New Technologies

Political, legal, economic and factual impact in Germany

A. Driverless/autonomous vehicles and vessels

- *Are there any specific laws already adopted in your jurisdiction, or proposals for laws, relating to liability in tort for injuries inflicted by the use of such vehicles or vessels? If so, please provide a short explanation.*
  ***Comment**: Answers may include the liability of drivers, producers of vehicles and the suppliers of satellite technology.*

I. Liability pursuant the German Road Traffic Act and its recent amendments

As the focus of German legislation and practice with regard to both classical and automated driving is on motor vehicles rather than on vessels, the present paper focusses on vehicles as well. The German Road Traffic Act (RTA; *Straßenverkehrsgesetz*, *StVG*) ensures that both the driver and the so-called keeper (*Halter*) – who is the registered holder of the car who decides on its use and who bears the running expenses, and who will often but not necessarily be its owner at the same time –[1] of a motor vehicle are liable for damages caused by the use of the vehicle.[2] The provisions of the RTA were originally aimed at regulating the use of vehicles that are fully controlled by a human being as driver. The liability of the driver is thus designed for situations in which the driver has full control over the vehicle and therefore may be held liable if due to a negligent use of the vehicle a damage is caused to a third party.[3] In contrast, the liability of the keeper does not require any kind of negligent behaviour.[4] In 2017 the RTA was amended in order to include rules for automated driving (see infra, 2).

1. General rules on liability of drivers and keepers

a. Liability of the driver

The liability of the driver is regulated in Sect. 18 RTA. According to that provision the driver has to compensate any third party for damages and financial losses that were negigently caused by the driver during the use of the vehicle on public roads. There is a legal presumption of negligence,[5] which however leaves the driver the possibility to prove that there was no negligence. The liability is in general limited to EUR 5 Mio. in

[1] *Bundesgerichtshof* (*BGH*) (10 July 2007) in [2007] Neue Juristische Wochenschrift (NJW), 3120 marginal no. 7.

[2] See Sect. 7 para. 1, 18 para. 1 RTA.

[3] See Sect. 18 para. 1 sent. 1 RTA.

[4] Sect. 7 para. 1 RTA.

[5] Sect. 18 para. 1 s. 2 RTA.

case of death or physical injury of one or more victims of the accident, and to EUR 1 Mio. in case of damage to property.[6]

b. Liability of the car keeper

Since the use of motor vehicles on public roads, while it offers the advantage of a high mobility, is a dangerous activity, Sect. 7 RTA states that the keeper of a vehicle is liable for any damage inflicted in relation to its use, regardless of whether or not the keeper was driving the car. Hence, Sect. 7 RTA disposes a strict liability of the keeper since liability does not require any kind of negligent action of the keeper or the driver.[7] In contrast to the driver, the keeper is not given any option to exculpate himself. This is to ensure that in case where the driver succeeds in exculpating himself the victim of the accident nevertheless does not go uncompensated. It is only if the accident was caused by an act of God[8] or if the vehicle was driven by an unauthorized person and this was not due to negligent behaviour of the keeper[9], that the keeper may avoid liability. However, similarly to the driver, responsibility is limited in height.

2. Recent changes to the Act with regard to automated driving

As shown, the liability system of the RTA is based on two pillars: First of all, fault-based liability of the driver with a presumption of negligence, and secondly, strict liability of the keeper. The German legislator recently addressed the question whether the use of highly or fully automatized vehicles on public roads requires modifications to this system. In fact on 21 June 2017 a number of new rules addressing this question entered into force, in particular the new Sect. 1a and 1b RTA.

a. New rules for the use of highly or fully automatized vehicles

Sect. 1a RTA states that highly or fully automatized vehicles may be used on public roads under the condition that the automized functions are working properly. The legislator left the abovementioned liability system untouched in its essence.[10] Hence, drivers and keepers of highly or fully automatized vehicles will be held liable for damages the use of a driver assistance system causes, e.g. due to a malfunction, under the conditions mentioned above.

---

[6] Sect. 12 para. 1 nos. 1 and 2 RTA.

[7] Cf. *Bundesgerichtshof* (*BGH*) (26 April 2005) in [2005] Neue Juristische Wochenschrift (NJW), 2081 et seq.

[8] Sect. 7 para. 2 RTA.

[9] Sect. 7 para. 3 RTA.

[10] *Armbrüster*, Automatisiertes Fahren - Paradigmenwechsel im Straßenverkehrsrecht, Zeitschrift für Rechtspolitik (ZRP), 2017, pp. 83 et seq.

b. No admission of fully autonomous cars on public roads

Even after the recent changes to the RTA, the German legal framework does not allow fully autonomous cars access to the use on public roads. "Fully autonomous" in this context means that the car drives by itself without any option for a human being to intervene and take over control during the ride. According to the recently amended Art. 8 para. 5bis of the Vienna Convention on Road Traffic of the United Nations[11], which has been transformed into national law and is thus directly applicable, the driver must at all times be able to control his vehicle and to switch off the automated function. Consequently, for the time being a fully autonomous car that drives all on its own and leaves no possibility for a driver to regain control cannot be admitted on German public roads.

c. Definition of highly of fully automatized vehicles

The newly implemented Sect. 1a RTA does not distinguish between the various stages of automatization of a vehicle. Rather Sect. 1a para. 2 RTA only defines which vehicles are categorized as highly or fully automatized in the sense of the wording of the RTA. According to Sect. 1a para. 2 RTA, vehicles are only highly or fully automatized if they have technical equipment, 1. which can control the respective motor vehicle after activation in order to cope with the driving task, including longitudinal and transverse guidance, 2. which is able to comply with the traffic regulations relating to vehicle guidance during the highly automatic or fully automated vehicle control, 3. which can be manually overridden or deactivated at any time by the vehicle operator, 4. which can detect the necessity of the vehicle's own control by the vehicle driver, 5. which can indicate visually, acoustically, tactilely or otherwise perceptibly to the vehicle operator the requirement of the vehicle control unit with sufficient time before the vehicle control is handed over to the driver; and 6. which refers the driver to a use contrary to the system description.

The car manufacturers are obliged to explicitly confirm the compliance of their vehicles with the above-mentioned requirements in the system description.[12] Furthermore the legislatur has expressly pointed out that the use of one or more driver assistance systems leaves the classification of the person enabling these systems as driver of the

[11] See https://www.unece.org/fileadmin/DAM/trans/conventn/crt1968e.pdf, last checked on 13/9/2017.

[12] Sect. 1a para. 2 sent. 2 RTA.

vehicle unaffected. This is meant to prevent an interpretation of the RTA that would automatically exculpate the person who makes use of the assistance systems from the liability as driver of the vehicle.

d. Liability of driver when using highly or fully automatized vehicles

Additionally the recent amendments of the RTA establish some important obligations of the driver when using driver assistance systems in a highly or fully automatized vehicle. According to Sect. 1b RTA the driver is not allowed to turn his attention completely away from the traffic. This means that he (or she) must not rely entirely on the automated driving system. In case the driver notices or has to notice because of obvious circumstances that the preconditions for the use of the highly or fully automatized mode are no longer met, he is obliged to take back control over the car. The same is true if the vehicle itself advises the driver to switch off the assistance system.[13] Those requirements specify the standard of care when using highly or fully automatized driving systems. They leave the presumption of negligence laid down in Sect. 18 RTA unaffected. This means that if the use of an automated driving system results in any damages caused to third parties, the driver must prove compliance with Sect. 1b RTA in order to avoid liability. Taking into account the fact that the danger automatized cars bring along cannot be fully estimated yet, the legislator decided to double the maximum liability for personal damage from EUR 5 to to 10 Mio.[14]

e. Liability of the keepers of highly or fully automatized vehicles

The RTA does not impose any special obligations on the keeper of the vehicle when he allows third parties to use the highly or fully automatized vehicle. As the general principles of Sect. 7 RTA prevail, the keeper is still responsible for any damage caused by the use of the highly or fully automatized vehicle. That holds true even in cases where the driver is exculpated. This seems reasonable, since the malfunction of a driver assistance system is undoubtedly part of the general danger which the use of vehicles on public roads entails. Sect. 7 RTA aims at protecting accident victims by ensuring that they always can raise claims at least against the keeper of the vehicle, who takes benefit from holding the car and deciding about its use. The victims' need of protection is neither higher or lower in comparison to cases where the damage is caused by the use of a non-automatized vehicle.

II. Liability of the producers of highly or fully automatized vehicles

[13] Sect. 1b para. 2 RTA.

