher risk of piracy[79]; conversely, however, there would not be any crew available for hostage-taking, and no unauthorised operation would be permitted; and (3) if there were to be any computer malfunction, it might take a longer time to reach an unmanned/autonomous ship in a remote ocean.[80]

The second change is related to the lack of a crew and master on board the vessel. As discussed, manning is the tough issue making for acceptance by both international and domestic law of an unmanned/autonomous ship; the new emerging party, including either on-board or shore-based vessel operators (hereafter called the Operator), will play an important role in the ship's sailing. Its roles and obligations need to be further explored; for example, how can the carrier fulfil its obligation to take care of the cargo during the voyage, especially if there is no crew, or less crew, on board?[81] In addition, what is the relationship between the shipowner and the operator? The ordinary ship operator mentioned here might be associated with the operation of the ship, while the shipowner is linked to the ownership of the ship.

These changes and their associated legal uncertainties could pose legal barriers for the introduction of unmanned/autonomous ships, which may further lead to uncertainties for the insurance industry. Any kind of marine navigation is high-risk, and needs insurance as a safeguard.

4 Insurance for Unmanned/Autonomous Merchant Ships

In any insurance case, it is necessary to discuss two basic ideas: (1) who is eligible to be the insured; and (2) who can provide insurance? In the case of unmanned/autonomous ships, it must also be asked whether or not it is necessary to consider any non-marine insurance.

[78]Rødseth Ø J, Burmeister H C. "Developments toward the Unmanned Ship", Proceedings of International Symposium Information on Ships–ISIS. 2012, 201, p. 10. Available at: http://www.unmanned-ship.org/munin/wp-content/uploads/2012/08/R%C3%B8dseth-Burmeister-2012-Developments-toward-the-unmanned-ship.pdf.

[79]With 23 years in the Merchant Marines, including 13 as captain of five vessels, Mr. Kinsey said: "I believe that a human presence on board with active piracy measures in place is an effective deterrent to a pirate boarding." See Mahoney (2016). Available at: https://search.proquest.com/docview/1766119189?accountid=16210.

[80]Mahoney (2016). Available at: https://search.proquest.com/docview/1766119189?accountid=16210.

[81]Mahoney (2016). Available at: https://search.proquest.com/docview/1766119189?accountid=16210.

4.1 Who Is Eligible to Be the Insured?

The answer to this question is not as easy as it may seem to be. It is necessary not only to identify the possible liable parties, but also to understand the apportionment of liabilities among different involved parties, such as the shipowner, the operator and others. Since many international treaties ascertain liability based on the fault of the ship as a whole,[82] it is thus likely that the shipowner and/or operator would both be eligible to be the insured.

The existing maritime liability regime is centred on an essentially tripartite apportionment of responsibility between flag state, shipowner and ship master.[83] The flag state has various obligations regarding the ships' technical conditions, administration of the ships, development of technical standards and codes of conduct for autonomous ships, giving ships their nationality, as well as many other shipping issues. However, it is not usual for the flag state to undertake civil liability, and therefore no mention of a need for the flag state to take out commercial insurance.

As far as the master is concerned, its definition has not been clearly defined by any maritime conventions,[84] but in shipping practice, the master is the physical person responsible for a ship (and any persons or things on board the ship) as well as for the enforcement of the flag State's acts and regulations.[85] Therefore, the use of unmanned/autonomous ships will certainly result in changes in the roles of the master, who is no longer needed to be on board.[86] However, if the master were to play a role in managing or navigating an unmanned/autonomous ship, he would be liable to the shipowner and the cargo owner or other person for damages caused by his wrongful or negligent actions.[87]

The shipowner does not merely mean the owner of the ship. It may also include the registered owner, bareboat charterer, manager and operator of the ship; for instance, under the Maritime Labour Convention 2006 (MLC), a shipowner is defined as "...the owner of the ship or another organisation or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for the operation of the ship from the owner and who, on assuming such responsibility..."[88]

---

[82]Van Hooydonk (2014), p. 421.

[83]Veal and Tsimplis (2017), p. 317.

[84]Veal and Tsimplis (2017), p. 317.

[85]Danish Maritime Authority. "Analysis of Regulatory Barriers to Autonomous Ships: Final Report", December 2017, p. 64. See also Cartner et al. (2009), p. 86.

[86]Van Hooydonk (2014), p. 412.
Veal and Tsimplis (2017), p. 317.

[87]Swedish Maritime Act, SFS 1994:1009 Sjölag, § 6:11.

[88]MLC, 2006, Article II, 1, (j). "shipowner means the owner of the ship or another organization or person, such as the manager, agent or bareboat charterer, who has assumed the responsibility for the operation of the ship from the owner and who, on assuming such responsibility, has agreed to take over the duties and responsibilities imposed on shipowners in accordance with this Convention, regardless of whether any other organization or persons fulfil certain of the duties or responsibilities on behalf of the shipowner."

In addition, the shipowner's liability may be fault-based or strict, which varies according to applicable national law or international conventions.

One of the key parties to the operation of an unmanned/autonomous ship is the shore-based vessel operator. Thus, the question may arise as to the need for it to take out insurance for civil liabilities toward the third parties. The operator may be either a master or an employee of the shipowner.[89] If that were to be the case, it would be difficult for the operator to be liable for civil liability independently, unless he has wrongly done something, either because of his own negligence or wilful misconduct. However, the situation would be different if the operator falls within the defining scope of "shipowner"; the operator would in that case bear the liability as the shipowner. The shipowner should bear the obligations and liabilities, not only for his own negligent acts or omissions, but also for his employees and those performing tasks in the service of the ship.[90]

As for unmanned/autonomous ships, the software designers and manufacturers may also have to undertake some civil liabilities.[91] The IT, software and communications systems will be significantly important for the operation and navigation of unmanned/autonomous ships, so then the question may arise as to how and in what circumstances liability to third parties may attach to software designers and manufacturers, and whether the liability should be fault-based or strict.[92] In the case of driverless cars, there is a proposal in the UK to create the first driverless car legislation, and to review the allocation of civil liability between the driver and manufacturer.[93] It is suggested that the manufacturers still need to accept liability if the accident was caused due to a product design defect, even if drivers were operating the car at the time.[94] For example, a radical presumption has been suggested in a collision incident: it is assumed that if all scientific and safety issues related to the introduction of unmanned/autonomous ships were perfect, there would not be any collision incidents, since unmanned/autonomous ships would be fully autonomous and smart. Therefore, a collision incident can only occur because of software or manufacturing defects; and in this event, product liability insurance will be very necessary.

---

[89]The employees of the shipowner are the people who have contracts with the shipowner and work for the ship no matter on board or off board, including the seafarer, manager, operator, etc.

[90]Rose (2004), p. 349.

[91]"*CMI International Working Group Position Paper on Unmanned Ships and the International Regulatory Framework",* p. 19, available at: http://comitemaritime.org/Maritime-Law-for-Unmanned-Craft/0,27153,115332,00.html.

[92]"*CMI International Working Group Position Paper on Unmanned Ships and the International Regulatory Framework",* p. 19, available at: http://comitemaritime.org/Maritime-Law-for-Unmanned-Craft/0,27153,115332,00.html.

[93]"Government to review law before self-driving cars arrive on UK roads", available at: https://www.theguardian.com/technology/2018/mar/06/self-driving-cars-in-uk-riding-on-legal-review.

[94]"Unmanned and Autonomous Vessels – The Legal Implications from a P&I Perspective", available at: https://www.shipownersclub.com/autonomous-vessels/.

In summary, although it is hard to draw a clear line for apportioning liabilities among different parties, it is however clear that the parties, in particular the shipowner, the software designer and the manufacturer, should consider taking out insurance against any possible civil liabilities.

4.2 Who Insures the Ship?

Another question that may arise in this context is whether or not the current insurance providers could accept unmanned/autonomous ships. As mentioned earlier, only H&M insurance and P&I insurance cover the various kinds of shipowners' third-party civil liability. Nevertheless, one of the big hurdles is that so far there has not been much data available for analysing the risks and premiums in respect of unmanned/autonomous ships.

An H&M policy protects shipowners against physical loss or damage to the vessel's hull, machinery and everything connected therewith. The vessel, including her machinery and equipment, is insured to her full value and, depending on the chosen cover, different forms of the hull policy have been developed, such as the Institute Time Clauses, Hulls, 1/10/83 and 1/11/95, and the International Hull Clauses under English law. Clearly, apart from collision liability, H&M insurance mainly aims to provide fundamental protection for a vessel against various losses or damages.

As for P&I insurance, it is worth noting that the board of directors may be given discretionary rights to waive compliance with some of the Club Rules, which indicates the possibility for Clubs to accept unmanned/autonomous ships. Further, the thirteen principal underwriting associations, which comprise the International Group, have provided liability cover (protection and indemnity) for approximately 90% of the world's ocean-going tonnage[95]; three Clubs, namely, the Gard,[96] the North,[97] and the Shipowners' Club,[98] out of those thirteen P&I associations, show positive attitudes, and in particular, the Shipowners' Club has expressed their

[95]International Group of Protection & Indemnity Clubs, available at: https://www.igpandi.org/about.

[96]Gard has seen three major developments in new product areas during the last six months, including involvement in the development of autonomous shipping. Available at: http://www.gard.no/web/news/article?p_document_id=24640524.

[97]"Shipping: An Autonomous Future?" Available at: http://www.nepia.com/insights/signals-online/ships/autonomous-ships/shipping-an-autonomous-future/.

[98]The Club is in communication with some of the top industry players developing autonomous vessel technology and preparing to provide equipment and related services to vessel owners. Available at: https://www.shipownersclub.com/pi-cover-autonomous-vessels/.

willingness to work together with shipowners to provide cover for unmanned/autonomous ships.[99]

4.3 Certain Non-marine Insurances

As we have already discussed, certain non-marine insurances, such as cybersecurity insurance and product liability insurance will need to be considered as unmanned/autonomous ships are introduced. However, since either no crew or less crew will be on board unmanned/autonomous ships, Kidnap and Ransom insurance (K&R) and Crew liability insurance will lose their relevance, as having no crew on board will of course lead to no one being kidnapped by pirates and no crew liability being incurred. Taking the instance of crew liability, the MLC 2006 requires ships to display certificates confirming that insurance or other financial security is in place for liabilities in respect of outstanding wages and repatriation of seafarers together with incidental costs and expenses[100] and compensation for death or long-term disability.[101] The P&I Club Rules will normally cover compensation for death or long-term disability, but do not, however, include repatriation costs and wages arising from the abandonment provisions set out in Standard 2.5.2 of the MLC, as amended.[102] In the case of unmanned/autonomous merchant ships, the shipowner would certainly be released from this insurance burden on crew liability.

Both the shipowner and software designer & manufacturer need to be cautious with the piracy and cybersecurity issues. In the coming age of unmanned/autonomous shipping, it is hard to expect that pirates and terrorists will disappear totally from the high seas.[103] Unmanned/autonomous navigation may be easier to be hacked; and some simple technical errors may cause serious accidents.[104] The cybersecurity of shipping was hotly debated by the IMO Maritime Safety Committee (MSC) in its 98th session, following which the MSC adopted a resolution on maritime cyber risk management in safety management systems.[105] It is reported that significant weaknesses have been identified in the cybersecurity of critical technology used for navigation at sea, such as GPS (Global Positioning System),

[99]"P & I Cover for Autonomous Vessels", available at: https://www.shipownersclub.com/autonomous-vessels/.

[100]MLC 2006, Regulation 2.5, Standard A2.5.2 and Guideline B2.5.

[101]MLC 2006, Regulation 4.2., Standard A4.2 and Guideline B4.2.

[102]Circular: Maritime Labour Convention 2006 as amended (MLC) Financial Security Requirements, available at: https://www.shipownersclub.com/publications/maritime-labour-convention-2006-as-amended-mlc-financial-security-requirements/.

[103]Van Hooydonk (2014), p. 418.

[104]Mahoney (2016). Available at: https://search.proquest.com/docview/1766119189?accountid=16210.

[105]Maritime Safety Committee (MSC), 98th session, 7–16 June 2017, available at: http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-98th-session.aspx.

AIS (Automatic Identification System), and ECDIS (Electronic Chart Display and Information System), etc.[106] As anything with an IT system or even a computer (including unmanned/autonomous ships) linked to the Internet can be hacked, this means that unmanned/autonomous ships can be cyber-attacked anywhere, not necessarily just during a marine adventure. In fact, there is clearly a lack of provisions in marine insurance as a whole in relation to cyber risk.[107] The insurability of the risks will undoubtedly be of major concern, particularly as to how the risks can be shared between the various marine insurances; otherwise, new insurance products covering cyber risks may need to be developed for unmanned/autonomous ships.

