PLATTFORM INDUSTRIE 4.0

WORKING PAPER

Industrie 4.0 – How well the law is keeping pace

Imprint

Publisher
The Federal Ministry for Economic Affairs
and Energy (BMWi)
Public relations
11019 Berlin www.bmwi.de
www.bmwi.de

Editors
Plattform Industrie 4.0
Bertolt-Brecht-Platz 3
10117 Berlin

Design and layout
PRpetuum GmbH, Munich

Version
October 2016

Print
MKL Druck GmbH & Co. KG, Ostbevern

Photo credits
Getty Images/Ralf Hiemisch (Title); fotogestoeber – Fotolia (p. 4); vege – Fotolia (p. 5); Nonwarit – Fotolia (p. 6); vectorfusionart – Fotolia (p. 9); iconimage – Fotolia (p. 10); bluebay2014 – Fotolia (p. 13); cunaplus – Fotolia (p. 15); sebra – Fotolia (p. 17); Maksim Kabakou – Fotolia (p. 18); deepagopi2011 – Fotolia (p. 23); industrieblick – Fotolia (p. 25); Syda Productions – Fotolia (p. 27); contrastwerkstatt – Fotolia (p. 29)

This brochure and other publications are available from:
The Federal Ministry for Economic Affairs and Energy (BMWi)
Public relations
e-mail: publikationen@bundesregierung.de
www.bmwi.de

To order please call:
Phone: 030 182722721
Fax: 030 18102722721

Introduction

The Legal Framework Work Group (WG 4) has in the past few months systematically identified and formulated what it perceives to be the most significant legal aspects of Industrie 4.0 processes. The first priority was to agree on recognisable problem areas. Then the more than 30 company lawyers, association lawyers and attorneys of the Work Group concentrated on analysing the application scenarios developed by the Plattform Industrie 4.0 technical work groups. The insight gained into technical possibilities provided by application scenarios was then used to structure the group's main areas of focus into 17 topics.

For each topic a fact sheet was prepared (Part A), containing the thematic focus and related questions and areas for action in connection with Industrie 4.0 processes.

Part B contains a legal assessment of the issues. This assessment contains a compilation and review of relevant legal norms that relate to the questions or areas requiring action.

Part C discusses the possible legislative courses of action for each subject area and specific recommendations for action from the Legal Framework Work Group.

Overview of topics

Civil Law and Civil Procedure

Freedom of contract

A: Fact sheet

What is involved?

The opportunities and potential offered by Industrie 4.0 can only be taken advantage of with innovative business processes and models to accommodate novel services and products.

Because important aspects of innovative business models are so novel, there are naturally no specific legal norms yet (for example, for "automated declarations of intent", performance specifications and distribution of risk). Accordingly, important aspects and factors can and must be determined by contract.

In order to economically implement innovative business processes and models for novel services and products, reliable contractual clauses are absolutely necessary. However, excessive application of the governing GTCB, also in the B2B area, is a hindrance in German law for a solid contractual base.

This poses a basic challenge to the business case for innovative business models and crucial investments.

Questions and areas for action:

- To what extent is it justified to apply the consumer protection regulations contained in German GTCB law to the B2B area? Areas for action: Assess the possibility of greater flexibility in GTBC law for B2B agreements relating to innovative business models.
- How can contractual agreements in the B2B area (once again) provide the scope that is both necessary and reliable?
- Uncertainty about the validity of agreements is a disincentive to investments in innovative business processes and models – how can this be remedied? Areas for action: Determine how to make innovative contract models internationally competitive.
- How can contracts be drafted to contain clauses that ensure that the costs of innovative business models and services are computable (for example validity of specific performance agreements, distribution of risk, definition of liability)?
- Areas for action: Determine the enforceability of contracts in an international context.