[14] Sect. 12 para. 1

If an accident solely resulted from the malfunction of a driver assistance system the keeper of the car may be able to take recourse against its producer. Currently, there are no specific rules for product liability with regard to highly or fully automatized vehicles. The Product Liability Act (PLA; *Produkthaftungsgesetz*, *ProdHaftG*), by which the EU Product Liability Directive[15] was transformed into German law, states in Sect. 1 para. 1, that when a defective product causes a person's death, bodily injury or health damage, or damage to property, the producer has to compensate the damage. In case of damage to property, however, this only applies if the damage was caused to an item of property different from the defective product itself, and if this other item of property is of a type ordinarily intended and actually disposed for private use or consumption. Similarly to Sect. 7 RTA the liability pursuant to Sect. 1 ProdHaftG is of strict nature, which means that does not require negligence of the producer. Rather the liability is linked to the general dangers that result from putting defective products into circulation. The amount of damages the producer may be held liable for is limited to EUR 85 Mio. in cases of personal injuries. If the damages in total exceed this limit the of each individual will be reduced *pro rata*.

Under certain circumstances however, which have to be proven by the producer, he will escape strict liability. An important case with regard to automated driving is Sect. 1 para. 2 no. 5 PLA. According to this provision, which transposes Art. 7 lit. e of the Product Liability Directive into German law, the liability of a producer is excluded if the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the defect to be discovered (so called development risk defense). Therefore if an automated driving system has been designed according to the state of the art at the time when the product was put into circulation, the producer can avoid any claims of victims of traffic accidents resulting from a malfunction (e.g. sensor defects due to interferences with other signals). In that case the keeper of the car – and in practice his motor liability insurer (see supra, III 1) will not be able to have recourse to the producer.

This finding does not necessarily hold true for other EU member states, since the Product Liability Directive does not fully harmonize product liability.[16] Thus the development risk defense has not been adopted in Finland and Luxembourg, while Spain and France adopted a limited defense clause, whereby the limitation has no impact on the liability concerning highly or fully automatized vehicles.[17]

---

[15] Directive 85/374/EEC.

[16] See Recital 18 Directive 85/374/EEC.

[17] Lovells Study on Product Liability in the European Union: A report for the European Commission, 2003, Appendix 2 (retraceable under http://ec.europa.eu/DocsRoom/documents/7106, last checked on 13/9/2017); Study of *Fondazione Rosselli* for the EU-Commission, *Analysis of the Economic Impact of the*

III. Compulsory Insurance

- *Are there any specific laws already adopted in your jurisdiction, or proposals for laws, relating to compulsory insurance coverage for injuries inflicted by the use of such vehicles or vessels? If so, please provide a short explanation.*
  Comment: *Answers may relate to motor vehicle insurance and product liability insurance.*

1. Motor vehicle Insurance

In accordance with EU directives, German law requires the keeper of a car to obtain liability insurance cover (Sect. 1 Compulsory Insurance Act [CIA, *Pflichtversicherungsgesetz, PflVG*]).[18] This rule applies for highly or fully automatized vehicles as well. It is therefore mandatory to conclude an insurance contract that covers personal injuries as well as property damage resulting from operating the car on public roads. This means essentially cover for the liability according to Sect. 7, 18 RTA which was presented above (supra, I 1; third party liability cover). This is aimed at offering victims of traffic accidents a solid basis for their claims to be compensated by the insurance company, that is generally a potent debtor, independently of the financial situation of the driver or keeper of the car. Since Sect. 7, 18 RTA are applicable to liability of drivers and keepers of highly or fully automated vehicles as well, the obligation to sign corresponding insurance cover addresses them in the same way as is the case with non-automated cars.

The insurance cover has to include damages caused by an unauthorized driver. Furthermore, the CIA establishes minimum standards with regard to the insurance sum and the obligations the insurance contract may contain. Clauses that deviate from the compulsory provisions are void. This minimum obligatory cover is flanked by a direct claim of the victim against the insurer (Sect. 115 Insurance Contract Act, ICA [*Versicherungsvertragsgesetz, VVG*]). As a rule this claim may even be brought forward in cases where the insurer is wholly or partially released from liability vis-à-vis the

---

Development Risk Clause as provided by Directive 85/374/EEC on Liability for Defective Products, p. 27 (retraceable under https://www.biicl.org/files/100_rosselli_report.pdf, last checked on 13/9/2017).

18 See Riedel, *Private Compulsory Long-Term Car Insurance in Germany,* The Geneva Papers on Risk an Insurance, Vol. 28 No. 2 (April 2003), pp. 275 et seq.; with regard to the nature of compulsory insurance coverage in general see F. Greis, *Legal basis of medical malpractice insurance in Germany – compulsory insurance cover*, in: *Law and medicine – Current topics in a German an Italian perspective*, 2017, pp. 265 (269 et seq.).

policyholder, e.g. due to a violation of contractual obligations (Sect. 117 ICA).[19] An exception is made only if the accident was caused intentionally.[20] But even then the victim is not unprotected since Sect. 12 para. 1 s. 1 nbr. 3 CIA grants a claim against a compensation fund which the motor insurance industry has been required to set up for such cases. In practice this system offers accident victims a swift and uncomplicated compensation of their damages.

In contrast, other car related insurance contracts, i.e. property insurance which covers damages suffered by the policyholder himself in case of an accident, are not mandatory under EU or German law. This underlines the fact that the legislatior cares about victim protection but does not intend to impose self-protection via insurance on vehicle keepers. Having said this, it should it be noted that in practice car insurance products are often sold as a package combining third party liability insurance and property insurance in Germany.

2. Product liability Insurance

With regard to product liability neither the EU nor the German legislator requires producers to take insurance against product liability risks. Hence, in cases of wide-spread product defects it is not assured that all damages will be covered by insurance.

IV. Future of motor vehicle insurance

- *How do you envisage the future of personal lines in motor vehicle insurance in the next 5-10 years in your jurisdiction?*
  Comment: *You may wish to comment on the future of motor vehicle insurance and the plans being made by the industry for new products*

There has been a lot of speculation recently about the question whether motor insurance as we know it will persist nonwithstanding the increasing use of digitalization in vehicles. Some authors argue that a massive shift from motor insurance to product liability insurance will take place in the near future given the new risks for producers who put highly or fully automatized cars into circulation.[21]

---

[19] Compare F. Greis, *Legal basis of medical malpractice insurance in Germany – compulsory insurance cover*, in: Law and medicine – Current topics in a German an Italian perspective, 2017, pp. 265 (269 et seq.).

[20] See *Bundesgerichtshof* (*BGH*) (18 December 2012) [VI ZR 55/12], in [2013] Neue Juristische Wochenschrift (NJW), pp. 1163 marginal nos. 15 et seq.

[21] *L. Lutz*, Autonomes Fahren als rechtliche Herausforderung, Neue Juristische Wochenschrift (NJW), 2015, pp. 119 (120).

Although the relevance of product liability insurance might in fact rise, this does however not mean that motor insurance will symmetrically lose importance. There are currently no legislative initiatives in Germany that aim at banning the legal obligation of a car keeper to procure motor liability insurance. With regard to the political goal of accident victim protection the system of compulsory motor insurance that covers the keeper's strict liability seems to be the only option, at least as long as product liability insurance is mandatory and there is no strict product liability and direct claim, which might offer a similarly high level of protection. In addition, while the absolute number of accidents is expected to decrease when automated systems become more widespread, the average damage per incident is likely to rise due to the additional digital features which might be damaged in an accident.[22] Thus there are sound reasons to assume that motor liability insurance will continue to fulfill its funtion as a reliable and well-established concept for an effective protection of accident victims. It is a different matter that driver assistance systems and their quality may significantly influence the premium, and that they might even replace the traditional system of no-claim bonuses.[23]

V. Other technological innovations and their impact on the insurance industry

- *Driverless cars and autonomous vehicles apart, how do you assess the following technological developments that are expected to not only reshape the auto sector but also the insurance industry around it?*

    - *connected cars (i.e., Internet enabled vehicles, (IEV))*
    - *automated driver assistance systems (ADAS)*
    - *car/ride sharing*
    - *alternative fuel vehicles*

  Comment: *answers may include identifying the legal and regulatory regime and provisions in your jurisdiction.*

1. Connected Cars

[22] *Armbrüster*, Automatisiertes Fahren - Paradigmenwechsel im Straßenverkehrsrecht, Zeitschrift für Rechtspolitik (ZRP), 2017, pp. 83 (85); J. Müller, *Wie das autonome Fahren die Kfz-Versicherung verändern wird*, retraceable under https://www.allianzdeutschland.de/wie-das-autonome-fahren-die-kfz-versicherung-veraendern-wird/id_79691618/index (last checked on 13/9/2017).