5 Conclusion

Apparently, there is not yet any commonly accepted legal definition and classification of the unmanned/autonomous merchant ship. This in turn affects the consideration of various aspects of the liabilities involved; and consequently, there is also no doubt that the operation and navigation of unmanned/autonomous merchant ships may affect the regime of third-party liability insurance. This article has thus analysed a number of key issues related to third-party liability insurance.

For the question as to who is eligible to be insured, it is argued that the shipowner and the software designer & manufacturer will likely be the parties needing to take out insurance. Regarding the parties who will provide insurance, it is possible that unmanned/autonomous vessels can follow the current practice, and that H&M insurance and P&I insurance will still be the main insurance providers. In addition, certain other non-marine insurances may play an increasingly important role; in this respect, insurance for cybersecurity and product liability will become more and more necessary. Consequently, although no significant legal barrier can be identified, traditional insurance providers should consider these new developments, and pay close and serious attention to them. Furthermore, it seems that certain additional non-marine insurance seems to be necessary to fill in the gaps for insurance cover of the upcoming unmanned/autonomous merchant ships.

References

Boisson P (1994) Classification societies and safety at sea: back to basics to prepare for the future. Mar Policy 18(5):363–377

[106]Marsh LLC, The Risk of Cyber Attack to the Maritime Sector, July 2014, p. 3, available at: https://www.marsh.com/uk/insights/research/the-risk-of-cyber-attack-to-the-maritime-sector.html.

[107]Marsh LLC, Cyber Gap Insurance Cyber Risk: Filling the Coverage Gap, July 2014, p. 3, available at: http://www.oliverwyman.com/content/dam/marsh/Documents/PDF/UK-en/Cyber%20Gap%20Insurance%20Cyber%20Risk%20Filling%20the%20Coverage%20Gap-07-2014.pdf.

Boyle A (2005) Further development of the law of the sea convention: mechanisms for change. Int Comp Law Q 54(3):563–584
Burmeister HC, Bruhn W, Rødseth ØJ et al (2014) Autonomous unmanned merchant vessel and its contribution towards the e-navigation implementation: the MUNIN perspective. Int J e-Navig Marit Econ 1:1–13
Cartner JAC, Fiske R, Leiter T (2009) The international law of the shipmaster. Informa Law from Routledge, p 86
Chatterton EK (1915) Sailing ships and their story: the story of their development from the earliest times to the present day. Sidgwick & Jackson, Ltd., p 273
Forde D (2015) Ancient mariners: the story of ships and sea routes. Maritime Press, p 13
Gurses O (2016) Marine insurance law. Taylor & Francis, p 2
Hazelwood SJ, Semark D (2010) P & I clubs: law and practice. Lloyd's List
Hodges S (2012) Cases and materials on marine insurance law. Routledge-Cavendish, p 308
Hurd HB (1952) The law and practice of marine insurance. Sir Isaac Pitman & Sons, pp 147–148
Kingham JD, McRae DM (1979) Competent international organizations and the law of the sea. Mar Policy 3(2):106–132
Mahoney D (2016) Underwriters get ready for crewless ships: five-year timeframe for unmanned vessels. Bus Insur 50(4)
McLaughlin R (2011) Unmanned naval vehicles at sea: USVs, UUVs, and the adequacy of the law. J Law Inf Sci 21:100
Noussia K (2007) The principle of indemnity in marine insurance contracts: a comparative approach. Springer, p 1
Rose F (2004) Marine insurance: law and practice[M]. LLP Press, p 349
Van Hooydonk E (2014) The law of unmanned merchant shipping – an exploration. J Int Marit Law 20(3):403–423
Veal R, Tsimplis M (2017) The integration of unmanned ships into the *Lex Maritima*. Lloyd's Marit Commer Law Q (2):303–335
Wahlström M, Hakulinen J, Karvonen H et al (2015) Human factors challenges in unmanned ship operations – insights from other domains. Procedia Manuf 3:1038–1045
Walker GK (2012) Definitions for the law of the sea: terms not defined by the 1982 convention. Martinus Nijhoff Publishers, p 138
Wróbel K, Montewka J, Kujala P (2017) Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliab Eng Syst Saf 165:155–169
Zhu L (2007) Compulsory insurance and compensation for bunker oil pollution damage. Springer, p 60
Zhu L (2014) Probing compulsory insurance for maritime liability. J Mar Law Com 45:64

Smooth Sailing or a Risky Expedition: A Critical Exploration into the Innovation of Unmanned Maritime Vehicles and Its Potential Legal and Regulatory Impacts on the Insurance Sector

Shanice N. Trowers

1 Introduction

It is an exciting time in history as technology has been evolving to create innovative products that have and will continue to impact global trade and commerce tremendously.[1] One such sector that has particularly benefited from this evolving technology is that of the transportation sector, where there has been an introduction of automated vehicles.[2] The manner in which people interact with different modes of transportation is about to change significantly within the next 5–10 years, perhaps more than it has changed within the last 100 years.[3] In the motor vehicle industry, many of the known car manufacturers such as Tesla, BMW and Volvo have vowed to introduce fully autonomous cars as early as the year 2020.[4] In the aero industry, unmanned aerial vehicles also known as drones have been used before in the past mostly by various militaries as a tool to aid in war.[5] However, in this modern era, there has been significant development in the use of drones by consumers for both leisure and commercial purposes.[6] It is therefore not surprising that in the maritime

[1]Leimbach et al. (2010), pp. 109–136.

[2]Yeomans (2014).

[3]'Preliminary statement of policy concerning automated vehicles'.

[4]Danielle Muoio 'These 19 companies are racing to put driverless cars on the road by 2020' (Business Insider, 15 July 2016). http://www.businessinsider.com/google-apple-tesla-race-to-develop-driverless-cars-by-2020-2016-7#volvo-is-aiming-to-make-its-cars-deathproof-by-2020-by-rolling-out-semi-autonomous-features-in-its-cars-eventually-working-up-to-fully-driverless-ones-.

[5]Springer (2013).

[6]de Miguel Molina (2018).

S. N. Trowers (✉)
University of Technology, Kingston, Jamaica

P. Marano, K. Noussia (eds.), *InsurTech: A Legal and Regulatory View*,
AIDA Europe Research Series on Insurance Law and Regulation 1,
https://doi.org/10.1007/978-3-030-27386-6_17

sector, several shipping manufacturers are currently exploring, developing and designing unmanned maritime vehicles which will also be referred to in this chapter as autonomous vessels interchangeably. These vessels, sometimes colloquially referred to as "ghost ships" are expected to replace the need for a master and crew, which are traditionally found on conventional manned vessels.[7] These autonomous vessels are expected to revolutionise the shipping industry in the very near future. As autonomous vessels are a relatively new phenomenon, there is not a large volume of scholarly papers on the topic. Corollary to this, there is also very little that has been written generally about the interrelation of autonomous vessels on international maritime law and marine insurance law. The author therefore deemed it necessary to contribute to the international maritime research database on autonomous vessels by writing this analytical chapter that will critically explore autonomous vessels and their potential impacts on marine insurance laws and international maritime law generally. At the end of the critical discussion and analysis, the author arrives at a conclusion on whether autonomous vessels when introduced will sail smoothly or whether this innovation will simply be a risky expedition. The first half of this analytical chapter will give a general background on the state of autonomous vessels generally, as well as critically explore its potential impacts on international maritime law. The second half of this analytical chapter will critically discuss important marine insurance law considerations that should be taken into account in relation to autonomous vessels. Additionally, although there are several types of proposed models for autonomous vessels, the focus of this chapter will be on autonomous vessels specifically designed to transport cargo goods.

2 Background

In this section, the author will provide general background information on unmanned maritime vessels. The author will provide a concise definition, critically discuss why there is a need for autonomous vessels, examine what is the current of the technological development of autonomous vessels and discuss whether autonomous vessels can legally be considered as ships.

2.1 Definition of Unmanned Maritime Vehicles

Unmanned maritime vehicles also known as unmanned vessels, autonomous vessels or *'ghost ships'* are simply vessels that are not operated by an on board master and

[7]Christian Matthews 'Unmanned 'ghost' ships are coming' (Independent, 6 September 2017) https://www.independent.co.uk/news/science/ghost-ships-coming-yara-birkeland-norway-maritime-law-changing-fewer-accidents-cheaper-shipping-a7930481.html.

crew.[8] This includes all unmanned vessels from those remotely operated by shore-based operators to those that are fully autonomous.[9] Where the author uses the words 'autonomous vessels' throughout this chapter, it is meant to include both remotely operated unmanned vessels as well as those that are fully autonomous.

2.2 The Need for Autonomous Vessels

Within the EU as well as internationally, maritime transport remains one of the main modes of transportation for international commerce and trade.[10] Notwithstanding this, the maritime transport industry constantly faces significant challenges, which include shortage of seafarers, who at times display a high level of absenteeism from work because of family responsibilities.[11] Additionally, there are environmental concerns, which arise from traditionally manned oil and bunkered vessels.[12] There is also the concern that some traditional manned vessels are incapable of carrying large volumes of cargo because of the fact that a large portion of the vessel is used for holds and rooms for the officers, master and crew.[13] Autonomous vessels it is hoped will provide the solution to these and other varying problems facing the maritime industry, as autonomous vessels are expected to be much more efficient, to use cleaner and more environmentally friendly energy and it will most certainly solve the problem of seafarers absenteeism which at times impact negatively on commerce and trade.[14]

[8]Simonsen Vogtwiig, 'Maritime Law in the wake of the unmanned vessel' https://svw.no/contentassets/f424f309bd304e99b39f11355e98571f/svw_maritime-law-in-the-wake-of-the-unmanned-vessel.pdf.

[9]Simonsen Vogtwiig ,'Maritime Law in the wake of the unmanned vessel' https://svw.no/contentassets/f424f309bd304e99b39f11355e98571f/svw_maritime-law-in-the-wake-of-the-unmanned-vessel.pdf.

[10]European Commission Statistical Pocketbook 2017-' EU Transport in figures' https://ec.europa.eu/transport/sites/transport/files/pocketbook2017.pdf.

[11]Alderton et al. (2004).

[12]Captain George Quick 'Would Autonomous Ships be good for Society?' (Maritime Executive, 31 October, 2016) https://www.maritime-executive.com/editorials/would-autonomous-ships-be-good-for-society#gs.UeDHR2E.

[13]Captain George Quick 'Would Autonomous Ships be good for Society?' (Maritime Executive, 31 October, 2016) https://www.maritime-executive.com/editorials/would-autonomous-ships-be-good-for-society#gs.UeDHR2E.

[14]MUNIN 'MUNIN Project web page' http://www.unmanned-ship.org/munin/.

2.3 What Is the Current State of Autonomous Vessels?

Yara Birkeland

At present, there are a number of ongoing research projects as it relates to unmanned and autonomous vessels. One such project is that of the Yara Birkeland, which will be the world's first zero-emission autonomous container vessel.[15] It is currently being developed by Marin Teknikk and Kongsberg Maritime[16] but it is owned by Yara International and was partly funded by the Norwegian Government.[17] It is expected that the vessel will be fully battery powered and will feature both autonomous and unmanned operations.[18] The vessel features an extensive safety plan, which includes three safety centers, which will handle different aspects of the vessels operation.[19] The vessel will be launched in 2019 and will feature an initial voyage with a small crew and thereafter, it is expected that by the year 2020, the Yara Birkeland should be able to sail autonomously.[20]

The MUNIN Project

Another research project that is currently underway is the Maritime Unmanned Navigation through Intelligence in Networks project, commonly referred to as the 'MUNIN' project.[21] The MUNIN project is an European Union collaborative research project, whose aim is to develop an autonomous ship.[22] The EU has identified the many benefits that can be derived from having autonomous vessels in operation and as such, this project has been co-funded by the European Commission under its Seventh Framework Programme.[23] MUNIN intends to develop a

[15]Ballin (2017).

[16]Konsgsberg 'Autonomous Ships' https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument.

[17]Konsgsberg 'Autonomous Ships' https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument.

[18]Konsgsberg 'Autonomous Ships' https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument.

[19]Konsgsberg 'Autonomous Ships' https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument.

[20]Konsgsberg 'Autonomous Ships' https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument.

[21]Ballin (2017).

[22]Thomas Porathe, 'Remote Monitoring and Control of Unmanned Vessels-The MUNIN Shore Control Centre' (Chalmers Univ of Technology, Gothenburg/Sweden) http://publications.lib.chalmers.se/records/fulltext/198197/local_198197.pdf.