B: Legal Assessment

Legal status is described by Sections 305 ff of the German Civil Code. Case law is increasingly and excessively applying the clause prohibitions to consumer transactions (Secs. 308 and 309 of the German Civil Code) and by means of Section 307 (2) of the Code, also to B2B transactions. The legislative proposal for a new construction contract law would even expressly provide that the rules governing consumer transactions shall be taken into account for transactions with entrepreneurs within the meaning of GTCB law. The provisions of Section 310 (1) sent. 2 of the German Civil Code, which require reasonable consideration of customary practice of the trade when applied in B2B transactions, are almost always disregarded in practice and in case law.

Prof. Leuschner of Osnabrück University prepared a comparative law study for the Federal Ministry of Justice and Consumer Protection (published February 2015) that found that – from the point of view of the legal reality – German GTCB law is detrimental to doing business in Germany and must be reformed. This trend is accelerated by new legislative proposals (e.g. construction contract law) that also leads to an escalation in use of consumer protection provisions of GTCB in business-to-business transactions.

This disadvantage is also demonstrated by a comparison with legal systems in bordering European countries. Foreign law contract provisions that are common in international use often cannot be applied in Germany.

This leads to a greater incentive or even a real necessity to flee German law. Because neither the Internet nor Industrie 4.0 are limited by national boundaries, this leads to greater flexibility regarding investment location. This also fulfils the prerequisites for choosing a foreign jurisdiction for contracts, which is permissible under German GTCB law.

Especially for small and medium-sized businesses, escaping to foreign jurisdictions means more cost and effort and greater risks, which increases the disadvantage of doing business in Germany for SMEs. This is especially true for start-ups, which sometimes establish their businesses outside of Germany from the start.

In addition, it is hardly possible to provide legal support for B2B transactions in the form of suitable and dependably applicable declaration and contract templates under current GTCB law. This problem also will also apply to any recommendations for terms and conditions to be applied in Industrie 4.0.

C: Options and recommendations for action

The goal and prerequisite for successful implementation of Industrie 4.0 is to create legal provisions that can be subjected to a reliable test of applicability to innovative business models.

Conceivable solutions could include:

- It must once again be possible to reliably define principal and secondary obligations in a contract without extensive limitations resulting from a test of reasonableness. Solutions could include a realistic definition of the term “negotiate”in the B2B area within the meaning of Sec. 305 (1) sent. 2 of the German Civil Code, and the elimination of the requirement to take into account Secs. 308 and 309 when applying the test of reasonableness as per Sec. 307 (2) of the Code, including consideration of innovative business models that do not closely resemble contracts typical at the time the Code was created in 1900.

- The requirement of sufficient transparency should be maintained, for the protection of SMEs.

- Protecting SMEs from abuse of a dominant market position is still the basic task of anti-trust and competition law – not however of contract law. An amendment to the Act against Restraints of Competition (9th GWB-Novelle) has already been drafted, and will provide for better treatment of digital business processes.

General terms and conditions of business must be made more flexible in order to place Industrie 4.0 on a solid legal footing in Germany. The goal is not to completely dismantle the protection provided by GTCB law for those companies earnestly in need of protection against unreasonable clauses, especially SMEs.

Ideas for possible changes can be found in the recommendations made in the AGB-Initiatives (GTCB) launched by the German Engineering Federation (VDMA) and the German Electrical and Electronic Manufacturers' Association (ZVEI), focussing on Sections 305 and 310 of the German Civil Code.

There is no alternative to this type of legislative action, according to Plattform Industrie 4.0. Maintaining current provisions without any changes would influence long-term case law, leading to increased disadvantages and restrictions for Industrie 4.0 in Germany. A European solution would not help, because the problem here is an isolated regulatory disadvantage in German law.

The market is forward-looking, and in particular requires reliable statutory provisions for innovative business models. To this end, the necessary freedom of contract must be reinstated.

Declaration of intent and concluding contracts

A: Fact sheet

What is involved?