[23] J. Müller, *Wie das autonome Fahren die Kfz-Versicherung verändern wird*, retraceable under https://www.allianzdeutschland.de/wie-das-autonome-fahren-die-kfz-versicherung-veraendern-wird/id_79691618/index (last checked on 13/9/2017).

Vehicles that communicate with their environment will evidently revolutionize not only the car industry but also the insurance business. For instance, the technology needed to facilitate "car to X" or "car to car" communication is vulnerable to interferences from the outside, be it an intentional cyber attack or a mere interference with other signals that disrupt communication. This is especially dangerous with regard to communication systems that allow automatized steering of the car. Aside from the expectation that judges (or the legislator) will find ways to deal appropriately with such scenarios when it comes to liability,[24] more specific insurance solutions might be desirable, such as specific cyber coverage for automatized cars. Thus the insurance sector may play a key part in establishing minimum security standards of connected cars. However for the time being special regulations concerning connected cars are not in effect in the EU or in Germany.

2. Driver Assistance Systems

Driver assistance systems are an integral part of vehicle automatization. Cars that are partially or fully operated by such systems can be granted admission to be used in public road traffic when meeting the requirements of Sect. 1a para. 2 RTA (see infra, I 2). As mentioned before, while the use of such assistance systems is expected to reduce the absolute number of accidents, the damage resulting from the malfunction of such a system can be high. Insurance companies will thus have to rethink their actuarial calculation, which will most likely affect the premium payable by the keeper of a car using assistance systems. Plus, the number of recourses by motor liability insurance companies to car producers will increase in cases where solely the malfunction of an assistance system caused the insured event.

3. Car/Ride Sharing

Car and ride sharing have been practiced for quite a while now. Those modern concepts of mobility originally created demand for ad hoc insurance, e.g. the driver can choose on the spot to start driving with the basic insurance package or add other elements (insurance on demand). Nowadays however car sharing services usually include sufficient insurance coverage. It seems accurate to assume that the effect of those mobility schemes on the insurance sector will be small. While some mobility services like "Uber" have faced legal challenges before the courts in Germany,[25] special regulations concerning car/ride sharing are not in effect in the EU or in Germany.

[24] In case of a cyber attack it may be discussed whether or not the strict liability of the keeper of a car may be excluded in analogy to Sect. 7 para. 3 RTA.

[25] E.g. Oberverwaltungsgericht Berlin-Brandenburg (10 April 2015) [OVG 1 S 96.14], in [2015] Computer und Recht (CR), pp. 376 et seq.

4. Alternative Fuel Vehicles

Taking into account the proven effects of human-made greenhouse gas emission on climate change, and in the wake of the Diesel scandal, German car producers as well as politicians have recently increased their efforts to replace the use of petrol with alternative fuels. In this context renewable energy sources are in the focus. New technologies support those ambitions. There is a variety of rules regulating the use of alternative fuels. However, for the time being no impact on the insurance sector may be identified, and the regulatory system governing the use of such fuels does not .

B. Cyber Risks

I. Legislation concerning Cyber Risks

- *Identify the concerns have emerged in your jurisdiction as a result of cyber risks. Is there any legislation in place or under consideration that might affect such risks?*
  ***Comment**: possible matters include cyber-terrorism, hacking, computer or software failure and financial fraud.*

The threat of cyber risks has recently moved up high on the political agenda of Governments worldwide. It is widely recognized that a comprehensive cyber security strategy is indispensable to meet the increasing global threats. In Germany, in order to protect the domestic economy various statutory regulations provide an obligation for members of specific business sectors to apply a proper risk management procedure to prevent information security breaches.

1. IT Security Act

With particular focus on the economic dimension of a potential breakdown of certain industrial sectors by massive cyber-attacks, in June 2015 the German legislator enacted the IT Security Act (*IT-Sicherheitsgesetz*)[26], which mainly aims to improve the IT security of companies. In this context, amendments were made to the various existing acts[27].

A main focus is put on protecting critical infrastructure, including energy and water supplies, healthcare systems, information technology and telecommunications, food and

[26] IT Security Act of 17 June 2015 (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*), BGBl. 2015 I Nr. 31.

[27] In particular, BSI Act (*BSIG*), Telecommunication Act (*TKG*), Energy Economic Act (*EnWG*), Atomic Energy Act (*AtG*).

transportation as well as finance and insurance. A potential breakdown or an impairment of supply services in these areas is expected to have dramatic consequences on the economy, the State and society in Germany. The precise scope of application (for services) within these sectors is specified by an ordinance (*KritisV*)[28] issued by the Federal Ministry of the Interior, considering their respective importance and the required supply levels.[29] However microenterprises[30] have been excluded from the scope of its application.

[28] The BSI Kritis ordinance (*BSI KritisV*) uses specific criteria to govern which operators meet the standards of the IT Security Act, cf. BGBl. 2016 I No. 20 p. 958 (including definitions of the sectors of energy, information technology and telecommunications as well as water and food), BGBl. 2017 I No. 40 p. 1903 (including definitions of the sectors of transport and traffic, health, finance and insurance).

[29] Sect. 2 para. 10 sent. 2 in conjunction with sect. 10 para. 1 BSI Act.

[30] A microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 Mio., according to appendix Art. 2 para. 1 Nr. 3 of the EC recommendation No. 2003/361.

a. IT security requirements for critical infrastructures

According to Sect. 8a para. 1 of the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik, BSI*) Act operators of critical infrastructure must provide reasonable organizational and technical precautions to prevent disruption of the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes. Such statutory provisions do not and cannot provide sufficiently detailed guidelines on the preventive technical security measures that have to be implemented; the provisions rather refer to the current state of the art. Organizational and technical precautions should therefore be considered as appropriate if the required effort is not disproportionate to the negative consequences of a potential breakdown of the respective critical infrastructure. According to the wording of Sect. 8a para. 1 sent. 2 BSI Act, providers of critical infrastructures "shall" comply with the current state of the art. The choice of the word "shall" implies that deviations are possible in justified exceptional cases. This takes account of the fact that providers of critical infrastructures are sometimes prevented from taking measures that are considered as the current state of the art from a security point of view. This applies, for example, in the case of the installation of security updates for operating systems with regard to the uncertainty of their impact to business processes.[31]

Beyond that, according to Sect. 8a para. 2 BSI Act, the providers of critical infrastructures and their industry associations are authorized to set out detailed requirements and guidelines regarding IT security which will be approved by the BSI after consultation with other authorities. In this respect, members of critical infrastructures are obliged to prove compliance with the above-mentioned security requirements periodically.[32] Proof can be supplied by recently undertaken security audits, recurring inspections or certifications.[33] In case of detection of security lacks, the BSI is empowered to order their clearance in accordance with the respective authorities. Further control mechanisms have also been implemented to ensure the obligation to establish appropriate security standards.[34] Non-compliance with the rules on IT security requirements is punishable with fines up to EUR 100.000.[35]

---

[31] G. Spindler, *IT-Sicherheitsgesetz und zivilrechtliche Haftung*, Computer und Recht (CR) 2016, pp. 297 (299); see the official justification of the German Federal Parliament, BT-Drs. 18/5121, p. 15.

[32] Sect. 8a para. 3 BSI Act.

[33] See the guidance for the proof of compliance with the requirements set down in Sect. 8a para. 3 IT Security Act : https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/IT-SiG/Was_tun/Nachweise/Orientierungshilfe/Orientierungshilfe.html;jsessionid=0C2BB5D35D181BF22EADD9DA4FA42764.1_cid369?nn=8391980 (last checked on 13/9/2017).

[34] Sect. 8a para. 4, 5 BSI Act.