[23]Thomas Porathe, 'Remote Monitoring and Control of Unmanned Vessels-The MUNIN Shore Control Centre' (Chalmers Univ of Technology, Gothenburg/Sweden) http://publications.lib.chalmers.se/records/fulltext/198197/local_198197.pdf.

vessel that is completely unmanned for majority of its voyage. To do this, MUNIN has critically examined the technical, economical and legal feasibility of unmanned vessels.[24] As it relates to technology, MUNIN has illustrated that they would need amongst other things the following items[25]:

1. A deep-sea navigation system, which would ensure that the vessel follows the designated voyage route. MUNIN has posited that a good deep-sea navigation system will be one that is flexible enough to accommodate or to allow for authorised deviations for things such as sea traffic and bad weather conditions;
2. Engine monitoring and control system, which would carefully monitor and control technical systems including the engine to ensure that it is functioning properly and should assist with preventing breakdowns throughout the voyage;
3. Remote maneuvering support- this is a device that will assist with maneuvering the vessel during certain constrained waters and in certain ports;
4. Advanced sensor-module- this is a very important device in an automated vessel as it replaces the officer at watch. This system assists with object detection, classification and environmental perception;
5. Energy efficiency system- this aims to optimise the fuel consumption and energy management by examining the vessels' power demands and uses;
6. Maintenance interaction system and;
7. Shore control system-The MUNIN project relies on the shore control center to handle complex situations that the vessels autonomous systems cannot handle.

The Rolls Royce "AAWA" Project

Another ongoing research project into the development of an autonomous vessel is that of the Rolls Royce Advanced Autonomous Waterborne Applications (AAWA) project.[26] This is a project led by Rolls Royce but financed by a Finnish agency named "TEKES".[27] The aim of the project is quite similar to that of the MUNIN project. It aims to produce an autonomous vessel by 2020 through the concept of "dynamic autonomy".[28] The idea behind dynamic autonomy is that different aspects

[24]MUNIN-'MUNIN's Objectives & Impact' http://www.unmanned-ship.org/munin/about/munins-objectives/.

[25]MUNIN-'MUNIN's Results' http://www.unmanned-ship.org/munin/about/munin-results-2.

[26]Rolls Royce-'AAWA project introduces the project's first commercial ship operators' (12 April 2016) https://www.rolls-royce.com/media/our-stories/press-releases/2016/pr-12-04-2016-aawa-project-introduces-projects-first-commercial-operators.aspx.

[27]Rolls Royce- 'AAWA project introduces the project's first commercial ship operators' (12 April 2016) https://www.rolls-royce.com/media/our-stories/press-releases/2016/pr-12-04-2016-aawa-project-introduces-projects-first-commercial-operators.aspx.

[28]Markus Laurinen, 'Advanced Autonomous Waterborne Applications Initiative' http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/12%20-%20AAWA%20Coordinator.pdf.

of the maritime operation will have different degrees or levels of autonomy.[29] The technology involves, an autonomous navigation system that includes collision avoidance, route planning, and situational awareness.[30]

2.4 Are Unmanned Vessels Legally Considered As Ships?

To properly analyse the legal status of autonomous vessels and their potential impact and interrelation with international maritime and insurance law, it is pertinent to examine whether an autonomous vessel can be considered as a ship within the general context of maritime law. Ships are often times the main subject of maritime laws and conventions and as such, it is important for owners of autonomous vessels to know if their vessels are considered ships, so they are aware of the relevant laws and conventions that they will be subject to if they are legally recognised as ships. Notwithstanding the fact that ships are often times the focal point of maritime laws, there is surprisingly no uniformed or single definition of the word 'ship.'[31] It varies from convention to convention and some national laws have varying definitions for the word 'ship'.[32] As such, as it currently stands, an owner of an autonomous vessel must examine each international convention specifically to determine whether their vessel would fall within the definition of a ship as defined by the specific international convention. In essence, the definition of a ship really depends on the scope of the relevant international convention and/or national laws.

The author will now examine selected international conventions and national laws to determine if an autonomous vessel could be considered a 'ship' within the meaning of these selected conventions and national laws.

Definition of 'Ship' in International Conventions

The United Nations Convention on the law of the seas (UNCLOS) is often times referred to as the 'constitution for the oceans,'[33] as it contains amongst other things, the navigational rights and relevant duties of ships. However, this very constitution

[29]Markus Laurinen, 'Advanced Autonomous Waterborne Applications Initiative' http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/12%20-%20AAWA%20Coordinator.pdf.

[30]Markus Laurinen, 'Advanced Autonomous Waterborne Applications Initiative' http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/12%20-%20AAWA%20Coordinator.pdf.

[31]Van Hooydonk (2014).

[32]Van Hooydonk (2014).

[33]United Nations- 'United Nations Convention on the Law of the Sea' https://sustainabledevelopment.un.org/topics/oceans/unclos.

itself does not have any definition as to what exactly constitutes a ship.[34] The lack of a definition has led this author to hold the view that it is possible that autonomous vessels be considered ships under the UNCLOS. This would mean that autonomous vessels would enjoy the same rights and benefits and must comply with the stipulated regulations under the UNCLOS.

There are other conventions however that define the word ship in such a manner that it could also apply to autonomous vessels. Article 2, Clause 4 of the International Convention for the Prevention of Pollution from Ships 1973 as modified by the Protocol of 1978 (MARPOL 73/78), defines a ship as

> a vessel of any type whatsoever, operating in the marine environment and includes hydrofoil boat, air-cushion vehicles, submersibles, floating craft and fixed or floating platforms.[35]

Similarly, Section 3(a) of the International Regulations for Preventing Collisions at Sea 1972 (COLREGs) defines ship as

> every description of water craft, including non-displacement craft, WIG craft and seaplanes, used or capable of being used as a means of transportation on water.[36]

Article 1 (d) of the International Convention for the Unification of Certain Rules of Law relating to Bills of Lading (also known as The Hague Rules) defines ship as

> any vessel used for the carriage of goods by sea.[37]

Likewise, the Athens Convention relating to the Carriage of Passengers and their Luggage by Sea defines ship to mean

> only a sea going vessel, excluding an air-cushion vehicle.

While it is not practical to outline and examine the definition of ship in every international maritime convention, it is evident from the above that autonomous vessels are able to be captured by several international maritime conventions. This is particularly so because these conventions define ships in general to mean a waterborne craft and does not specify the need for a crew or a master for a vessel to be considered a ship. If however, there are any international conventions that define ship to mean a vessel that is manned or has a crew or a master, then arguably, it is most likely that the convention would not apply to an autonomous vessel.

[34]See the United Nations Convention on the Law of the Sea (Montego Bay 10 December 1982).

[35]International Convention for the Prevention of Pollution from Ships, 1973 as modified by the Protocol of 1978.

[36]International Regulations for Preventing Collisions at Sea 1972.

[37]International Convention for the Unification of Certain Rules of Law relating to Bills of Lading.

Definition of Ship in National Laws

As it relates to the definition of ship in national legislations, the author has chosen to examine the definition of ship found in selected national legislations in the United Kingdom, United States of America, Netherlands and France.

In the United Kingdom, a vessel is defined by the Merchant Shipping Act of 1995 as

> any ship or boat, or any other description of vessel used in navigation.

Similarly, in the United States of America, Section 3 of the Rules of Construction U.S.C defines vessel as every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on water. In the EU, the Dutch Civil Code defines ships as

> all things, that are no aircraft and that are due to their construction destined to float and are floating or have been floating.

In France, ship is defined as

> a floating, moveable craft designed for ocean navigation.[38]

From the above comparative definitions, it is clear as well that autonomous vessels are able to fall within the ambits of legislations at the national level, as it is evident that similar to international conventions, national legislations tend to define ship or vessel in a general manner, without any reference to the words master and/or crew. Thus, it is only if a national legislation defines the word ship or vessel to include one that has to be manned by a master and one that has to possess a crew that an autonomous vessel would not fall within the ambits of legislation generally.

3 Potential Impacts of Autonomous Vessels

3.1 The Potential Benefits of Autonomous Vessels

Autonomous vessels are considered one of the most revolutionising technologies to be developed in this era. It is expected that autonomous vessels will significantly change how the global world conducts international trade and commerce. As such, the author finds it pertinent to critically examine what are some of the general benefits that can potentially be achieved from the use of autonomous vessels.

One of the most discussed benefits to be derived from the use of autonomous vessels is the fact that there will be an absence of an onboard master and crew and as such, ship-owners are able to save on labour costs.[39] The absence of an on board master and crew will not only save on labour costs but it is expected that this absence

[38]International Encyclopedia of Comparative Law (2002) Vol. 36.

[39]Deketelaere (2017).

will contribute significantly to a decrease in maritime accidents.[40] This is because of the fact that it has been reported that human error is responsible for up to 75% of marine casualties.[41] As such, it is expected that with the absence of an onboard master and crew, there should be less accidents involving vessels at sea if autonomous vessels are widely used in the near future. Autonomous vessels will therefore contribute significantly to sea safety.[42] From an insurance point of view, this can be particularly beneficial to insurance companies as with a reduction in accidents, there will be less maritime claims for insurance companies to attend to and less claims for them to make a monetary payment for.[43] This means that insurance companies are able to save on both human resources and financial resources.

Another benefit to be derived from the use of autonomous vessels is that there will be more hold space for cargo, as there will be an absence of accommodation rooms and other facilities usually used for the master and crew onboard manned vessels.[44] This means that the amount of cargo a vessel can hold will be increased. This will benefit both ship-owners and charterers, as charterers will be able to transport a larger volume of cargo in one shipment, while ship-owners can benefit from increased freight as a result of an increase in the volume of cargo shipped. From an insurance law point of view, this will also be beneficial to marine insurance companies as there may be an increase in the coverage for cargo policies from the same. This therefore means that insurance companies can earn more revenue from an increase in the coverage for cargo policies.

Additionally, it is predicted that autonomous vessels will operate more efficiently than traditional manned vessels.[45] This is so because traditional vessels typically feature a steamer system, which uses one or more steam engines.[46] These traditional vessels have over the years, not been very fuel efficient and as such many shipping personnel have had to resort to what is considered as slow steaming.[47] Slow steaming is the process whereby the speed of the ship is deliberately slowed down

[40]ibid.

[41]Safety4Sea 'Allianz: Human error behind 75 percent of marine casualties' https://safety4sea.com/allianz-human-error-behind-75-percent-of-marine-casualties/.

[42]ibid.

[43]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[44]Deketelaere (2017).

[45]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[46]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018 https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[47]Lee Hong Liang, 'The Economics of slow steaming' (7 October 2014) http://www.seatrade-maritime.com/news/americas/the-economics-of-slow-steaming.html.

as a way to lower costs by reducing fuel consumption.[48] Slow steaming however means that the transportation of cargo takes much longer to reach its destination.[49] To combat these problems, it has been reported that many of the models of autonomous vessels that are currently being developed are using batteries for energy.[50]

Another significant benefit to be derived from the use of autonomous vessels is that several models that are currently being developed, feature a zero-emissions design. It has been reported in Norway that autonomous vessels will be electric vessels, and that once they are in operation, they are expected to replace 100 diesel truck journeys.[51] It is hoped that this will reduce noise and dust emissions, improve the safety of local roads and reduce nitrogen oxide (NOx) and carbon dioxide (CO2) emissions.[52] Excess carbon dioxide has a harmful effect on the environment as it increases global warming, causes smog and acid rain among other things.[53]

Additionally, many marine fuels contain a high level of sulfur, which emits sulfur dioxide by the combustion of marine fuel in the vessels engine.[54] It has also been reported that the shipping industry's sulfur dioxide limit was 3500 times more than diesel cars on European roads. This is particularly alarming, as sulfur dioxide inhalation has been linked to lung cancer and heart disease. With the advent of zero-emissions electric autonomous vessels, the environment will certainly benefit from a decrease in sulfur dioxide, nitrogen oxide, carbon dioxide and other harmful fumes in the atmosphere. Further, insurance companies will also benefit from less claims arising from environmental damage and health concerns caused by inhalation of harmful fumes coming from vessels.

Another benefit that the marine insurance industry will have specifically is the fact that they must develop new and innovative products to satisfy the autonomous vessels market. There must be a special type of manufacturer's liability policy for manufacturers who design and manufacture these autonomous vessels developed, as it is very likely that these manufacturers would be the subjects of claims arising from autonomous vessels in the future. Additionally, there must also be a special type of product liability policy for companies that purchase from manufacturers and resell to

[48]Lee Hong Liang, 'The Economics of slow steaming' (7 October 2014) http://www.seatrade-maritime.com/news/americas/the-economics-of-slow-steaming.html.

[49]Lee Hong Liang, 'The Economics of slow steaming' (7 October 2014) http://www.seatrade-maritime.com/news/americas/the-economics-of-slow-steaming.html.

[50]See the Yara Birkeland currently being developed in Norway.

[51]Asle Skredderberget, 'The first ever zero emission, autonomous ship' (YARA, 14 March 2018) https://www.yara.com/knowledge-grows/game-changer-for-the-environment/.