One major innovative step of Industrie 4.0 is automatic control and optimization of business processes and production processes by connecting machines and IT systems across companies. This is essential to take advantage of efficiency and cost benefits and to make business processes more flexible.

To do this, machines communicating directly with each other must exchange valid declarations and conclude binding agreements. However, current legal provisions are only tailored to declarations and agreements made between people, not machines (machine declarations).

Without binding declarations and agreements made by machines, Industrie 4.0 business and production processes are up against fundamental obstacles.

Questions and areas for action:

What conditions must machine declarations fulfil to be legally valid?

- Which parties are responsible for machine declarations? Areas for action: Review the actual risks to attributability and validity of machine declarations.
- Are machine declarations binding even if the content was not clearly predictable for the machine operators? Areas for action: Using AI systems to categorize autonomous declarations of intent.
- How can the effects of an "incorrect" machine declaration be eliminated?
- How can machine declarations be monitored and verified?
- How can a contract be concluded between machines with binding effect? Areas for action: Delineating roles of simple machine declarations (as the technical means/messenger/representative) from autonomous declarations issued by systems using artificial intelligence systems (AI systems).
- What are the due diligence duties of the sender and the receiver of machine declarations?

B: Legal Assessment

The German Civil Code does not contain any provisions that are expressly applicable to machine communication. Current jurisprudence applies provisions of the Code intended for human declarations of intent, in some cases also to digital communication using machines.

The Work Group sees the consequences of applying the provisions on human declarations of intent also to machine declarations as follows:

- Declarations (also those sent by "intelligent" machines) are always attributable to the sender if they actually stem from its sphere. The "sender" is the party that recognizably wants to give a declaration that is effective for itself or for a third party. This is usually the party using the machine for its own purposes or commissioning the machine for its own purposes, however not necessarily the technical sender of the digital message.
- Declarations are also binding on the sender if the sender could not specifically foresee the contents of these declarations (an exception is when the recipient recognises that contents are obviously defective).
- Declarations of intent can only be set aside under general provisions (for example by challenge).
- The sender may only assert claims against third parties for binding "incorrect" declarations – under certain conditions.

C: Options and recommendations for action

It might be advisable to create specific legal provisions for machine declarations. This however could not be expected to bring about any improvement over the current regulations on declarations of intent. For this reason, too, there is no need for specific rules.

In order to safely apply rules for human declarations of intent to machine communication and to avoid uncertainty or contradicting interpretations in the literature or case law, however, it would be advisable to clarify the statutory rules:

> *"The provisions for declarations of intent and contract conclusions also apply if they are made using machines."*

If for no other reason than legal certainty, in particular for the respective recipient of the declaration, there is no other alternative to using these legally anchored principles. The recipient of the declaration will frequently not recognize or be able to recognize how the declaration was provided by the sender. Accordingly, this clarification should also be conducted independently of the role of the machine, in particular independently of a legal qualification as either a messenger or representative.

However, additional clarifications or additions are not being conducted. Nevertheless, the practical implementation should be continually observed and analysed, in order to assess any need for more specific rules or regulations for Industrie 4.0.

IT and Data Protection Law

IT Security

A: Fact sheet

What is involved?

Guaranteeing IT security is one of the core topics of the entire digitalised economy, and therefore not purely a phenomenon of Industrie 4.0. However, as systems and production facilities become more and more interconnected and production processes increasingly autonomous, the risk of cyberattacks and threats also increases significantly. Furthermore, cyberattacks are becoming more targeted and are carried out with more technologically sophisticated means – which also heightens the security threat. In view of this growing significance of cyberspace and information systems it is important to minimise risks and threats to network and information security.