[35] Sect. 14 para. 2 BSI Act.

b. Obligation to notify security breaches

Apart from the development of a high IT security level, members of critical infrastructures are obliged to notify security breaches to the BSI (Sect. 8b para. 4 BSI Act). The latter obligation applies if a member of a critical infrastructure recognizes a significant disruption of the availability, integrity, authenticity or confidentiality of their information technology system that could cause or already has caused a breakdown or an impairment of his respective critical infrastructure.[36] The notification should be made by the company's notified contact office[37], which is responsible for procuring administrative support to the BSI. During the legislative procedure, the industry persistently demanded for the opportunity of pseudonymous notification in order to protect the company's reputation.[38] However, Sect. 8b para. 4 sent. 3 BSI Act provides for this option solely in cases where critical infrastructures are not charged with an impairment of functionality by a security incident. The notification obligation of telecommunication providers is even stricter since they do not have any right to report a security incident anonymously. In addition, following the amendment of the Telecommunications Act (*Telekommunikationsgesetz, TKG*)[39], telecommunication providers now are obliged to inform users even in cases of suspected impairments of user systems, e.g. potential risks of botnets.[40]

c. Federal Office for Information Security (BSI)

In order to meet legislative targets, the IT Security Act strengthens the position of the BSI, particularly by extending duties and powers as stated above. Sect. 8b BSI Act clarifies that the BSI is the central reporting office for members of critical infrastructures in the field of information technology. For this purpose, the BSI is supposed to collect, inter alia, all relevant information concerning the prevention of dangers regarding the IT

---

[36] Spindler, *IT-Sicherheitsgesetz und zivilrechtliche Haftung*, Computer und Recht (CR) 2016, pp. 297 (300); see also the official justification by the *German Federal Parliament*, BT-Drs. 18/4096, p. 27 f.

[37] See the obligation to notify a contact office in Sect. 8b para. 3 IT Security Act.

[38] See P. Bräutigam/S. Wilmer, *Big brother is watching you? – Meldepflichten im geplanten IT-Sicherheitsgesetz*, Zeitschrift für Rechtspolitik (ZRP) 2015, pp. 38 (41); see also the final statement of the Confederation of German Industry (*BDI*) concerning the IT Security Act of 16 April 2015, p. 8 f.
< https://www.bundestag.de/blob/370300/8c907d1750439b380668c12f98a80d1b/18-4-284-e-data.pdf >.

[39] Sect. 109 para. 5 Telecommunication Act.

[40] Spindler, *IT-Sicherheitsgesetz und zivilrechtliche Haftung*, Computer und Recht (CR) 2016, pp. 297 (301).

security of critical infrastructures, detected security lacks as well as malware, and to transfer this knowledge to the various recipients and the respective authorities.[41] In order to fulfill its duties, the BSI is also authorized to carry out compliance checks on products in terms of their safety.[42] In the event of security breakdowns, the BSI is even entitled to force the producer of the respective IT systems to corporate if necessary.[43] The legislative objective was to create a stronger obligation on software manufacturers to provide security patches.[44] It is also worth mentioning that the BSI is obliged to draw up an annual report on current threats in the field of information technology. This serves both for public information and also in order to achieve a higher level of security.[45]

d. Sector-specific provisions

In addition to the statutory framework for the protection of critical infrastructures from risks which may arise in the event of cyber attacks, the German legislator and the competent administrative authorities have enacted further specific rules on cyber security in different acts.[46] While a complete overview would go beyond the scope of this report, individual sectors have already been mentioned, such as telecommunication providers. Another notable sector concerns the area of telemedia providers. According to Sect. 13 para. 7 Telemedia Act (*Telemediengesetz, TMG*), commercial telemedia providers have to provide technical and organizational measures to prevent unauthorized access as well as breaches of personal data and disruptions to technical systems wherever technically possible and economically reasonable. This is of particular importance because of the broad term of telemedia providers.[47] Public WLAN hotspots in the hospitality sector, for instance, are sufficient to fit in with the term of commercial telemedia providers. The aim of the provision is to prevent the danger of unperceived transmission of malware merely by the call of single web pages (so called "*drive-by downloads*").[48] Infringements against these security measures may incur fines up to EUR 50.000.[49]

---

[41] Sect. 8b para. 2 Nr. 1 BSI Act.

[42] Sect. 7a BSI Act.

[43] Sect. 8b para. 6 BSI Act.

[44] Cf. the official justification of the German Federal Parliament, BT-Drs. 18/5121, p. 16.

[45] See the latest annual report of the Federal Office for Information Security, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5 (last checked on 13/9/2017).

[46] See Sect. 109 Telecommunication Act (*TKG*), sect. 13 Telemedia Act (*TMG*), Sect. 25a Banking Act (*KWG*), Sect. 33 Securities Trading Act (*WpHG*), Sect. 44 Atomic Energy Act (*AtomG*), Sect. 11 Energy Economic Act (*EnWG*).

[47] Sect. 2 Nr. 1 Telemedia Act.

[48] See the official justification of the German Federal Parliament, BT-Drs. 18/4096, p. 34.

[49] Sect. 16 para. 2 no. 3 in conjunction with sect. 16 para. 3 Telemedia Act.

2. NIS Directive

In July 2016, the EU Directive on Security of Network and Information Systems (NIS Directive) passed the European Parliament. This directive has to be implemented into national laws by EU member states by April 2018. As the obligations laid down in the German IT Security Act and the NIS Directive are widely identical (the former is actually a premature implementation of the latter), major amendments to the German IT Security Act are not to be expected.[50] However, in several aspects, changes to the present German law have been required.[51] In particular, the scope of operators of critical infrastructure concerning the IT Security Act does not entirely mirror the respective requirements of the NIS Directive.[52] One substantial amendment is the extension for providers of digital services as defined in Sect. 2 para. 11 BSI Act. These particularly include online marketplaces, online research engines as well as cloud-computing services. Similarly to the provisions that apply to critical infrastructures, specific requirements concerning preventive measures are provided in Sect. 8c BSI Act.

3. Data Protection Law

EU and German Data Protection law also contains IT security requirements to protect personal data, however not with a particular focus on cyber threats. Part B Sect. 32 to 34 EU General Data Protection Regulation (*Datenschutzgrundverordnung, DSGVO*) draws up provisions regarding security of personal data. Even though the requested measures are not defined in detail but rather depend on criteria of reasonability, the regulation does mention some specific actions, e.g. the encryption of personal data, the ability of data recovery in cases of technical incidents or proof of efficacy concerning security measures. The notification of a personal data breach to the supervisory authority unless the fact that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons is of particular importance with regard to cyber risks.[53] If however the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the company responsible for data processing shall communicate the personal data breach also to the affected parties without undue delay.

---

[50] https://deutschland.taylorwessing.com/de/the-german-it-security-law-fact-sheet (last checked on 13/9/2017).

[51] *Umsetzungsgesetz für die NIS-Richtlinie vom 23. Juni 2017*, BGBl. I p. 1885.

[52] https://deutschland.taylorwessing.com/de/the-german-it-security-law-fact-sheet (last checked on 13/9/2017).

[53] Differently to Sect. 42a Federal Data Protecion Act (*Bundesdatenschutzgesetz*) which requires an anticipated severe impairment for the rights or legitimate interests of the affected person.

The latter obligation may apply in cases of unauthorized perusal of confidential data (e.g. bank details). Corporations that process personal data must also be aware of the high level of potential fines in cases of non-compliance with data protection provisions.[54]

4. Product liability of software manufacturers

In response to the impact of cyber risks, the issue of liability of software manufacturers is largely recognized in the political debate. In Germany, the political debate has been encouraged especially by a serious cyber attack in November 2016, that hit many router devices provided by Deutsche Telekom. There are calls for an obligation of software manufacturers to monitor their products after they have been placed on the market, and to force the manufacturers to supply a regular patch management.[55] Appropriately, the European Commission has launched a consultation on the effectiveness of the Product Liability Directive 85/374/EWG in terms of damages caused by new technology developments (e.g. autonomous driving, Internet of Things, non-embedded software).[56] Based on the legal discussion in Germany, uncertainties are especially recognized in regards to the question whether non-embedded software falls within the term of "product" according to Art. 2 Product Liability Directive.[57]

II. Reactions to cyber risks

- *How has the insurance industry responded to cyber risks? In particular:*
  - *(a) do property policies cover losses from cyber risks, or is special insurance required?*
  - *(b) is insurance and reinsurance readily available?*
  - *(c) are there any special restrictions imposed on cyber risks, e.g. event limits or deductibles?*

1. Cyber exposure in traditional lines of insurance

[54] See Sect. 83 EU General Data Protection Regulation.

[55] Cf. GDV position paper relating to smart home products, retraceable under http://www.gdv.de/wp-content/uploads/2017/06/GDV_Positionspapier_Smart_Home_IoT_final_.pdf (last checked on 13/9/2017).

[56] http://ec.europa.eu/growth/tools-databases/newsroom/cf/itemdetail.cfm?item_id=9048&lang=de (last checked on 13/9/2017).

[57] *G.Wagner*, in : *Münchener Kommentar zum BGB* (7th ed. 2017), § 2 ProdHaftG no. 17 ff.