[52]Harry Croome, 'Autonomous & Crewless Ships-The Risks & Reality' (24 October 2017) https://www.hemisphere-freight.com/autonomous-crewless-ships-are-there-risks-to-the-ocean-freight-industry/.

[53]Bartleby 'Air Pollution, Smog, Acid Rain, the Greenhouse Effect, and Ozone Depletion' https://www.bartleby.com/essay/Air-Pollution-Smog-Acid-Rain-the-Greenhouse-F3CJKHPYTC.

[54]'What is Sulphur Oxides or Sox air pollution from Ships?' (Marine Insight, 21 July 2017) https://www.marineinsight.com/maritime-law/what-is-sulphur-oxides-or-sox-air-pollution-from-ships/.

a third party ship-owner. These companies will require product liability protection because they may also be the subject of claims in the future for any accidents or incidents, which results from a malfunctioning autonomous vessel.

Additionally, the global community will benefit from either reformation of existing legislations and conventions, which are incapable of accommodating autonomous vessels or the development of novel legislations and conventions that relate to autonomous vessels specifically.

Lastly, another important benefit of autonomous vessels is the fact that they will no longer be heavily reliant on humans as a resource.[55] Autonomous vessels as stated above will either be remotely operated by shore-based operators or they will be fully autonomous which means that they can operate without the need for any human interaction on board the vessel. This means that the issue of seafarers' absenteeism, which tends to affect trade and the smooth operation of vessels, will no longer be an issue.[56] Similarly, it is arguable that from a human rights perspective, seafarers will have a better quality of life, as they no longer will be away from their families for any extended period of time, which tends to in some cases, tremendously affect family life.[57] Further, insurance companies will also no longer see claims for injury on the job or vicarious liability claims from seafarers who are injured while on board a vessel, or who by virtue of their actions, caused their employers to suffer loss.

3.2 Disadvantages of Autonomous Vessels

Although there are undoubtedly great benefits to be achieved from the use of autonomous vessels, there are certain aspects of this novel development that the author believes may be of concern.

Although named as a benefit, the lack of human resources will also prove to be detrimental.[58] This is because of the fact that autonomous vessels will be heavily reliant on computer technology. Thus, there has been reports that seafarers fear that their jobs will become obsolete.[59] As such, they worry that they will no longer be able to provide for their families and will thus be forced to find another career path.

Another area of concern also relates to the heavy dependency of autonomous vessels on computer technology. It is expected that these computer technology would be just as vulnerable to the usual software attacks from software viruses

[55]Mathieu (2016).

[56]Mathieu (2016).

[57]Alderton et al. (2004).

[58]Mathieu (2016).

[59]John Snyder 'Autonomous vessels: Not so remote' https://www.marinelog.com/index.php?option=com_k2&view=item&id=26653:autonomous-vessels-not-so-remote&Itemid=257.

and other malware which computers are generally exposed to.[60] This poses tremendous danger to all players involved including ship-owners, charterers and insurance companies. It therefore means that manufacturers of autonomous vessels must ensure that the technology used in autonomous vessels is of a high standard and of such fortitude, that it is able to withstand any virus and other malware that may be developed by mischievous entities. From an insurance law point of view, these are novel risks that insurance companies must now consider when drafting policies for autonomous vessels.

Corollary to the above is the fact that these new risks will most likely result in higher premiums having to be paid. Although it was reported by the International Union of Marine Insurance in September 2017 that global marine underwriting premiums continue to fall,[61] it is thought that once autonomous vessels are introduced, there will be a higher premium to be paid by owners of autonomous vessels because of the novelty and uncertainties associated with these vessels. However, once autonomous vessels are widely used and the risks associated with them become well known by marine insurance companies, the high premiums that owners of autonomous vessel may face would become less overtime.

Another concern as it relates to autonomous vessels is that of piracy. With autonomous vessels in use, piracy may become more prevalent because pirates will know that these vessels are traversing the sea crewless and as such, they may hold the belief that these vessels can be easily accessed and raided. As such, it is imperative that the security features installed on an autonomous vessel is at the highest level. The actual infrastructure of an autonomous vessel may need to be bulletproof and made of very strong material. Additionally, outside of simply physically raiding a ship, there is also the concern of cyber piracy, which may occur where an autonomous vessel is remotely attacked by a cyber pirate and steered to another destination. To prevent this from happening, again the software used in autonomous vessels must be able to resist such cyber pirate attacks.

Lastly, as autonomous vessels are new and emerging, another drawback of these vessels is that there must be a significant overhaul of the marine insurance industry for it to be able to properly accommodate these vessels. This therefore means that there must not only new policies but also new standard forms, documents and clauses developed, if the existing ones are incapable of properly accommodating autonomous vessels. To develop such policies and documents there may potentially be a strain on the human and financial resources of the marine insurance sector. To reiterate, there must also be new legislations and conventions developed in law generally that relate specifically to autonomous vessels, which may also prove to be an expensive venture for legislators to undertake.

[60]John Snyder 'Autonomous vessels: Not so remote' https://www.marinelog.com/index.php?option=com_k2&view=item&id=26653:autonomous-vessels-not-so-remote&Itemid=257.

[61]IUMI'Global marine underwriting premiums continue to fall, reports IUMI (18 September 2017) https://iumi.com/news/press-releases/global-marine-underwriting-premiums-continue-to-fall-reports-iumi.

4 The Interrelation of Autonomous Vessels and International Maritime Law

It has been established above that there is no uniform definition of the word ship or vessel in international law and it is concluded that there is a strong possibility that autonomous vessels will be captured by most international maritime conventions. As such, it is prudent to discuss the potential impact that the introduction of autonomous vessels may have on international maritime law practices before discussing more specifically their potential impact on marine insurance law.

4.1 Will Autonomous Vessels Be Able to Satisfy the Requirement of a Genuine Link to the Flag State?

Article 91 of the UNCLOS[62] states that

> 1. Every State shall fix the conditions for the grant of its nationality to ships, for the registration of ships in its territory, and for the right to fly its flag. Ships have the nationality of the State whose flag they are entitled to fly. There must exist a genuine link between the State and the ship.
>
> 2. Every State shall issue to ships to which it has granted the right to fly its flag documents to that effect.[63]

As evidenced from Article 91 (1) above, for a ship to fly a state's flag, there must be a genuine link between the state and the ship. It has been argued that genuine link means that there must be a substantial entity that can be made responsible for the actions of the ship located within the flag state.[64] As was established earlier in this chapter, autonomous vessels will still be considered as ships under the UNCLOS.[65] As such, it is arguable that for an autonomous vessel to sail within the high seas, it must be flying the flag of a state and to do so, it must have a genuine link with the flag state. This should not be difficult for autonomous vessels to satisfy. This is so because as it relates to remote-controlled autonomous vessels, there will be a center for shore-based operators to operate from within the particular flag state which arguably could be considered as the substantial entity that would be responsible for that vessel. Additionally, it is foreseeable that for completely autonomous vessels, there will nonetheless be a hub situated in the particular flag state that oversees the entire operation of the autonomous vessel while it is undergoing a voyage, which could also arguably be considered as the substantial entity that is

[62]See the United Nations Convention on the Law of the Sea (Montego Bay 10 December 1982).

[63]See the United Nations Convention on the Law of the Sea (Montego Bay 10 December 1982).

[64]Geneva Convention of the High Seas 'The Genuine Link' http://www.armatorlerbirligi.org.tr/Sites/1/upload/files/THE_GENUINE_LINK.pdf.

[65]See para 2.4 above.

responsible for the vessel within the flag state. Alternatively, the ship-owner could have an administrative office based in the respective flag state, which could arguably be considered as the substantial entity within the flag state that is responsible for the vessel. Therefore, there is no difficulty for autonomous vessels to satisfy this article of the UNCLOS.

As it relates to Article 91 (2) of the UNCLOS, which requires that every state must issue to ships documents to that effect if the ship has the right to fly its flag, with the advent of autonomous vessels, it should not be absolutely necessary for physical copies of these documents to be on board an autonomous vessel. Rather, in the case of autonomous vessels, it should be acceptable that these documents be digitally issued and perhaps even stored on the hard drive of an autonomous vessel.

4.2 Duties of the Flag State-Would They Still Be Applicable to Autonomous Vessels?

Article 94 of the UNCLOS outlines the duties of the flag state in relation to vessels flying its flag. Article 94 (1) of the UNCLOS states that:

> Every State shall effectively exercise its jurisdiction and control in administrative, technical and social matters over ships flying its flag.[66]

Article 94 (2) (a) of the UNCLOS states that

> . . .every state shall maintain a register of ships containing the names and particulars of ships flying its flag, except those which are excluded from generally accepted international regulations on account of their small size.[67]

It would appear that this duty of a flag state as it relates to autonomous vessels could be easily satisfied, as it would appear that all that would really be required is to have the autonomous vessel registered on the ship register of the particular flag state. The UN Convention on Condition for Registration of Ships 1986, although not in force, has provided guidance to many states as it relates to the information that should be contained in any ship register.[68] The register should contain amongst other things, the name of the vessel, place of port registration, name of builders and the particulars of any mortgage.[69] However, if this convention comes into force in this modern day, it would be necessary for the convention to stipulate that a ship register should specify the classification of the vessel. That is, it would be necessary to include in any ship register whether it is a manned, remote-operated or fully autonomous vessel. Therefore, the states should now include in their registers, a category which specify or classify the vessels for completeness.

---

[66]See the United Nations Convention on the Law of the Sea (Montego Bay 10 December 1982).

[67]See the United Nations Convention on the Law of the Sea (Montego Bay 10 December 1982).

[68]The United Nations' Convention on Condition for Registration of Ships 1986.

[69]Article 11 of the United Nations' Convention on Condition for Registration of Ships 1986.

Article 94 (2) (b) of the UNCLOS states further that among other things, every state shall assume jurisdiction under its internal law over each ship flying its flag, its master, officers and crew in respect of administrative, technical and social matters concerning the ship. It is questionable if Article 94 (2) (b) will be directly applicable to autonomous vessels, as they do not have a master, officer or crew on board. It has been argued however that shore-based operators for remotely operated autonomous vessels may be viewed similarly in the context of a master or crew[70] and as such, it may be possible for Article 94 (2) (b) to be relevant to remotely operated vessels which are operated by shore-based operators. Article 94 (3) illustrates that every state shall take such measures for ships flying its flags to ensure the safety at sea.[71] Upon careful examination of this subsection and subsection 94 (4), it is evident that a pivotal aspect of ensuring safety at sea is the requirement that the vessel be manned by a master and the crew be properly trained and possess the requisite certification.[72] This convention like many others was drafted during a time when autonomous vessels were not even remotely in the contemplation of the drafters of the convention. However, this will pose a challenge for states that allow autonomous vessels to fly their flags while sailing within the high seas, as it may prove difficult for them to satisfy that they have done all that is necessary to ensure that these vessels are safe to traverse the high seas within the meaning of Section 94 (4) of the UNCLOS.

In this respect, unless a different convention is drafted specifically for autonomous vessels or the UNCLOS 1994 is extensively modified to properly accommodate autonomous vessels, states may be reluctant in giving autonomous vessels the authorisation to fly their flags while sailing in the high seas, as they are unable to guarantee the vessels' safety as defined by the convention and are fearful of liability as a result. In this respect, it is therefore accurate to state that some of the duties of a flag state under the UNCLOS would still be relevant to autonomous vessels but certainly not all duties.

Other duties of a flag state as defined by the UNCLOS that may be difficult to satisfy with respect to autonomous vessels include Article 98 of the UNCLOS, which states that:

> Every State shall require the master of a ship flying its flag, in so far as he can do so without serious danger to the ship, the crew or the passengers:
>
> (a) to render assistance to any person found at sea in danger of being lost;
> (b) to proceed with all possible speed to the rescue of persons in distress, if informed of their need of assistance, in so far as such action may reasonably be expected of him;
> (c) after a collision, to render assistance to the other ship, its crew and its passengers and, where possible, to inform the other ship of the name of his own ship, its port of registry and the nearest port at which it will call.[73]

[70] Van Hooydonk (2014).

[71] See Article 94 (3) of the United Nations Convention on the Law of the Seas 1994.

[72] See Article 94 (4) of the United Nations Convention on the Law of the Seas 1994.

[73] See Article 98 of the United Nations Convention on the Law of the Sea 1994.

As the vessels are autonomous, it would be rather difficult for such vessels to render assistance to persons in danger or to rescue such persons. Unless the vessels are built with such advanced technology to detect genuine distress that they may be unable to comply with this article and as such, flag states arguably would be in breach of this duty as specified by the UNCLOS in relation to autonomous vessels.