Maintaining IT security involves two parallel thrusts:

1. Protecting humans and the environment against IT systems
2. Protecting facilities and products from unauthorized access

In general, five respected basic values are central to implementing IT security:

1. Providing availability: ensuring IT system functionality
2. Integrity: preventing manipulation of information
3. Confidentiality: access to data and information only for individuals with proper authorisation
4. Authenticity: verification of the source
5. Quality: continual monitoring of proper implementation of security safeguards

IT security regulations are spread over a number of statutory provisions and apply only to individual parts of the German economy, usually very sensitive, or to particularly sensitive data. Accordingly, IT security statutes only focus on protecting critical infrastructure, not however on enhancing confidentiality or ensuring the integrity of information systems overall. However, with regard to Industrie 4.0 applications it is important to remember that any regulatory adjustments also represent interference in the transactional and contractual autonomy of companies.

Questions:

- To what extent are Industrie 4.0 applications oriented toward the public good?
- Is the company location a factor of the company's own interests?
- Are liability clauses offered by IT manufacturers and vendors for IT services in case of defects in data protection and IT security sufficient?
- Is there a need to make adaptations for transborder collaboration?

B: Legal Assessment

The aspect of operational safety of manufacturing facilities and thereby the safety of humans and the environment are well studied, with a resulting multitude of norms and standards.

An example of these provisions are the European Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and the German implementation in the context of the Ninth Regulation of the Product Safety Act (9. ProdSV). According to the relevant literature[1], there is an acute need to take action to protect IT systems and manufacturing facilities from external attacks. This applies both to interconnected smart production sites as well as to similar types of sites (Industrie 3.0; interaction between informatics, electronics and mechanics) and includes the basic values described in Section A.

1. Orientation toward the public interest

The legislative measures taken up until now, first and foremost the German IT Security Act and the European Directive on security of network and information systems (NIS Directive), aim not to increase the level of security in general, rather "only" to maintain functionality of the Internet as a critical infrastructure, and to protect various areas with critical infrastructures, such as energy, transportation and health. These measures are based on a constitutional consensus regarding the public good and therefore only regulate those areas affecting the public interest (critical infrastructures). The legal framework of the IT Security Act is only applicable to Industrie 4.0 activities if parts of the interconnected systems are based on critical infrastructures or are themselves part of a critical infrastructure. Even the NIS Directive will change this focus in the context of Industrie 4.0 only marginally. Also with respect to the particular systemic relevance, the focus on the public good is not a sufficient criterion for a) categorizing Industrie 4.0 applications as critical infrastructures and thereby b) enhancing cyber security across all application scenarios.

2. Self-interest

The focus must therefore be placed more on company self-interests. In general, companies are obligated to ensure proper systems and controls, which also includes proper protective precautions for ensuring IT security.[2] Sec. 91 (2) of the German Stock Corporation Act provides a general basis for this in connection with the duties of the management board, where early warning systems or "surveillance systems are concerned, to ensure that developments threatening the continuation of the company are detected early".