Many damages relating to cyber risks are already covered by standard indemnity and property insurance policies. The cyber exposure in insurance policies that have not excluded damages resulting from cyber risks is often referred to as the "silent cyber risk". In order to get an idea of what cyber exposure really means, first of all it is necessary to describe the scope of the term of "cyber risk". Cyber risks can be both cyber related losses resulting from malicious cyber attacks, such as infecting an IT system with malicious code (e.g. ransomware), and non-malicious acts like loss of data caused by negligent behavior or data breaches in cases of accidental release of personal/confidential data.[58]

Against this background, it is more precise to use the term of information security breach. This establishes a connection to potential damages, while the term of cyber risk rather could be seen as a peril resulting from the transformation of processes, products as well as services through an intensified use of modern information and communication systems. The term of information security breach is used to describe an impairment of the availability, integrity and confidentiality of data or of information processing systems. A potential damage that may occur in that case is e.g. a business interruption caused by the non-availability of business data or processes. The essential question is therefore whether damages caused by information security breaches are covered in traditional lines of insurances, such as the property and technical insurances as well as liability and fidelity insurances.

a. Property Insurance

As the name implies, property as well as technical insurance policies basically cover damages to property. So far, as there has been no general exclusion of damages caused by information security breaches in the event of cyber attacks, property as well as technical insurance cover the related losses. However, unless insurance policies do not provide specific conditions, the occurrence of a material damage is necessary for a claim of insurance benefits.[59] A prominent example is the malfunction or overheating of technical machines of a major steel plant triggered by a takeover of control devices by hackers. Certainly, special situations may arise if the insurance coverage is restricted to damages caused by named perils, e.g. explosion. In this case, the material damages has to be caused by any such event, although the coverage is not excluded if an information security breach has occurred immediately prior to an insured risk. However, usually losses from cyber risks occur independently of damages to property. In such cases, there

[58] https://www.lexology.com/library/detail.aspx?g=54176adb-7f80-43cf-8552-a5a63e018c72 (last checked on 13/9/2017).

[59] Erichsen, *Cyber-Risiken und Cyber-Versicherung: Abgrenzung und/oder Ergänzung zu anderen Versicherungssparten*, Corporate Compliance (CCZ) 2015, pp. 247 (249).

is basically no insurance coverage provided by traditional property as well as technical insurances.

In addition, it should be noted that the International Association of Engineering Insurers (IMIA) has developed a risk exclusion regarding damages directly or indirectly caused by cyber incidents.[60] At the same time, the IMIA developed particular terms for a subsequent reinclusion. The idea of the IMIA advanced cyber exclusion is to offer underwriters an overview of the wide range of cyber perils. This facilitates a consideration within the risk assessment and the premium calculation.

b. Third-party Liability Insurance

A third party liability insurance provides coverage if the policyholder is held liable by a third party for a loss occurrence that has resulted in personal injury, property damage or pure financial losses arising therefrom. Basically, damages resulting from information security breaches are covered if they fall within the insured risk and are not excluded. Claims for damages resulting from the exchange, transmission or provision of electronic data are mainly covered on the basis of the supplementary conditions for the use of IT technologies relating to the general business liability insurance.[61] Specific types of liability insurance are extended to claims for compensation of strictly pecuniary losses. Since they do not exclude claims for damages resulting from an information security breach – which is not the case at the present time in Germany –, insurance cover is provided under the terms of these policies.

One example is the directors & officers liability insurance.[62] If negligent disregard of IT security measures become apparent during a cyber attack and if the companies board member is responsible for adhering to them, a directors and officers liability insurance covers the liability of managing and supervisory boards for financial damages to the company (internal liability). Furthermore, various types of professional liability insurances are extended to third-party claims for compensation of strictly pecuniary losses (e.g. lawyers, notaries, insurance intermediaries, etc.), which means that cyber risks are also extensively covered in these sectors. Of course, with respect to compulsory

[60] Cf. the endorsement regarding the IMIA advanced cyber exclusion https://www.imia.com/wp-content/uploads/2017/03/Endorsement-IMIA-Advanced-Cyber-Exclusion-2017-final-15-03-2017.pdf (last checked on 13/9/2017).

[61] Cf. the general terms and condition provided by the German Insurance Association (GDV), http://www.gdv.de/wp-content/uploads/2015/03/14-Nutzer-Internet-Technologien-Jan2015.pdf (last checked on 13/9/2017).

[62] Cf. the general terms and condition provided by the German Insurance Association (GDV), http://www.gdv.de/wp-content/uploads/2016/02/AVB_DandO_Feb2016.pdf.pdf (last checked on 13/9/2017).

insurance it has to be considered that insurance sums which are primarily reserved for damages caused by genuine professional activities could be exhausted by indemnifying losses arising from cyber-attacks.

c. Fidelity insurance

Cyber risks have evolved beyond traditional hacking to include sophisticated social engineering methods that rely on undeliberate representatives to effectuate fraud.[63] Social engineering is a method of gathering information by manipulation. In the past years, major companies have been victims of multi-million dollar fraud schemes concerning financial transactions that were perpetrated online using social engineering.[64] Those risks as well as financial losses caused by deliberative fraud of company representatives are covered by specific fidelity and fraud insurance policies.

2. Specific cyber insurance coverage concepts

Today, a modern business's most valuable property frequently exists in cyberspace without physical form.[65] Therefore the perils that these businesses face are not the traditional perils of fires, floods, and other physical forces.[66] The existing insurance concepts do not appear sufficient to handle these new perils because of the merely fragmentary coverage for pecuniary losses, the occurrence of damages irrespective to the fact that no substantial damage to property is ascertainable as well as the need for assistance services in the event of cyber attacks, which help to mitigate the loss or damage that occurred.

Against this background, the German Insurance Industry Association (*Gesamtverband der deutschen Versicherungswirtschaft, GDV*) has recently developed specific model terms and conditions of cyber risk insurance,[67] which have been published as noncommittal recommendations for the industry. This cyber risk insurance covers financial losses caused by an information security breach. Designed as a cross-segment multi-line-policy cyber risk insurance contains several elements from traditional lines of insurance such as

[63] Cf. *Crowe/Farina/Hanson/Thomson*, Beyond Hacking : Coverage for social engineering scams and schemes, 2016, p. 2.

[64] Cf. *Crowe/Farina/Hanson/Thomson*, Beyond Hacking : Coverage for social engineering scams and schemes, 2016, p. 2.

[65] *Hazel Glen Beh*, Physical losses in cyberspace, Connecticut Insurance Law Journal, Vol. 8, 2001, p. 55 f.

[66] *Hazel Glen Beh*, Physical losses in cyberspace, Connecticut Insurance Law Journal, Vol. 8, 2001, p. 55 f.

[67] Cf. the general terms and conditions of cyber risk insurance (T&Cs Cyber) provided by the GDV, http://www.gdv.de/wp-content/uploads/2017/04/AVB_Cyber_April_2017.pdf.

the liability, property and technical insurances. The concept adopts a modular structure and consists of four components: a basic component (A1), a component for reimbursable expenses (A2), a component for insurance cover against third-party liability (A3), as well as against first-party damage (A4). The basic component draws up general provisions, which apply to all modules (e.g. the subject-matter of the insurance, the definition of the insured event, general exclusions, the policyholder's obligations, etc.). The component for reimbursable expenses includes, inter alia, costs for forensic investigations to determine an insured security breach, expenses related to crisis management in the purpose of restoration of public reputation, costs for notification in the event of data breach and finally costs for call management. In addition, measures to prevent a forthcoming security breach are also covered up to an agreed sublimit. Being limited to pure pecuniary losses, a cyber insurance also covers third party damages, for example if a customer or a business partner submits a claim against the policyholder on the basis of a breach of privacy. Finally, the policy concept provides insurance cover against business losses (first-party damage), such as a damage caused as a result of an interruption to business operations. In case of loss of data or data alteration caused by an information security breach, expenses for data recovery are covered too.

3. Availability of Insurance / Reinsurance

In principle, cyber insurance as well as reinsurance is currently available in Germany. Supply even has so far exceeded demand, as – especially in the field of small and medium-sized enterprises – business operators have only recently become more and more aware of their cyber risk exposure and of both the opportunity and the necessity to obtain adequate insurance coverage. The expected rapid growth will be likely to reduce the present difficulties in risk modelling, which are due to the absence of appropriate claims data. Particular problems are caused by the unpredictable accumulation risks in the event of cyber attacks. An example is the scenario of a breakdown of a cloud service provider. In such a case, all cloud users are affected by one single loss event. The general terms and conditions of cyber risk insurance provided by the GDV respond to this challenge by clarifying that no insurance cover is being provided for any loss resulting from failure, interruption or malfunctioning of external service providers.[68] Another example for an accumulation risk scenario is a self-reproducing computer virus. The latter includes ransomware, such as „Locky" or „WannaCry".