4.3 Training of Seafarers

Another area of international maritime law that will be affected by the introduction of autonomous vessels is that which relates to the training of seafarers. The introduction of autonomous vessels will certainly impact the manner in which masters, officers, watch personnel and other shipping employees are trained internationally.[74] At present, the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) 1995, outlines the minimum qualification standards that seafarers including masters, officers and watch personnel should possess before they can work on a merchant ship.[75] This is a widely accepted convention in the maritime arena and at present, there are one hundred and sixty one (161) countries that are parties to this convention.[76] This clearly indicates how critical, far-reaching and impactful this convention is. Arguably, for autonomous vessels, international conventions such as the STCW 1995, which address training and manning levels, would not be relevant and would arguably not apply to autonomous vessels. This is because with autonomous vessels, the crew, masters, officers and watch personnel are all replaced by technology. As such, there would arguably be no need to train persons on manning levels and other vessel management techniques as it relates to autonomous vessels. However, it is important to note that as it relates to remote-controlled autonomous vessels, it is arguable that a similar convention to the STWC 1995 could be drafted, which would allow for a uniformed training regime of shore-based operators. Additionally, as it relates to fully autonomous vessels, a similar convention to the STWC 1995 could be drafted to train the in-house staff who would be based at the respective hubs, on how to properly monitor autonomous voyages. This would particularly be vital if autonomous vessels are widely used in the future.

[74]Van Hooydonk (2014).

[75]See the International Convention on Standards of Training Certification and Watchkeeping for Seafarers (STCW) 1995.

[76]Erik Kravets 'Look beyond the flag' (Maritime Executive, 23 March 2018) https://www.maritime-executive.com/magazine/look-beyond-the-flag.

5 Insurance Law Considerations for Autonomous Vessels

5.1 Overview

It is imperative to discuss with more specificity, the insurance law considerations that relate to autonomous vessels. The marine insurance sector's response to the innovation of autonomous vessels will be largely dependent on the risks associated with autonomous vessels.[77] If autonomous vessels are able to successfully achieve their goals of being reliable, more environmentally friendly, more cost-effective and more efficient, ship-owners of autonomous vessels should have little difficulty in finding insurance companies who are willing to insure their vessels and the associated risks.[78] It is therefore necessary to firstly critically examine what are the important insurance contract law considerations that owners of autonomous vessels should contemplate before entering into an insurance policy for their autonomous vessel.

The Definition or Interpretation Section

It is common to find in some insurance contracts, a definition or interpretation section which defines key terms that are relevant to the contract. It would therefore be pertinent to ensure that this section is properly drafted and that the items defined are properly described, and that they accurately relate to the contents of the contract. Therefore, it would be of utter importance that in an insurance policy for an autonomous vessels, if the words ship or vessel are defined, that no reference is made to the need for it to be manned or crewed. If the policy relates to a remote controlled autonomous vessel, perhaps the word ship or vessel could be defined to include off-shore operators but it would be best to have a generic and wide definition of ship without any limitations as to any need for a crew or master in a policy relating to autonomous vessels.

The Risks

In any insurance contract, it is very important to outline the risks that are covered by the contract.[79] It is quite possible that the risks that would typically be covered by

[77]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[78]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[79]Great Britain Law Commission (2012).

ordinary marine insurance contracts for traditional manned vessels may vary from the risks that would be covered by an insurance contract for an autonomous vessel. It is expected that some current risks may be reduced or removed entirely because of the lack of human presence on board the vessel while other risks will increase.[80] There will also be novel risks that will arise. Risks that may possibly increase relate to issues such as piracy including cyber piracy, cyber attacks, software viruses and malfunctioning of on board technical hardware. Cyber risks are defined as any risk of accidents, incidents, financial loss, business disruption or damage to the reputation of an organisation through failure of its electronic systems or by the persons using those systems.[81] Currently, the International Group of Protection and Indemnity clubs currently do not exclude losses or liabilities that arise from cyber risks unless the cyber risk constituted an excluded war risk.[82] The author suspects that cyber risks for autonomous vessels will be addressed in the same manner, and opines that owners of autonomous vessels should ensure that this is a risk that they have adequate coverage against.

Additionally, another increased risk that should be in the contemplation of shipowners of autonomous vessels is that relating to privacy and the storage of sensitive data. This will be a real concern as the vessels would be storing sensitive information on their hard drives and black boxes.[83] If private and sensitive information is leaked, there could be serious consequences and as such, it would be pertinent to cover this kind of risk under any insurance coverage relating to autonomous vessels.

The Premium

It is already a known fact that marine insurance costs multimillions of dollars for traditional manned vessels.[84] With the advent of autonomous vessels, it is expected that at least initially, the cost to insure these vessels will be much higher than the cost to insure a traditional manned vessel.[85] This is because it is novel and risky and as such, insurance companies will most likely charge a higher premium than usual for

[80]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[81]de Vleeschhouwer (2017).

[82]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[83]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[84]Deketelaere (2017).

[85]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

autonomous vessels. Over time however, if owners of autonomous vessels are able to demonstrate through use of their black box and other technology that they are able to operate at a much safer level than manned vessels, the cost of the premium to insure the vessels may be reduced.[86]

Liability

Liability is a very important aspect of any insurance contract and as such, it is extremely important to address how liability will possibly be addressed as it relates to autonomous vessels. The author will critically examine the different types of liability that will become relevant in insurance contracts relating to autonomous vessels.

1) *Product Liability:*

Product liability refers to a manufacturer or seller being held liable for selling a defective product to a consumer.[87] Generally, the law requires that a product must meet all the ordinary expectations of a consumer.[88] An entity that sells any defective product will thus be liable to the end user of the product for any injury or loss, which occurs because of defects.[89] There are three distinct ways in which a product may be classified as defective in the eyes of the law.[90] It may be defective in manufacture, in design and/or by failing to have adequate warnings or instructions.[91]

With the advent of autonomous vessels, there will be an increase in the demand for marine insurance policies, which cover product liability. This is because the vessels will operate without the presence of any humans on board and as such, the computer devices that are developed to replace the master and crew have to be of very high standard. This therefore means that manufacturers of these novel vessels, would want to ensure that if the vessel malfunctions because of a defect from the poor manufacturing of the vessel or a defect in design or one that relates to inadequate warnings or instructions, then they would have adequate insurance cover to protect them against such claims.

---

[86]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[87]Findlaw 'What is product liability?' https://injury.findlaw.com/product-liability/what-is-product-liability.html.

[88]Stapleton (1994).

[89]Stapleton (1994).

[90]Dolman Law Group '3 Types of Product Liability Claims' https://www.dolmanlaw.com/3-types-product-liability-claims/.

[91]Dolman Law Group '3 Types of Product Liability Claims' https://www.dolmanlaw.com/3-types-product-liability-claims/.

2) *Pollution Liability:*

Marine disasters are inevitable.[92] Over the last century, there have been many notable maritime accidents, which caused pollution to the environment.[93] Although it is expected that autonomous vessels will operate more efficiently and as such it is expected that there will be less accidents or incidents that should pollute the environment,[94] this is not an absolute certainty. Additionally, although some autonomous vessels are expected to have zero emissions, it is not yet known what other novel polluting substances that autonomous vessels that are not zero-emissions will release. Therefore, it would be prudent for any owner or operator of an autonomous vessel, to ensure that their insurance policies cover pollution liability.

3) *Personal Injury Liability*

Under conventional manned vessels, there is usually insurance to cover personal injury done to crew, masters and passengers.[95] Although autonomous vessels will be without a master and a crew, an insurance to cover personal injury claims would still be pertinent. This is because collisions may occur with other vessels that are carrying crew and passengers and as such, the ship-owner or charterer may be the subject of personal injury claims. As such, personal injury should be covered in any insurance contract being entered into by the owner and/or charterer of an autonomous vessel.

4) *Collision Liability*

Although it is expected that collisions should be less because of the use of autonomous vessels, as humans, who are the main cause of maritime accidents are eliminated, it is still a possibility that systems can malfunction and a collision with another vessel at sea may occur. As such, provisions against collisions should be covered in any insurance contract that relates to autonomous vessels.

5) *Vicarious Liability*

Vicarious liability usually occurs where an employer is liable for the negligent actions of his employee who was not acting on a frolic of his own.[96] Arguably, if the vessel is fully automated, there would be no employees and as such no need for coverage for vicarious liability. However, if it is simply unmanned and is remotely controlled by a shore-based operator, it is arguable that it would be prudent to have coverage against vicarious liability in those circumstances. This is because shore based operators could negligently operate the vessel remotely and cause damage which the owner or charterer would be responsible for.

[92]Ceyhun (2014).

[93]Theodore Styliadis, Ioannis Koliousis 'Shipping Accidents, damage assessment & accident consequences' https://www.onthemosway.eu/wp-content/uploads/2015/06/ship-accidents-1final.pdf.

[94]Deketelaere (2017).

[95]Gurses (2015).

[96]Giliker (2010).

Claims

Another very important aspect of marine insurance law that should be considered is that of claims. It has been posited that as it relates to claims and autonomous vessels, insurance companies may see a decline in the number of claims and the amount of money they have to pay out if autonomous vessels are used extensively in the future.[97] It is arguable however that the total number of claims may not necessarily be reduced but what may happen is that the nature of the claims might very well change.[98] It has been stated as an example that in autonomous vessels, there may be fewer claims as it relates to cargo loss because of human error during the loading process but there may be an increase in the number of claims arising from delay because of malfunctioning technology or breaches of cyber security. However, claims may be settled at a faster rate than before because of the high quality technology that should produce high quality evidence in the aftermath of an incident.[99] It is expected that there will be a digital log of all activity that takes place on board an autonomous vessel and this log should not be susceptible to human manipulation.[100] If this is so, whenever a claim is made, the logs for the various systems should be able to generate an automated report and could possibly provide the relevant parties with a digital record of what exactly took place. Additionally, ship-owners and their insurers may seek to take advantage of indemnity insurance, where claims for losses are not because of any fault on the part of the ship-owner, but because of some manufacturing defect.[101] This may be heavily dependent however on the warranty or the sales contract between the manufacturer and the ship-owner.[102]

[97]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[98]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[99]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018 https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[100]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[101]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

[102]Jessica Maitra, 'Unmanned Vessels and the Carriage of Goods-Contractual and Insurance Considerations' (Clyde & Co., 18 January, 2018) https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid.

5.2 *Standard Form Charter-Parties and Their Application to Autonomous Vessels from an Insurance Law Perspective*

A charter party may be defined as a document of contract by which a ship-owner agrees to lease, and the charterer agrees to hire, a vessel or all the cargo space, or a part of it, on certain terms and condition.[103] In simpler words, a charter party is essentially a deed between a ship-owner and a trader for the hire of a ship and the delivery of cargo.[104] The charter party is arguably one of the most important commercial shipping instruments because it provides generally great utility and protection to the parties involved, as well as it outlines clearly their agreed negotiation terms.[105] Parties are generally free to draft their own charter parties to suit their respective needs but it is usually preferred in the marine trade industry to use what is known as standard charter parties.[106] Typically, there are three types of charter parties. These are:

1) Voyage charter party;
2) Time Charter party; and
3) Bareboat charter party.[107]

The focus of the discussion in this section will be mostly on standard voyage charter parties and standard time charter parties as they are the most common forms of charter parties. It has been reported that the Baltic and International Maritime Council (BIMCO) has approved over fifty (50) charter parties with the majority being for voyage charter-parties.[108] The most common standard form charter parties however are the GENCON 94 for voyage charter parties and the New York Produce Exchange FORM (NYPE) 93 and 15 for time charter parties.[109] The author will now critically examine how autonomous vessels will impact these charter parties and what are the important insurance law considerations in relation to same.

The GENCON 94

The General Charter Conditions (GENCON) 94 charter party is the most common standard voyage charter party form that has been used worldwide.[110] It was first

[103] Antoniadou (2016).
[104] English Oxford Living Dictionaries https://en.oxforddictionaries.com/definition/charter_party.
[105] Antoniadou (2016).
[106] Rogers et al. (2016).
[107] Rogers et al. (2016).
[108] Antoniadou (2016).
[109] Antoniadou (2016).
[110] Baughen (2004).

issued in 1922 and then it was revised twice in 1976 and then in 1994 to be up to date with shipping practices at the time.[111] It has thus been over 24 years since the GENCON was last revised.