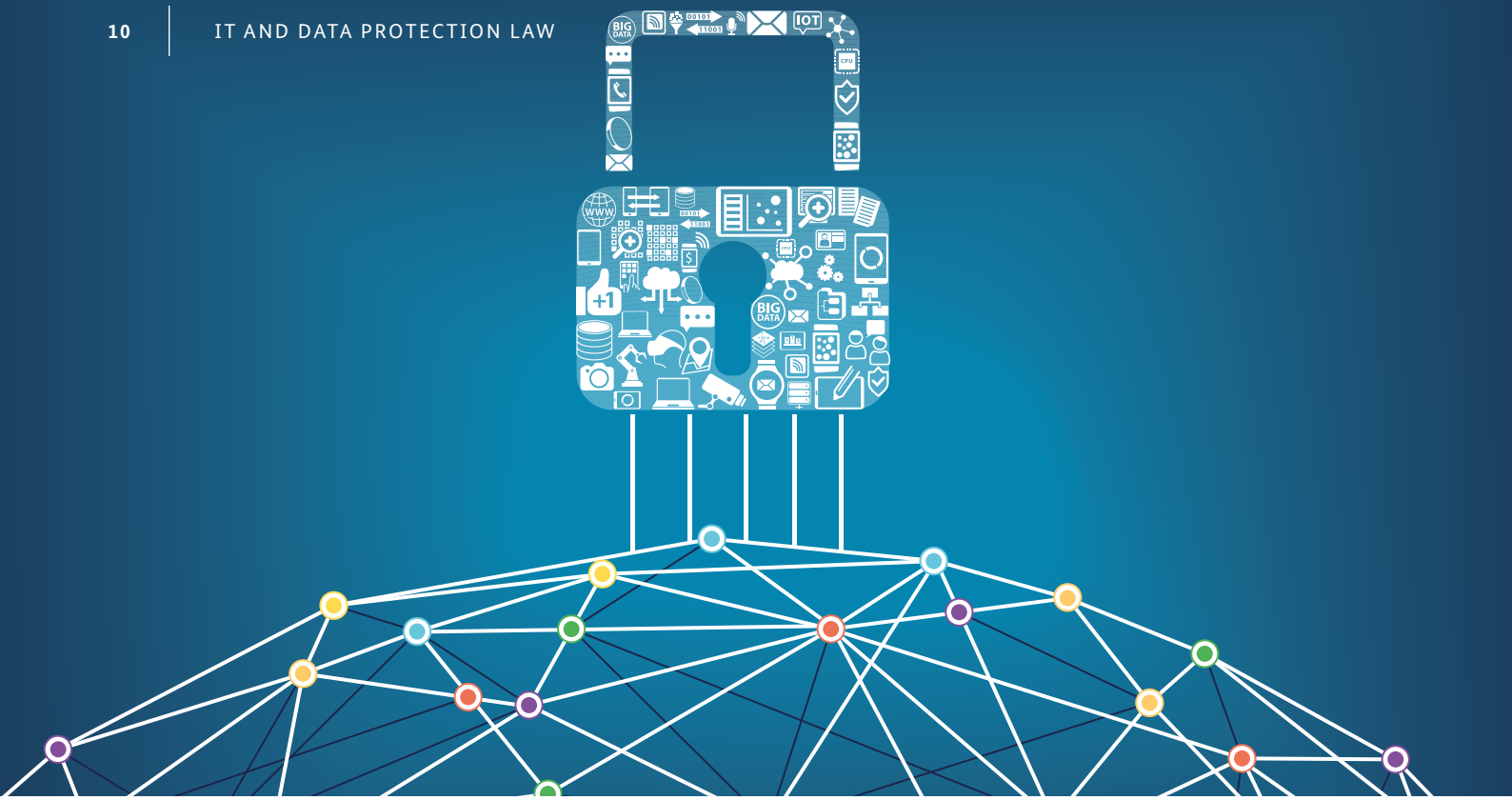
On the one hand, this does not provide a basis for any clearly defined security standards. What's more, these early warning systems are concerned with the continuation of a company as such, but not necessarily the risk to or impairment of ongoing operations. However, it may be worthwhile considering how to incorporate into Sec. 91 (2) of the Stock Corporation Act more firmly, or clarify, that "surveillance systems" also include in particular security mechanisms against cyber risks.

The term IT security primarily means functional security of a component of operational reliability, and not so much the topic of protection against attacks[3]. "It is generally advisable to adjust security measures and processes to the

1 See inter alia Forschungsunion/acatech, Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, p. 50, BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, p. 108.

2 See BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, p. 109

3 BITKOM, Rechtliche Aspekte von Industrie 4.0, April 2016, S. 28.



company's specific needs [...] ".[4] The company's own interest in creating a high level of IT security, for example in interconnected cyber-physical systems, can be deduced from other primary motives. At the fore of a company's security concerns is protection of process know-how and intellectual property rights (IPR). However, this also means – with respect to areas needing action – that self-interest does not give rise to any legislative motivation. With a view to IT security, such as preventing industrial espionage or protecting IPR, there are no special legal aspects of Industrie 4.0 compared to current processes, except that the increasing connectivity of systems will heighten the "risk of break-in and abuse" and that accordingly access controls and encryption methods must be improved. In the current state of things, it is ultimately up to user demand – or in interconnected Industrie 4.0 structures, to the interconnected companies acting as a consortium – to decide whether they individually will implement a higher security level than the minimum standards.