4. Special restrictions imposed on cyber risk

The insurance of ransom demands is still subject to supervisory restrictions. According to an announcement of the Federal Supervisory Office (*Bundesanstalt für*

[68] Cf. Sect. 2.2 para. 2 T&Cs Cyber.

Finanzdienstleistungsaufsicht, BaFin) for Insurance from 1998[69] the insurance of ransom demands, inter alia, must not be offered in combination with other insurance products. Since these restrictions seem to be no longer appropriate particularly with regard to the insurance of cyber risks, there is an assumption that the supervisory authority will revise the administrative practice in the near future.

Apart from this, there are some special requirements concerning insurance licensing and financial reporting following from the multi-line character of the cyber risk insurance. Authorization as well as financial reporting in each case has to be made for a particular class of direct insurance. Since cyber risk insurance does not become a separate class of direct insurance, insurance companies have to seek authorization as well as perform financial reporting for any class that is affected by the general terms and conditions of cyber risk insurance. Finally, even if there is no explicit legislation or jurisdiction, it is noteworthy that the legal admissibility of insurance cover for financial penalties is being discussed controversially in Germany.[70] In this context, it is often assumed that the insurance of financial penalties may create negative incentives and is therefore contrary to the preventative purpose of the respective sanctions.[71]

C. New technologies and the insurance process

- *To what extent have the availability of new technologies affected the way in which insurance policies are placed? In particular:*

I. Effect on the traditional use of agents and brokers

1. General Remarks

New technologies have already begun to disrupt the traditional distribution of insurance products by agents and brokers. A vast variety of new competitors, mainly start-ups (so called FinTechs or, more specifically, InsurTechs), have entered the distribution sector relying on new technologies, namely comparison portals, online insurers, broker apps for smartphones, etc. These newcomers have induced traditional distributors to rethink their own means of distribution and to adopt new technology standards. This is especially because via such means of distribution the insurance industry could easily

[69] R 3/98.

[70] *P. Ruttmann*, in: *Die Versicherbarkeit von Geldstrafen, Geldbußen, Strafschadensersatz und Regressansprüchen in der D&O-Versicherung* (1st ed. 2014), p. 85 ff.; *T. Gädtke*, in: E. Bruck/H. Möller, *VVG*, *Band 4, Haftpflichtversicherung, §§ 100-124* (9th ed. 2014), AVB-AVG 2011/2013, no. 5 recital 104 ff.

[71] Ch. Armbrüster/D. Schilbach, *Nichtigkeit von VersVerträgen wegen Verbots- oder Sittenverstoßes*, Recht und Schaden (r+s) 2016, pp. 109 (112 et seq.).

assess and mobilize new costumer groups, especially youngsters, who have a genuine affinity towards digital product supply, and who would not easily be motivated to use traditional lines of distribution, such as agencies.

The effects and influences of new technologies on the traditional use of agents and brokers are immense and of a vast variety. The following remarks address selected issues that are of particular importance to the distribution sector.

2. Distributor or mere "tip provider"?

Distributors of insurance products (agents and brokers[72]) have to seek permission of the local Chamber of Industry and Commerce before they start offering and distributing insurance products in Germany.[73] Carrying out such activity without formal admission can be fined up to EUR 5.000.[74] In contrast, a mere "tip" to the insurance company that a certain individual might be interested in concluding a contract, or the providing of contact data of a certain insurance company or a broker, do not qualify as distribution in the legal sense. Hence, such activities may be conducted without a formal concession by the competent authorities.

Therefore, it is necessary to distinguish between mere "tip providers" and distributors, especially when online distribution is at stake, since the variety of different business schemes and models is considerably high. The German Federal Court (*Bundesgerichtshof, BGH*)[75] ruled that in order to achieve a high level of consumer protection the term "distribution" must not be interpreted narrowly. Nevertheless, the classification of an activity as "insurance distribution" requires at least the advice to conclude a specific contract. Accordingly, providing general information on certain insurance products does not constitute an activity of distribution and may therefore be carried out without concession. The *BGH* ruling particularly concerns online distribution, and it offers guidelines for a variety of business models that deal with or are related to distance selling of insurance contracts.

3. Pre-Contractual duty to advise insurance seekers

[72] See. Sect. 59 para. 1 VVG.

[73] See. Sect. 34d para. 1 *Gewerbeordnung, GewO*.

[74] Sect. 144 para. 4 GewO.

[75] 28 November 2013 [I ZR 7/13] in [2009] Multimedia und Recht (MMR), pp. 466 marginal no. 21.

When distributing insurance products analogously distributors have a legal duty to advise the seeker of insurance if and what kind of policy to sign.[76] During the revision of the German Insurance Contract Act (*Versicherungsvertragsgesetz, VVG*) in 2008, the German legislator thought that distributors relying on distance selling by means of the internet were disadvantaged when it comes to rendering qualified advice to the costumers with regard to their product choice. The prevailing opinion was that – given the technological possibilities at the time – online insurers were unable to consult and advise insurance seekers in the way the law obliges distributors and insurers to do.[77] Therefore, online insurers were exempt from the pre-contractual duty to advise customers on the insurance product that meets their needs best. Rather inconsistently, this statutory exception did solely apply to online insurers and not to online brokers, raising the question if such a differentiation was justified.[78] However, just recently, in the course of transforming the EU Insurance Distribution Directive[79] into national German law[80] the aforementioned exception was abolished on the basis of the finding that technological progress has now enabled online insurers to pre-contractually advise their customers properly.[81] This change will come into effect on 23 February 2018. From that date on, online brokers and insurers have to pre-contractually advise clients to the same extent their colleagues who operate in the analogous mode are obliged to. Given the numerous digital tools provided through technological progress facilitating identification and assessment of individual risks (e.g. question tools with explanation boxes, instant chat tools, video chats, broker apps, etc.) the abolishment of the exception seems more than appropriate.

4. Broker Apps

Broker apps, which have flooded the German distribution sector in recent years, have triggered a lot of controversy and brought up a number of legal issues.[82] In general, those apps are frequently structured as a kind of "digital insurance folder", which allows

[76] Sect. 6, 61 VVG.

[77] See Sect. 6, 61 VVG.

[78] For an overview see Ch. Armbrüster, in: *Münchener Kommentar zum VVG* (2nd ed. 2016), § 6 VVG marginal no. 362.

[79] Directive (EU) 2016/97 (hereafter referred to as IDD).

[80] See *Gesetz zur Umsetzung der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb und zur Änderung anderer Gesetze*, BGBl. 2017 I p. 2789.

[81] Cf. Ch. Armbrüster, *Aktuelle Rechtsfragen der Beratungspflichten von Versicherern und Vermittlern*, pp. 17 et seq.

[82] Ch. Armbrüster/S. Pfeiffer, *Rechtsfragen rund um Versicherungs-Apps*, Zeitschrift für Versicherungswesen (ZfV), 2016, pp. 277 et seq.

not only to conclude new contracts through the app, but also to digitalize existing policies. Therefore, app operators have concluded framework contracts with insurance companies that provide a digitalized copy of the customers policy when having been given a brokerage mandate by the user.

This business model therefore significantly depends on the IT infrastructure of the individual insurance company since it has to provide a digital interface in order to exchange data with the operator of the broker app. Such business models have a high market potential as long as they comply with existing rules and provisions. They might even fundamentally reshape the view on insurance selling.

Broker apps have brought up specific transparency issues. Since those apps work on the basis of a broker mandate customers have to give such a mandate before using the app. Given the fact that in practice for the time being only a few of the broker apps available at the market explain the users the legal consequences of such a mandate, and especially the fact that any existing mandates with another broker will be cancelled, traditional distributors have criticised this business model. In some cases, broker apps do not even properly offer the legally required[83] information about their status at all.

Another example for the ongoing discussion in Germany is offered by contract clauses waiving liability for the loss of policy documents. Since such apps were often commercially marketed as instruments that provide for the entire policy management, those waivers have risen concerns about their compliance with statutory law.[84]

Eventually, a key issue with broker apps is the proper transmission of information to the costumers.[85]

II. Impact of Data on the underwriting process

Big data models and analysis methods, as well as new data sources, have enabled insurers and distributors to gather information concerning the individual risk on a large scale. They therefore play a key role in risk assessment. The collection of huge amounts of data, especially from public sources, and the aggregation and interlinking of those data, have facilitated the calculation of insurance products noticeably. An example is

[83] Sect. 11 *Versicherungsvermittlerverordnung, VersVermV.*

[84] Ch. Armbrüster/S. Pfeiffer, *Rechtsfragen rund um Versicherungs-Apps*, Zeitschrift für Versicherungswesen (ZfV), 2016, p. 277 (279).