In Part II of the GENCON 94, Clause 2 describes the owners' responsibilities. Clause 2 states that

> the Owners are to be responsible for loss of or damage to the goods or for delay in delivery of the goods only in case the loss, damage or delay has been caused by personal want of due diligence on the part of the Owners or their Manager to make the Vessel in all respects seaworthy and to secure that she is properly manned, equipped and supplied, or by the personal act or default of the Owners or their Manager...[112]

On careful examination of this clause, it is observed that if there is loss or damage or delay in the delivery of goods because of the owner or their manager not making the vessel in all respects seaworthy and ensuring the she is properly manned, then the owners will be responsible for such loss or damage or delay. The GENCON94 neither contemplate nor accommodate usage by autonomous vessels. Simply having a vessel unmanned would make an owner liable for any loss or damage that arises regardless of whether this was the cause of the loss or damage. The author finds further support in this by examining other clauses in Part II of the GENCON94. When one carefully observes the provisions of the GENCON94, one will observe that the text is heavily laden with the words master and crew. Clause 5 (c) of Part II of the GENCON94 for example makes reference to damage done by stevedore.[113] The GENCON 94 makes the Charterers responsible for damage to the vessel caused by stevedores and requires that the master notify the charterer as soon as possible as to any damage caused to the vessel by stevedores.[114] However, in a situation where there are autonomous vessels, this would not be practical. Therefore, this particular clause would have to be amended. It would also be pertinent for an insurance company to ensure that the charter party terms adequately outlines the respective roles and liabilities to ensure that the various risks are properly covered. Further, charter party terms where they are parallel to clauses of an insurance contract should also, where possible, correspond with these insurance contract terms.

Similarly, Clause 5 (b) of the GENCON 94 makes reference to crane men and winch men and that they shall be under the charterer's risk and responsibilities and are deemed as servants.[115] It also notes that they shall always work under the supervision of the master.[116] This clause must also be amended or modified to accommodate autonomous vessels. This could be done either through the development of a more modern version to the GENCON 94 or by the insertion of a rider

[111] Singh (2011).

[112] See Part II, Clause 2 of the GENCON 94.

[113] See clause 5 (c) of Part II of the GENCON 94.

[114] See clause 5 (c) of Part II of the GENCON 94.

[115] See clause 5 (b) of the GENCON 94.

[116] See clause 5 (b) of the GENCON 94.

clause.[117] Additionally, from an insurance law perspective, the charterer who is using a standard form charter party such as the GENCON 94 could assume less risk and responsibilities in this respect as the vessel would be crewless and as such there would be no liability for how the crane men and winch men operate the vessels cargo handling gear which is typical in a manned vessel situation.[118] However, what a charterer must now contemplate is whether in the case of a shore-operated autonomous vessel, the shore operators who are responsible for the cargo handling gear can be considered as virtual winch men and crane men. A charterer will in that regard must consider what liability they would have under the GENCON 94 in relation to these shore-operated autonomous vessels.

NYPE 93 and NYPE 15

The New York Produce Exchange Form (NYPE) 15 is a revised version of the New York Produce Exchange Form (NYPE) 93.[119] The idea behind any charter party revision over the years was to, as stated earlier, enable the charter party to be up to date with modern times and modern trends.[120] Upon a comparative examination of NYPE 15 against NYPE 93, it is questionable if this recent revision in the year 2015 has really been updated enough to be in tandem with modern trends.

Article 2 of NYPE 93 for example which addresses delivery stated that:

> The Vessel on her delivery shall be ready to receive cargo with clean-swept holds and tight, staunch, strong and in every way fitted for ordinary cargo service, having water ballast and with sufficient power to operate all cargo-handling gear simultaneously.[121]

However, Article 2 of NYPE 15 is far more extensive than the previous corresponding section mentioned in the NYPE 93. It interestingly includes amongst other things, that

> The vessel on delivery shall be seaworthy and in every way fit to be employed for the intended service. . .with full complement of Master, officers and ratings who meet the Standards for Training, Certification and Watchkeeping for Seafarers (STCW) requirements for a vessel of her tonnage.[122]

The author questions the rationale for including this in Article 2 of the NYPE15, especially since a similar section exists in Article 6 under the heading of *'Owners to Provide.'* This is particularly curious the author finds having regard to the fact that

[117] Rider clauses may be defined as a set of additional clauses which substitute or supplement a standard charter party. If a rider clause conflicts with a printed clause in a standard charter party, then the rider clause prevails.

[118] See clause 5 (b) of the GENCON 94.

[119] Soyer et al. (2017).

[120] Antoniadou (2016).

[121] See Article 2 of NYPE 1993.

[122] See Article 2 of NYPE 2015.

research into automated and unmanned vessels predated 2015.[123] The author ponders therefore if the additional inclusion of a clause, which speaks to a vessel having on delivery a full complement of master, officers and crew in the NYPE15, is the maritime industry subtly indicating its reluctance to the innovation of autonomous vessels? The author acknowledges however that it is also a possibility that such a clause was included which in essence excludes autonomous vessels from using the charter, without any direct consideration for autonomous vessels, as they had not began sailing at that moment.

Nevertheless, from a marine insurance point of view, an owner of an autonomous vessel should be very hesitant when using the NYPE 15 without modifications and without rider clauses, as it would hold a vessel unseaworthy if it were delivered without a full complement of a master, officers and crew.[124] Thus, it is arguable that if any loss should happen from simply sailing a vessel without a master and crew and such loss was not related to such absence on the vessel of a master officers and crew, the vessel would still be considered to be unseaworthy. Insurance companies would also be reluctant to insure an autonomous vessel that is in the habit of trading using a standard charter time party such as the NYPE15, as they could possibly face a large amount of claims because technically a vessel being delivered without any master and crew according to the NYPE15 is one that is unseaworthy and thus unfit to undertake any voyage.

On further perusal of the NYPE15, it is evident that there are other clauses that would not directly be applicable to autonomous vessels. Clause 7 for example, illustrates that the owner will provide fumigations due to illness of the crew under the charter party.[125] This would certainly no longer be necessary for autonomous vessels. Similarly, Clause 8 also illustrates that the master shall perform the voyages with due dispatch and shall render such customary assistance with the crew. In this respect, it would not particularly be applicable to autonomous vessels as it is not practical for autonomous vessels to render customary assistance to another vessel in distress without an onboard crew.

It is interesting to note that NYPE15 has allowed in Clause 32 the usage of BIMCO Electronic Bills of Lading Clause, which was not previously mentioned in NYPE 93.[126] It could be argued that reference to such clause neither was mentioned in NYPE 93 as they were not at the time being researched nor were they in use. However, it is puzzling why autonomous vessels were not accounted for in the NYPE15 owing to the fact that at the time of the update, there were discussions and research being conducted on autonomous vessels. The author is pleased to observe that the drafters have included an innovative element in the new NYPE15 but

[123]Extensive research into the commercial use of autonomous vessels began as early as 2010. See Manda (2016).

[124]See Article 2 of NYPE 2015.

[125]See clause 7 of the NYPE 15.

[126]See the NYPE 93.

believes that more could be done. The drafters of the NYPE charter parties need to be more pro-active rather than reactive.

Another clause in the NYPE 15 that may prove problematic for autonomous vessels is that of Clause 39, which is the BIMCO Piracy Clause for time charter parties 2013.[127] This clause states that the vessel shall not be obliged to proceed or required to continue to or through any port, place, area or zone, waterway or canal which in the reasonable judgment of the master and/or the owners, is dangerous to the vessel, her cargo, crew or other persons on board the vessel because of actual, threatened or reported acts of piracy and/or violent robbery. This of course will prove challenging for autonomous vessels to comply with because it requires direct human action and requires critical thinking of the human mind. The master is required to use his judgment to avoid entering an area, which is plagued by piracy. However, with the master being removed from the equation, these vessels must be equipped with such high level of artificial intelligence that they are able to detect if an area is one that is dangerous to the vessel because of piracy. It can be observed however that this clause puts the obligation not only on the master but also on the owners. This therefore means that if the master were absent, as in the case of an autonomous vessel, the onus would now be on the owners to use their judgment to prevent the vessel from proceeding to a dangerous area. This in theory sounds workable for autonomous vessels but this may nonetheless be difficult to comply with. Owners must ensure that the vessels are equipped with proper sensors that are of such high artificial intelligence that they are able to detect a dangerous area. However, as this is heavily independent on artificial intelligence, there may be malfunctioning systems, which may result in a port or another area not being detected as one that is dangerous, and similarly, it may mistakenly detect a safe area as a dangerous one.

Additionally, as it relates to piracy, this clause should have made reference to cyber piracy so as to properly accommodate the situations that may arise as it relates to autonomous vessels. Clause 39 (c) states that if the owners consent to the vessel proceeding to an area that is exposed to the risk of piracy, the owners should amongst other things, comply with underwriters requirements under the terms of the vessel's insurance.[128] It is arguable that in the case of an autonomous vessel, their insurance contracts should contain risks, which address cyber piracy and thus, the owner must be mindful of such clauses when proceeding in an area that research has shown to be more prone to attacks by cyber pirates.

Another clause that is of concern in the NYPE 15 is Clause 42, which addresses stowaways. The Convention on Facilitation of International Maritime Traffic, 1965, as amended, defines stowaway as

> A person who is secreted on a ship, or in cargo which is subsequently loaded on the ship, without the consent of the shipowner or the Master or any other responsible person and who is detected on board the ship after it has departed from a port, or in the cargo while unloading

[127] See clause 39 if the NYPE 15.

[128] See clause 39 (c) of the NYPE 15.

> it in the port of arrival, and is reported as a stowaway by the master to the appropriate authorities.[129]

The presence of stowaways on board vessels can cause serious consequences for the vessel as their presence can cause considerable delay in a port as well as the repatriation of stowaways to their national country can be an expensive venture for all parties involved.[130] In addition, there are human rights considerations as stowaways can die from suffocation or lack of food while on board a vessel.[131]

Clause 42 (a) of the NYPE 15 state that if a stowaway has gained access to a vessel by means of secreting away in the goods and/or containers or by any other means related to the cargo operation, it shall be a breach of the charter party and the charterers shall be liable for the consequences of such breach and shall hold the owners harmless and indemnify them against all claims. However, Clause 42 (b) of the NYPE 15 state that if a stowaway has gained access to the vessel other than through the conditions of 42 (a), then the owners shall be liable and shall hold the charterers harmless and indemnify them against all claims as a result of the breach.

With the introduction of autonomous vessels, stowaways will become a major issue. It is foreseeable that stowaways will think that since nobody is physically on board the vessel, it is much easier to enter and remain on board a vessel without detection. The author ponders if Clause 42 should be considered as fair where there is an autonomous vessel involved. Shouldn't there be another class of persons to whom liability can be placed on, namely the manufacturers of the vessel? There should be a part (c) added to Clause 42 of the NYPE15 that would state something to the effect that if stowaways enter the vessel because of malfunctioning or defective detection software, then the owners are entitled to be indemnified from any claims by the manufacturers. This clause itself will also be problematic as it raises questions of privity to contract and whether a third party could really be held liable on a charter party contract where he or she is not a direct party of that contract. If this proves to be extremely problematic to include as part of the charter party terms, it is suggested that in the alternative, owners should ensure that a similar clause is included in their sale contracts with manufacturers, as it is extremely unreasonable that an owner should be held liable for stowaways presence on a vessel, when the stowaway was only able to enter the automatic vessel because of a defective software.

---

[129]IMO 'Stowaways'http://www.imo.org/en/OurWork/Facilitation/Stowaways/Pages/Default.aspx.

[130]IMO 'Stowaways'http://www.imo.org/en/OurWork/Facilitation/Stowaways/Pages/Default.aspx.

[131]"Stowaways: the hidden problem at sea" (Ship Technology, 03 January 2017) https://www.ship-technology.com/features/featurestowaways-the-hidden-problem-at-sea-5708512/.

6 National Marine Insurance Laws and Their Ability to Accommodate Autonomous Vessels

It is of great importance to discuss the effect that autonomous vessels will have on national marine insurance laws. It is not practical to discuss the marine insurance legislation which exists in every territory and as such, the author has chosen to the critically examine the marine insurance legislations of the United Kingdom (UK) and the Nordic countries. The author will thus critically examine specifically the Marine Insurance Act 1906 of the United Kingdom and the Nordic Insurance Plan of 2013 Version 2016. These two legislations were selected because the Marine Insurance Act 1906 has been considered as the '*mother of all insurance statutes*'[132] and the Nordic Insurance Plan 2013 Version 2016 represents a modern and up to date marine insurance legislative model.[133] Additionally, as it relates to regulations for autonomous vessels, both the United Kingdom and Norway are leading the research in these aspects. In October 2016, Norway opened the world's first designated test area for unmanned vessels and there is a UK-sponsored project called the Machine Executable Collision Regulations for Marine Autonomous Systems that are currently matching navigation algorithms for unmanned vessels and conducting extensive research into regulations.[134]

6.1 The UK's Marine Insurance Act 1906

The UK's Marine Insurance Act 1906 (MIA 1906) which was drafted by Sir Mackenzie Chalmers,[135] is an Act that did not seek to redefine the law as it then was but was simply a codification of existing laws.[136] Over the years there have been many debates that the UK's 1906 Marine Insurance Act is obsolete and many calls have been made for it to be repealed in its entirety.[137] The UK finally yielded to these calls over one hundred (100) years later when they introduced the Insurance Act 2015.[138] The Insurance Act 2015 replaced some sections of the Marine Insurance Act 1906 but there are some sections of the Act, which still remains exactly the same.[139] The author will now critically examine some of the existing sections of the

[132]Fitzmaurice (2016).

[133]The Nordic Association of Marine Insurers 'Nordic Plan 2013' http://www.cefor.no/Documents/Clauses/Nordic%20Plan%202013/2013/Brochure%20-%20Nordic%20Plan%202013.pdf.

[134]The Nordic Association of Marine Insurers 'Annual Reports' http://www.cefor.no/Documents/Statistics/Annual%20reports/Cefor%20Annual%20Report%202016.pdf.

[135]Thomas (2016).

[136]Thomas (2016).

[137]Noussia (2007).

[138]Clarke et al. (2017).

[139]See the Marine Insurance Act 1906 and compare same with Insurance Act 2015 of the UK.

Act, which have not been repealed to discover if these sections can accommodate autonomous vessels.

Are Unmanned Vessels Covered by the Marine Insurance Act 1906?

Firstly, it is critical to the discussion of whether the Marine Insurance Act 1906 is able to properly accommodate autonomous vessels, to critically examine whether the Act is applicable to autonomous vessels.

Section 2 (2) of the Marine Insurance Act 1906 states that

> Where a ship in course of building, or the launch of a ship, or any adventure analogous to a marine adventure, is covered by a policy in the form of a marine policy, the provisions of this Act, in so far as applicable, shall apply thereto; but, except as by this section provided, nothing in this Act shall alter or affect any rule of law applicable to any contract of insurance other than a contract of marine insurance as by this Act defined.[140]

Based on the above section, it is evident that the Marine Insurance Act 1906 can certainly apply to insurance policies governing autonomous vessels. The section does not specify that it has to be a ship that has a master and/or crew but simply states that once a ship is covered by a marine policy, then the provisions of the Act will apply. Additionally, it is unlikely that an autonomous vessel would set sail without a marine insurance policy, as that would be grossly negligent. Thus, it is strongly viewed that the Marine Insurance Act 1906 will apply to UK insured autonomous vessels.

Additionally, Section 3 (1) of the MIA 1906 states that every lawful marine adventure may be the subject of a contract of marine insurance. The section goes on to state that there is a marine adventure where amongst other things, any ship goods or movables are exposed to maritime perils.[141] This section further supports the view that the MIA 1906 is applicable to autonomous vessels.

Are Risks Associated with Autonomous Vessels Covered by the MIA 1906?

It is also imperative to examine whether marine insurance policies that are applicable to the MIA1906 are able to adequately protect against the risks associated with autonomous vessels.

Section 2 (1) of the MIA 1906 state that

> A contract of marine insurance may, by its express terms, or by usage of trade, be extended so as to protect the assured against losses on inland waters or on any land risk which may be incidental to any sea voyage.[142]

---

[140] See Section 2 (2) of the UK's Marine Insurance Act 1906.

[141] See Section 3 (1) of the UK's Marine Insurance Act 1906.

[142] See Section 2 (1) of the UK's Marine Insurance Act 1906.

As discussed above, autonomous vessels will be exposed to similar land and sea risks as are typically incidental to manned vessels. However, it has been noted that autonomous vessels also face novel risks such as cyber risks and as such, Section 2 (1) of the MIA 1906 needs to be amended to include cyber risks to adequately apply to autonomous vessels. It may however be argued in the alternative that land risks should be interpreted to include cyber risks.

It could also further be argued in the alternative that the MIA 1906 is capable of incorporating cyber risks and thus being adequately applicable to marine insurance policies concerning autonomous vessels because of how wide it has defined the term "maritime perils." Section 3 of the MIA 1906 has defined the term to mean:

> Maritime perils" means the perils consequent on, or incidental to, the navigation of the sea, that is to say, perils of the seas, fire, war perils, pirates, rovers, thieves, captures, seisures, restraints, and detainments of princes and peoples, jettisons, barratry, and any other perils, either of the like kind or which may be designated by the policy.[143]

The fact that the section includes the phrase *"and any other perils"*,[144] the MIA 1906 is able to apply to other perils such as cyber attacks and cyber piracy which are risks that are arguably unique to autonomous vessels.

Applicability of Masters' and Seamen's Wages Under the MIA 1906 to Autonomous Vessels

Section 11 of the MIA 1906 states that

> The master or any member of the crew of a ship has an insurable interest in respect of his wages.

It is arguable that this section would not be applicable to autonomous vessels as they are void of a master and a crew. Only if it is a remotely controlled autonomous vessel, then the shore based operator, it may be argued, may be able to fall within the ambits of a master and the computer programmers or network engineers could fall within the definition of "crew" then this section would be applicable. It therefore means that this section in its current form is unlikely to apply to autonomous vessels but it has to be considered whether other employees of autonomous vessels are able to claim an insurable interest in respect of his or her wages.

Measure of Insurable Value and Autonomous Vessels Under the MIA 1906

Section 16 of the MIA 1906 states that

[143] See Section 3 of the UK's Marine Insurance Act 1906.

[144] See Section 3 of the UK's Marine Insurance Act 1906.

> Subject to any express provision or valuation in the policy, the insurable value of the subject-matter insured must be ascertained as follows:—
>
> (1) In insurance on ship, the insurable value is the value, at the commencement of the risk, of the ship, including her outfit, provisions and stores for the officers and crew, money advanced for seamen's wages, and other disbursements (if any) incurred to make the ship fit for the voyage or adventure contemplated by the policy, plus the charges of insurance upon the whole: The insurable value, in the case of a steamship, includes also the machinery, boilers, and coals and engine stores if owned by the assured, and, in the case of a ship engaged in a special trade, the ordinary fittings requisite for that trade

This section essentially states that as it relates to insurance for a ship, the insurable value includes the value of the provisions for the officers and crews, money advanced for seafarer's wages and other disbursements. There must be an express provision in marine insurance policies that relate to autonomous vessels to either exclude the application of Section 16 of the MIA 1906 in its entirety or an express provision that modifies the wording of the clause in the respective policy. In the case of an autonomous vessel, the insurable value would neither include provisions and stores for officers as there would be no humans on board, nor would such insurable value include advanced money for seafarer's wages. Rather, the insurable interest would include wages for marine computer engineers and shore based controllers as well as the value of the on-board hardware and software technology. Additionally, reference to a steamship and boilers should be removed altogether as it is unlikely that autonomous vessels would be steamrolled.

Applicability of Deviation Clauses Under the MIA 1906 to Autonomous Vessels

Clauses in the MIA 1906 that address deviation and delay are of utmost importance to autonomous vessels. This is because there is a higher risk of a vessel being deviated remotely without authorisation by what is known as a cyber pirate, or an autonomous vessel deviating because of malfunctioning of its on- board technology.

Section 46 of the MIA 1906 states that

> Where a ship, without lawful excuse, deviates from the voyage contemplated by the policy, the insurer is discharged from liability as from the time of deviation, and it is immaterial that the ship may have regained her route before any loss occurs.[145]

Section 49 of the MIA 1906 further outlines the circumstances under which deviation or delay may be excused. The section states that

> Deviation or delay in prosecuting the voyage contemplated by the policy is excused—
>
> (a) Where authorised by any special term in the policy; or
> (b) Where caused by circumstances beyond the control of the master and his employer; or
> (c) Where reasonably necessary in order to comply with an express or implied warranty; or
> (d) Where reasonably necessary for the safety of the ship or subject-matter insured; or

[145] See Section 46 of the UK's Marine Insurance Act 1906.

(e) For the purpose of saving human life, or aiding a ship in distress where human life may be in danger; or
(f) Where reasonably necessary for the purpose of obtaining medical or surgical aid for any person on board the ship; or
(g) Where caused by the barratrous conduct of the master or crew, if barratry be one of the perils insured again[146]

It is possible that deviation or delay in the case of an autonomous vessel where the cause of such deviation or delay was from a cyber attack or a technological malfunction, then these could possibly be considered as lawful excuse under Section 49 (b) of the MIA 1906. This is so because it could successfully be argued that these were circumstances beyond the control of the owner. Alternatively, it is suggested that deviation or delay because of a cyber attack and/or technological malfunction could be argued as the kind of deviation or delay that is authorised as a special term under the specific policy, as was stated in Section 49 (a) of the MIA 1906. This would therefore mean that such deviation or delay must be explicitly excused under the respective policy.

Applicability of Signature on Policy Clause Under the MIA 1906 to Autonomous Vessels

Section 24 (1) of the MIA 1906 states that

> A marine policy must be signed by or on behalf of the insurer, provided that in the case of a corporation the corporate seal may be sufficient, but nothing in this section shall be construed as requiring the subscription of a corporation to be under seal.

To fully accommodate autonomous vessels, this section could be modified to allow for digital or electronic signatures rather than actual physical signatures.[147]

6.2 The Nordic Marine Insurance Plan 2013 Version 2016

The author will now examine the Nordic Marine Insurance Plan (NMIP) 2013 Version 2016 and its potential impact on insurance policies concerning autonomous vessels. The Nordic Marine Insurance Plan 2013 was developed out of an agreement dated November 3, 2010 between the Nordic association of marine insurers, the Danish Shipowners Association, the Finnish Shipowner's Association, the Norwegian Shipowner's Association and the Swedish Shipowner's Association.[148] It replaces the Norwegian Marine Insurance Plan of 1996 which dates back to

[146]See Section 49 of the UK's Marine Insurance Act 1906.

[147]Merkin et al. (2014).

[148]Trine-Lise Wilhelmsen, 'The Nordic Marine Insurance Plan of 2013 Version 2016'http://www.nordicplan.org/The-Plan/Preface/.

1871.[149] The present version of the NMIP is the 2016 version and it is expected that a new version of same will be adopted in 2019.[150]

The Insurable Value

Clause 2-1 of the Nordic Marine Insurance Plan 2013 Version 2016 states that the insurable value is the full value of the interest at the inception of the insurance. This clause also states that the parties may by agreement, fix the insurable value at a certain amount, which shall be called the agreed insurable value.[151] From a comparative perspective, it is clear that the NMIP insurable values' clause is able to accommodate insurance policies that are drafted for autonomous vessels. This is because the clause states that the insurable value is simply the value of the interest, which would be the autonomous vessel for this chapter. In comparison with the MIA 1906, the wording of this section is certainly more modern and less restrictive than the MIA 1906. The MIA 1906 as discussed above states that the insurable interest includes things such as advances for seamen wages and stores for crew and officers on board which is not required by the NMIP.[152] Another important comparative observation made is the fact that in the corresponding section on insurable value under the MIA 1906, distinction was made for the insurable value as it relates to steamships. However, under the more modern Nordic Insurance plan, there is no distinction made between the type of vessel and as such, this section will certainly be applicable to insurance policies relating to autonomous vessels.

Perils Insured Against

Under the Nordic Marine Insurance Plan 2013 Version 2016, Clause 2-8 addresses what marine perils are. Unlike the MIA 1906, the NMIP 2013 Version 2016 divides perils into marine perils, and war perils. As it relates to marine perils, it states that

> An insurance against marine perils covers all perils to which the interest may be exposed, with the exception of:
>
> a. the perils covered by an insurance against war perils in accordance with Cl. 2-9,
> b. intervention by a State power. A State power is understood to mean individuals or organisations exercising public or supranational authority. Measures taken by a State power for the purpose of averting or limiting damage shall not be regarded as an intervention, provided that the risk of such damage is caused by a peril covered by the insurance against marine perils,
> c. insolvency,
> d. perils covered by the RACE II Clause:

[149] See clause 2-1 of the Nordic Marine Insurance Plan 2013 Version 2016.

[150] See clause 2-1 of the Nordic Marine Insurance Plan 2013 Version 2016.

[151] See clause 2-1 of the Nordic Marine Insurance Plan 2013 Version 2016.

[152] See clause 2-1 of the Nordic Marine Insurance Plan 2013 Version 2016.