[85] For a closer examination of that problem see infra, sub III.

offered by telematics-based tariffs in the motor insurance sector, which rely on the constant gathering of data about the driving behaviour.[86]

However, there are comprehensive legal requirements that must be met when collecting, assessing and interlinking data on such a scale for the purpose of pre-contractual risk assessment. The following remarks address the key issues of data protection law in Germany and in Europe with regard to big data analysis methods.

Basically, any processing of personal data[87] needs to be justified either by consent or by statutory provision. Otherwise the data processing is unlawful and can be severely fined with up to EUR 20 Mio. or 4% of the total worldwide annual turnover of the preceding financial year, depending on which amount is higher.[88]

Without consent of the data subject, the processing of ordinary personal data is lawful if it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.[89] The pre-contractual risk assessment is undoubtedly a prerequisite for the conclusion of an insurance contract. Hence, general data processing in that phase is legally allowed, even without consent.

Special provisions apply to so-called special categories of data. If the personal data processed are classified as such special categories of personal data (such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation),[90] the permissiveness of processing such data for the purpose of risk assessment – at least in the ordinary course of events – depends on the consent of the data subject (applicant).

---

[86] For an overview in respect of the legal problems such policies entail see D. Klimke, *Telematik-Tarife in der Kfz-Versicherung*, Recht und Schaden (r+s) 2015, pp. 217 et seq.; Ch. Armbrüster/F. Greis, *Telematik in der Kfz-Versicherung aus rechtlicher Sicht*, Zeitschrift für Versicherungswesen (ZfV) 2015, pp. 457 et seq.

[87] Personal data is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art. 4 para. 1 GDPR).

[88] Art. 83 para. 5 GDPR.

[89] Art. 6 para. 1 lit. b GDPR.

[90] Art. 9 GDPR.

Furthermore, data protection law limits big data analysis methods and the required gathering of large amounts of data by stating that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (principle of data minimization).[91] The gathering of enormous amounts of personal data just for the purpose of accidentally finding links between them is therefore forbidden under EU and German data protection law.

In addition, even when big data analysis methods comply with the principle of data minimization, the aggregation of data for the purposes of profiling is further limited and restricted by Art. 22 of the EU General Data Protection Regulation (*GDPR*)[92]. For the purposes of the GDRP profiling is defined as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.[93] The regulation grants the data subject the right to not be subject to (contractual) decisions of the controller[94] which are based solely on automated processing. An exception is made in Art. 22 para. 2 lit. a GDPR for cases where the decision is necessary for entering into or performance of a contract between the data subject and the controller meaning that even profiling is allowed as long as and to the extent automated decisions on the basis of the profiling results are necessary for contract conclusion. In case of a dispute the controller is obliged to demonstrate this necessity. These provisions are flanked by procedural requirements that aim at securing compliance with Art. 22 GDPR.[95]

Finally an important development consists in the use of big data in order to improve risk assessment with regard to non-personal data that are not subject to data protection law. For instance the predictability e.g. of natural catastrophes or of the economic consequences of supply chain interruptions may be improved, and risk-adequate premiums be calculated more precisely by collecting and evaluating such non-personal data.

III. Impact on the means of providing information

It is generally acknowledged that new technologies have considerably affected the way distributors and insurers provide information to their customers in Germany. This is

[91] Art. 5 para. 1 lit. c GDPR.
[92] Regulation (EU) 2016/679.
[93] Art. 4 para. 4 GDPR.
[94] Art. 4 para. 7 GDPR.
[95] See Art. 22 para. 3 GDPR.

basically due to the fact that the use of digital technology is cost efficient (or at least more efficient than providing printed information). Since insurers are legally obliged to not only provide the terms and conditions of the policy, but also a so-called product information document as well as the documentation of given advice[96] prior to the conclusion of the contract it is attractive for insurance companies and mediators to provide any such information through a digital channel.[97]

Generally, the German law does not prohibit the transmission of pre-contractual information via the internet. The only requirement that must be met is that all pre-contractual information has to be communicated to the customer on a durable medium.[98] A durable medium is defined as a medium that enables the recipient to retain or store an information included on the medium that is addressed to him personally such that it is accessible to him for a period of time adequate to its purpose, and that allows the unchanged reproduction of such declaration.[99] This means that the mere presentation of the pre-contractual information on a display is not sufficient to meet these requirements.

Hence, the discussion focuses mainly on whether or not so-called sophisticated websites can be categorized as durable mediums given that legal definition.[100] Generally, the term of sophisticated website refers to two different website designs:[101] At first, it is possible to require the applicant to download the pre-contractual information before transmitting his contractual acceptance to the insurer by blocking the further proceedings as long as such a download has not taken place. If the applicant initiates and completes the download, the information – then stored on the hard drive of his terminal device – has been communicated according to the statutory requirements.[102]

---

[96] Sect. 6 para. 2 sent. 1 VVG for insurers and Sect. 62 para. 1 VVG.

[97] See Sect. 7 VVG.

[98] See. Sect. 7 para. 1 sent. 1, 61 para. 1 VVG and Art. 25 IDD.

[99] Sect. 126b *Bürgerliches Gesetzbuch, BGB.*

[100] See Ch. Armbrüster, *Der Abschluss von Versicherungsverträgen über das Internet*, Recht und Schaden (r+s) 2017, pp. 51 (62).

[101] According to the distinction established by the ESME's Report on Durable Medium: Distance Marketing Directive and Markets in Financial Instruments Directive, p. 8, retraceable under http://docplayer.net/11387476-Esme-s-report-on-durable-medium-distance-marketing-directive-and-markets-in-financial-instruments-directive.html (last checked on 13/9/2017); compare the ruling of the EFTA Court of Justice (27 January 2010) [E-4/09], in (2010) Versicherungsrecht (VersR), pp. 793 et seq.

[102] Pars pro toto P. Reiff, *Zu den Anforderungen an die Webseite eines Vermittlers als dauerhafter Datenträger*, Versicherungsrecht (VersR) 2010, pp. 797 (798); P. Reiff, *Anmerkung zum Urteil des BGH vom 29.04.2010 (I ZR 66/08, VersR 2011, 269) – Zum Beginn der Widerrufsfrist bei allein durch Abrufbarkeit der dem Verbraucher zu erteilenden*

However, such a website design might still entail difficulties when it is controversial whether the download was in fact carried out successfully.[103] Hence, insurance companies have started to create a personalized storage spaces for applicants, which are located on their servers, where the insurer stores the pre-contractual information and additionally informs the applicant that he can download the files by accessing the server via his personal profile (usually protected by username and password). This option aims at avoiding any controversy about downloads.[104] However it is not beyond doubt if such a private storage on servers controlled by the insurer qualifies as a durable medium. A recent ruling of the European Court of Justice (ECJ)[105] may lead to the assumption that such website designs are acceptable. Nevertheless, this ruling is based on the inaccurate factual assumption that the data stored on the insurer's servers on behalf of the applicant cannot be changed once they are stored. As long as the insurer controls the server this – at least factually – includes control of the information stored on that server, which might at least theoretically be modified (e.g. by exchanging General Contract Terms without the knowledge or consent of the policyholder). Therefore, the discussion has not yet terminated. Using such website designs thus still entails a certain legal risk.

IV. Genetic testing and insurance

- *To what extent is genetic testing regarded as important by life and accident insurers? Is there any legislation in place or in contemplation restricting requests for genetic information, and are there any relevant rules on privacy that preclude its disclosure?*

Taking into account the importance of pre-contractual risk assessment, the economic significance of information about an applicant's genetic disposition is evident, especially with regard to life and health care insurance.[106] A genetic precondition might enhance the personal risk of the applicant to get a serious medical condition and thus point to a risk that may be far higher than average.

Informationen auf der Website des Unternehmens, Versicherungsrecht (VersR) 2011, pp. 541 (542).

[103] See Ch. Armbrüster, *Der Abschluss von Versicherungsverträgen über das Internet*, Recht und Schaden (r+s) 2017, pp. 51 (62).

[104] Ch. Armbrüster, *Der Abschluss von Versicherungsverträgen über das Internet*, Recht und Schaden (r+s) 2017, pp. 51 (62).

[105] 25 January 2017 [C-375/15], in (2017) Neue Juristische Wochenschrift (NJW), pp. 871 et seq.