1. ionising radiations from or contamination by radioactivity from any nuclear fuel or from any nuclear waste or from the combustion of nuclear fuel,
2. the radioactive, toxic, explosive or other hazardous or contaminating properties of any nuclear installation, reactor or other nuclear assembly or nuclear component thereof,
3. any weapon or device employing atomic or nuclear fission and/or fusion or other like reaction or radioactive force or matter,
4. the radioactive, toxic, explosive or other hazardous or contaminating properties of any radioactive matter. The exclusion in this sub-clause does not extend to radioactive isotopes, other than nuclear fuel, when such isotopes are being prepared, carried, stored, or used for commercial, agricultural, medical, scientific or other similar peaceful purposes.
5. any chemical, biological, bio-chemical, or electromagnetic weapon.[153]

Clause 2-9 of the NMIP illustrates what an insurance against war perils should cover. It states that

An insurance against war perils covers:

a. war or war-like conditions, including civil war or the use of arms or other implements of war in the course of military exercises in peacetime or in guarding against infringements of neutrality,
b. capture at sea, confiscation and other similar interventions by a foreign State power. Foreign State power is understood to mean any State power other than the State power in the ship's State of registration or in the State where the major ownership interests are located, as well as organisations and individuals who unlawfully purport to exercise public or supranational authority. Requisition for ownership or use by a State power shall not be regarded as an intervention,
c. riots, sabotage, acts of terrorism or other social, religious or politically motivated use of violence or threats of the use of violence, strikes or lockouts,
d. piracy and mutiny,
e. measures taken by a State power to avert or limit damage, provided that the risk of such damage is caused by a peril referred to in sub-clause 1 (a)–(d).[154]

The section also excludes insolvency and perils covered by RACE II Clause.

Upon critical examination of these sections, it is evident that an insurance covering only marine perils would not be sufficient in the case of an autonomous vessel, if a policy is being taken out subject to the Nordic Marine Insurance Plan. This is because it explicitly excludes war risks such as piracy and mutiny, which would be a risk that is directly relevant to autonomous vessels as they can be the subject of cyber pirates. As such, it would mean that the owner of an autonomous vessel, who is interested in insuring an autonomous vessel under the Nordic Marine Insurance Plan, must take out two policies, one against marine perils and one against war perils. This would mean that the owner would have two premiums to pay, which may be more expensive than if they simply took out one policy that protects against marine perils including piracy, as is done under the MIA 1906. Therefore, this section of the Nordic Marine Insurance Plan could be amended to consolidate war perils under the heading of marine perils.

[153] See clause 2-8 of the Nordic Marine Insurance Plan 2013 Version 2016.

[154] See Clause 2-9 of the Nordic Marine Insurance Plan 2013 Version 2016.

Nevertheless, the Nordic Marine Insurance Plan 2013 Version 2016 still represents a more modern plan than the MIA 1906, and this is evident from the fact that the NMIP 2013 is not so focused on the concept of master and crew as is heavily done under the MIA 1906. The author could only find very few clauses in the NMIP 2013 Version 2016 that explicitly used the word master. One such example is that of Clause 3-29. This clause states that:

> If a casualty threatens to occur or has occurred, the assured shall, without undue delay, notify the insurer and keep him informed about further developments. The assured and the master are required to notify the insurer of maritime inquiries and surveys which are to be held in connection with the casualty.[155]

It is interesting that in the first half of the above clause, it only requires the assured to notify the insurer if a casualty occurs or has occurred. The first half of the clause can easily be satisfied by the assured of an autonomous vessel, as the computer systems onboard the vessel should be so advanced that it would be able to notify the assured of the threat of a casualty or if a casualty actually occurs. However, interestingly, the second half of the Clause 3-29 of the NMIP requires both the assured and the master to notify the insurer of maritime inquires and surveys, which are to be held in connection with the casualty. This will be a bit onerous and impractical for owners of autonomous vessels, as they do not have a master. Further, this section should be modified to state that either the assured or the master should notify the insurer, or simply require the assured alone to do same, so that it is not too difficult for autonomous vessels to comply with this section.

Overall, there should be very little difficulty in autonomous vessels complying with the Nordic Marine Insurance Plan 2013 Version 2016, as from the critical observation of the legislation in its entirety, majority of its clauses are compatible with autonomous vessel.

7 Conclusion

Autonomous vessels are an astounding innovation that is likely to yield tremendous benefits to international trade. Highlighted throughout this chapter are several benefits that are likely to be derived from the commercial use of autonomous vessels. These benefits include a possible decrease in maritime accidents because most accidents are caused by human error, the expectation that autonomous vessels should operate in a more environmentally friendly manner, as well as the likelihood that there will be more cargo space on board autonomous vessels which may lead to increase freight for ship-owners. Notwithstanding the several benefits highlighted, it was also illustrated that there are several drawbacks that may be presented as a result of autonomous vessels, which include the fact that traditional seafarers may lose their jobs, which could cause financial strain on these traditional seafarers. Overall,

[155] See Clause 3-29 of the Nordic Marine Insurance Plan 2013 Version 2016.

autonomous vessels from the perspective of international maritime law and marine insurance law may initially be a risky expedition because it is novel and as such, it will involve much *'trial and error'* before it can sail smoothly. The expedition may be rocky because of the fact that many international conventions are not currently in a position to properly accommodate autonomous vessels. This may require the development and implementation of a working group that has the dedicated task of developing new international maritime conventions that properly considers autonomous vessels or it may require in some cases, a wide scale reformation of existing international maritime conventions so that they can become more compatible with autonomous vessels. Other circumstances that may contribute to the journey being a risky expedition include the fact that many standard charter parties, as discussed throughout this chapter, are not able to adequately accommodate trade by autonomous vessels unless rider clauses are used heavily. Similarly, issues relating to the novelty of the risks associated with autonomous vessels and how liability should be addressed may also lead to a quite rocky voyage. Further, it can be foreseen that national legislations will have to undergo an intensive reforming regime, where existing marine insurance laws are either updated or new laws are implemented that will properly account for the usage of autonomous vessels.

Lastly, initially it may be tedious to properly adjust all the relevant laws and update the necessary documentations, but once autonomous vessels become properly integrated as part of international trade practices, they would be smooth sailing and the global community shall truly enjoy the many benefits that autonomous vessels have to offer.

References

Table of Legislation

The Insurance Act 2015 UK
The Marine Insurance Act 1906 UK
The Nordic Marine Insurance Plan 2013 Version 2016

International Conventions

International Convention for the Prevention of Pollution from Ships, 1973 as modified by the Protocol of 1978
International Convention for the Unification of Certain Rules of Law relating to Bills of Lading
International Convention on Standards of Training Certification and Watchkeeping for Seafarers (STCW) 1995
International Regulations for Preventing Collisions at Sea 1972
United Nations Convention on Condition for Registration of Ships 1986
United Nations Convention on the Law of the Sea (Montego Bay 10 December 1982)

Commissioned Papers

The Law Commission Consultation Paper No 204 and The Scottish Law Commission Discussion Paper No 155: *"Insurance Contract Law: The Business Insured's Duty of Disclosure and the Law of Warranties."*

Books, Journal Articles, Thesis

Alderton T et al (2004) The Global Seafarer: living and working conditions in a globalized industry, 1st edn. ILO, Geneva

Antoniadou N (2016) Charter parties- an outdated form of contract?. M.Sc. Thesis, University of Piraeus

Ballin C (2017) Electric boats and ships-A history, 1st edn. McFarland & Company, Jefferson

Baughen S (2004) Shipping law, 3rd edn. Cavendish, Singapore

Ceyhun GC (2014) The impact of shipping accidents on Marine Environment: a study of Turkish Seas. Eur Sci J 10

Clarke M et al (2017) The Insurance Act 2015: a new regime for Commercial and Marine Insurance law, 1st edn. Routledge, Abingdon

de Vleeschhouwer S (2017) Safety of data. The risks of cyber security in the maritime sector. Netherlands Maritime Technology

Deketelaere P (2017) The legal challenges of unmanned vessels. M.Sc. thesis, University of Ghent

Fitzmaurice M (2016) The IMLI manual on international maritime law: shipping law, vol 2. Oxford University Press, Oxford

Giliker P (2010) Vicarious liability in tort: a comparative perspective, 1st edn. Cambridge University Press, Cambridge

Great Britain Law Commission (2012) Insurance contract law: the business insured's duty of disclosure and the law of warranties. Crown copyright

Gurses O (2015) Marine insurance law, 1st edn. Routledge, Abingdon

International Encyclopedia of Comparative Law (2002) Vol. 36

Leimbach M et al (2010) Technological change and international trade-insights from REMIND-R. Energy J 31:109–136

Manda D (2016) Development of autonomous surface vessels for hydrographic survey applications. M.Sc. Thesis, University of New Hampshire

Mathieu B (2016) Unmanned vessels: a major challenge for the next decades. M.Sc. thesis, University of Ghent

Merkin R et al (2014) Marine Insurance legislation, 5th edn. Routledge, Abingdon

de Miguel Molina M (2018) Ethics and civil drones: European policies and proposals for the industry, 1st edn. Springer, Berlin

Noussia K (2007) The principle of indemnity in marine insurance contracts: a comparative approach, 1st edn. Springer, Berlin

Rogers A et al (2016) Cases and materials on the carriage of goods by sea, 4th edn. Routledge, Abingdon

Singh L (2011) The law of carriage of goods by sea, 1st edn. Bloomsbury, London

Soyer B et al (2017) Charterparties: law, practice and emerging legal issues, 1st edn. Routledge, Abingdon

Springer PJ (2013) Military Robots and Drones: a reference handbook, 1st edn. ABC-CLIO, Santa Barbara

Stapleton J (1994) Product liability, 1st edn. Butterworths, Oxford

Thomas R (2016) The modern law of Marine Insurance, 1st edn. Routledge, Abingdon

Van Hooydonk E (2014) The law of unmanned merchant shipping-an exploration. J Int Maritime Law 20:403–423
Yeomans G (2014) Autonomous vehicles-handing over control: opportunities and risks for insurance. Lloyds Exposure Management

Websites

http://publications.lib.chalmers.se/records/fulltext/198197/local_198197.pdf
http://www.armatorlerbirligi.org.tr/Sites/1/upload/files/THE_GENUINE_LINK.pdf
http://www.businessinsider.com/google-apple-tesla-race-to-develop-driverless-cars-by-2020-2016-7#volvo-is-aiming-to-make-its-cars-deathproof-by-2020-by-rolling-out-semi-autonomous-features-in-its-cars-eventually-working-up-to-fully-driverless-ones-6
http://www.cefor.no/Documents/Clauses/Nordic%20Plan%202013/2013/Brochure%20-%20Nordic%20Plan%202013.pdf
http://www.cefor.no/Documents/Statistics/Annual%20reports/Cefor%20Annual%20Report%202016.pdf
http://www.imo.org/en/OurWork/Facilitation/Stowaways/Pages/Default.aspx
http://www.nordicplan.org/The-Plan/Preface/
http://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/12%20-%20AAWA%20Coordinator.pdf
http://www.seatrade-maritime.com/news/americas/the-economics-of-slow-steaming.html
http://www.shipinspection.eu/index.php/chartering-terms/84-r/4870-rider-clauses
http://www.unmanned-ship.org/munin/
http://www.unmanned-ship.org/munin/about/munin-results-2/
http://www.unmanned-ship.org/munin/about/munins-objectives/
https://ec.europa.eu/transport/sites/transport/files/pocketbook2017.pdf
https://en.oxforddictionaries.com/definition/charter_party
https://injury.findlaw.com/product-liability/what-is-product-liability.html
https://iumi.com/news/press-releases/global-marine-underwriting-premiums-continue-to-fall-reports-iumi
https://safety4sea.com/allianz-human-error-behind-75-percent-of-marine-casualties/
https://svw.no/contentassets/f424f309bd304e99b39f11355e98571f/svw_maritime-law-in-the-wake-of-the-unmanned-vessel.pdf
https://www.bartleby.com/essay/Air-Pollution-Smog-Acid-Rain-the-Greenhouse-F3CJKHPYTC
https://www.clydeco.com/insight/article/unmanned-vessels-and-the-carriage-of-goods-contractual-and-insurance-consid
https://www.dolmanlaw.com/3-types-product-liability-claims/
https://www.hemisphere-freight.com/autonomous-crewless-ships-are-there-risks-to-the-ocean-freight-industry/
https://www.independent.co.uk/news/science/ghost-ships-coming-yara-birkeland-norway-maritime-law-changing-fewer-accidents-cheaper-shipping-a7930481.html
https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/4B8113B707A50A4FC125811D00407045?OpenDocument
https://www.lexology.com/library/detail.aspx?g=4d7c0773-4692-4922-a469-4a384f6c8340
https://www.marineinsight.com/maritime-law/what-is-sulphur-oxides-or-sox-air-pollution-from-ships/
https://www.marinelog.com/index.php?option=com_k2&view=item&id=26653:autonomous-vessels-not-so-remote&Itemid=257
https://www.maritime-executive.com/editorials/would-autonomous-ships-be-good-for-society#gs.UeDHR2E

https://www.maritime-executive.com/magazine/look-beyond-the-flag
https://www.onthemosway.eu/wp-content/uploads/2015/06/ship-accidents-1final.pdf
https://www.rolls-royce.com/media/our-stories/press-releases/2016/pr-12-04-2016-aawa-project-introduces-projects-first-commercial-operators.aspx
https://www.ship-technology.com/features/featurestowaways-the-hidden-problem-at-sea-5708512/
https://www.yara.com/knowledge-grows/game-changer-for-the-environment/