[106] Ch. Armbrüster/M. Obal, *Genetic information and testing in the underwriting process of insurance contracts in Germany*, in: The Impact of Genetic Data on Medicine and Insurance Practice (2014), pp. 25 et seq.

On the other hand, it is generally acknowledged that the insurer must be allowed to ask the applicant questions concerning his state of health, about any kind of medical precondition, etc.[107] For that purpose the insurer is – with consent of the applicant – even allowed to collect medical information about the applicant from health care professionals such as medical doctors or hospitals.[108] The applicant has a corresponding obligation to disclose such information asked for by the insurer.[109] If the answer to a question asked by the insurer in the context of pre-contractual risk assessment turns out to be inaccurate this may lead to severe remedies, such as the right of the insurer to withdraw from the contract or the right to retroactively exclude the respective risks.[110]

In that context, the question arises whether or not insurers should be unrestrictedly entitled to ask applicants not only about the results of genetic testing which the applicant already underwent, but also oblige him to undergo such tests in order to obtain insurance cover. Taking into account the right (and the obligation, with regard to other policyholders) of the insurer to assess the individual risk of the applicant properly and correctly, one would tend to grant the insurer such powers. However Art. 2 para. 1 of the German Constitution (*Grundgesetz*, *GG*) guarantees the right of free development of the personality. This fundamental right includes the right not to know about one's own genetic dispositions,[111] which the legislator is constitutionally obliged to protect.[112] Furthermore, the disclosure of results of tests the applicant had already undergone before seeking insurance cover may lead to discrimination based on the genetic dispositions of the applicant.[113]

In order to address this issue, in 2010 the German legislator passed the Genetic Diagnostics Act (GDA, *Gendiagnostikgesetz*, *GenDG*), which strictly limits the right of the insurer to ask applicants to disclose results of tests already conducted and the right to oblige applicants to undergo genetics examination.[114] As a rule the GDA bans the insurer from asking for any kind of genetic testing or information before and after the contract is

[107] See Sect. 19 para. 1 VVG.

[108] See Sect. 213 VVG.

[109] Ch. Armbrüster, in: *Prölss/Martin, Versicherungsvertragsgesetz*: VVG (29th edition), § 19 VVG marginal no. 1.

[110] See Sect. 19 para. 2 – 4 VVG.

[111] Di Fabio, in: Maunz/Düring, *Grundgesetz-Kommentar* (79th edition 2016), Art. 2 GG marginal no. 192.

[112] See *Bundesverfassungsgericht* (BVerfG), 1. Senat (25 Feburary 1975) [1 BvF 1 – 6/74] = Neue Juristische Wochenschrift (NJW) 1975, 573 ff.; 1. Senat (16 October 1977) [1 BvQ 5/77] = Neue Juristische Wochenschrift (NJW) 1977, 2255 [Schleyer].

[113] Compare Verwaltungsgericht Darmstadt (24th June 2004) [1 E 470/04 (3)] marginal no. 37.

[114] Sect. 18 GenDG.

concluded. Furthermore, the insurer is not allowed to ask for results of previously taken tests. Thus the legislator aims at ascertaining that the insurer shall neither receive nor use any such information.[115] However an exception is made with regard to life, occupational disability, disability and long-term care insurance given that the insurance sum exceeds EUR 300.000 or an annuity exceeds EUR 30.000, as in this case the interest of the insurer to know the results of genetic testing the applicant has already undergone surpasses the interest of the applicant not to disclose such information. This exception has been implemented in order to prevent applicants from abusing their information advantage in large policies (risk of adverse selection).[116] Furthermore, in any case illnesses and pre-existing conditions remain to have to be disclosed upon demand even if they were diagnosed with means of genetic analysis.[117]

V. Impact of data on claims assessment

- *Has the assessment of claims been affected by the availability of data? In particular, are there any industry-wide arrangements in place whereby insurers can share information on fraud?*

First of all, the sheer endless availability of data has enormously influenced and reshaped the means which insurers use to assess individual claims. For instance, the data collected by a black box used for telematics-based car insurance policies can be used in order to properly reconstruct the course of an accident giving indications about whether or not the insurer is released from liability, data collected by so-called smart homes facilitates the assessment whether or not the policyholder has complied with contractual obligations, etc.

Furthermore, when it comes to (attempted) fraud, the German insurance industry established the reference and information system (*Hinweis- und Informationssystem der Versicherungswirtschaft, HIS*).[118] The purpose of this system is to prevent fraud and to secure and protect the interests of the insurer as well as the collective of policyholders.

---

[115] See Sect. 18 para. 1 GenDG.

[116] *Ch. Armbrüster/M. Obal*, Genetic information and testing in the underwriting process of insurance contracts in Germany, in: *The Impact of Genetic Data on Medicine and Insurance Practice* (2014), pp. 25 (31 et seq.), also addressing controversial questions in relation with Sect. 18 GenDG.

[117] See. Sect. 18 para. 2 GenDG.

[118] For an overview see GDV, *Hinweis- und Informationssystem der deutschen Versicherer – HIS. Was es ist und was es leistet*, retraceable under http://www.gdv.de/wp-content/uploads/2016/07/HIS_Infoblatt_lang_Internet_Neu_2016.pdf (last checked on 13/9/2017).

The system is compliant with EU and German data protection provisions. In case it is found that a policyholder is suspected of committing fraud or attempted to commit fraud (e.g. by faking or pretending an insured event) the respective data are under certain conditions stored on the servers of the HIS. Other insurance companies can access these data when pre-contractually assessing the risk of an applicant or assessing the righteousness of a claim brought before them by a policyholder. It is worth noticing that an entry in the HIS does not trigger any kind of automatism with regard to the insurer's decision to reject applications or claims. An entry might just be used as an indication for the insurer to carry out special means of risk assessment or to have a closer look at certain aspects of the claim.[119]

D. Other new technology risks

- *Are there any other particular risks from the new technologies that have been identified in your jurisdiction? If so, is there any legislation in place or under consideration to regulate them?*

I. Robotic

Further risks from new technologies refer to the field of robotics and artificial intelligence. Particularly at the EU level a debate regarding harmonized liability rules has already begun. There is a broad consensus that EU-wide rules are needed for the fast-evolving field of robotics, e.g. to enforce ethical standards or establish liability for accidents involving driverless cars. Members of the European Parliament have already asked the European Commission to propose rules on robotics and artificial intelligence in order to fully exploit their economic potential and to guarantee a standard level of safety and security. The European Parliament has decided to adopt their resolution of 16 February 2017 with a recommendation to the Commission on Civil Law Rules on Robotics.[120] However, as mentioned above the European Commission has already launched a consultation on the effectiveness of the Product Liability Directive[121] with regard to damages caused by new technology developments.

[119] For an overview see GDV, *Hinweis- und Informationssystem der deutschen Versicherer – HIS. Was es ist und was es leistet*, retraceable under http://www.gdv.de/wp-content/uploads/2016/07/HIS_Infoblatt_lang_Internet_Neu_2016.pdf (last checked on 13/9/2017).
[120] 2015/2103(INL).
[121] 85/374/EWG.

II. Nanotechnology

Risks resulting from the use of nanotechnology also fall within the scope of new technology risks. Products made with nanotechnology comprise yet unknown or unassessed risks which are hence to be categorized as emerging risks.[122] Further technological and scientific progress thus depends on reliable insurance solutions. Therefore, insurance companies play a key role with regard to setting the basis for innovation in the field of nanotechnologies. Although the risk itself – at least in its entirety – may in fact hardly be assessed correctly, the contractual practice offers instruments that are suitable to stem that challenge, e.g. the limitation of insurance sums and of the duration of the policy, the establishment of minimum security standards, the definition of the insured event based on the claims made principle, etc.[123]

[122] Ch. Armbrüster, *Nanotechnologie – Rechtliche Aspekte zur Versicherbarkeit von Produkten am Anfang neuer wissenschaftlicher Erkenntnisse*, Zeitschrift für die gesamte Versicherungswissenschaft (ZVersWiss) 2013, pp. 183 (184); for a closer examination of the insureability of emerging risks see H. Teschabai-Oglu, *Die Versicherbarkeit von Emerging Risks in der Haftpflichtversicherung*, 2012.

[123] Ch. Armbrüster, *Nanotechnologie – Rechtliche Aspekte zur Versicherbarkeit von Produkten am Anfang neuer wissenschaftlicher Erkenntnisse*, Zeitschrift für die gesamte Versicherungswissenschaft (ZVersWiss) 2013, pp. 183 et seq.