3. Liability

Due to the difficulty of defining standard security norms, the issue of liability, even in the context of providing a high level of IT security, is a very important aspect.

However, as experience with the IT Security Act has shown, it is a well-known fact that it is difficult for legislation to provide a specific level of IT security. Regulating the technical level of security by statute would continually fail due to the lengthy legislative process, such that defining the "state of the art" would be a never-ending parallel process. In this situation, contractual rules are better suited for addressing the specific requirements of the individual situation and the necessary security aspects, and so to better accommodate individual needs for protection.

In the area of product liability, there is an unresolved issue as to whether and to what extent, given the state of the art, maintaining specific IT security standards without an additional contractual basis can be required. This topic was dealt with in more detail by Sub Work Group 3 (Product liability).

4. Transborder collaboration

In view of network architecture logic, according to which network architecture is not designed according to national boundaries, it can be assumed that growing connectivity will be accompanied by an increase in transborder cooperation, which could lead to substantial friction and discussions when creating legislative standards.

4 BITKOM, Rechtliche Aspekte von Industrie 4.0, April 2016, S. 28.

In general, it can be observed that in the EU there is a sufficient level of legal certainty and harmonization, and that also outside of the EU there is a number of bilateral and international agreements and similar agreements on data protection and security (e.g. In the framework of decisions on adequacy in international data transmission). A decisive factor in determining the level of IT security is ultimately the specific legal situation in the country in which a product is being brought to market or in which Industrie 4.0 technologies are used. There is also a clear legal framework for transborder collaboration in the context of Industrie 4.0 (see inter alia Council Directive 85/374/EEC), which presently requires no adjustment.

C: Options and recommendations for action

The IT security regulations are largely generic, which is a continual source of uncertainty, especially for affected companies, as to which specific measures should be taken in a specific situation. For this reason, any discussion of a specific legislative option should address the question as to whether it will enhance the general level of IT security and, for the affected parties in particular. This applies to a much greater degree to small and medium-sized enterprises. "Lawmakers can – theoretically – impose on them the obligation to take certain precautions, yet whether this alone will result in economical solutions that are in the interest of the companies is very questionable".[5] In addition, extending for example the reporting obligations under Sec. 8b (4) of the Act on the Federal Office for Information Security could place an onerous burden on all affected parties, without achieving significant improvement in security. Much more effective would be approaches that – accompanied with political efforts – could enable companies to create a generally high level of IT security. Apart from companies that as critical infrastructures are relevant to the public good, it should be in the own interest of the companies themselves to ensure IT security – and accordingly not require any "regulatory incentives". Any efforts to strengthen future IT security should start here, and require practical measures such as encryption or "security by design", if necessary on the basis of customary trade standards (see Sec. 8a(2) of the Federal Act on the Federal Office for Information Security) and certifications (e.g. ISO) that would need to be developed.

Data protection law

A: Fact sheet

What is involved?

Data protection in connection with Industrie 4.0 scenarios is an important issue whenever personal data is being collected. This could be the case:

1. In human-machine interaction, particularly in the context of operations (e.g. partially-automated robot operation), which involves the interface between data protection and behaviour control (right of co-determination);

2. In the context of the actual application if creating a link to the individual is directly or retroactively possible or actually takes place (example: sensor data in a vehicle motor that is used to determine the facts of an accident and thereby the driver's conduct);

3. By linking sensor data to other data sources during Big Data procedures, if a personal profile can be created on this basis

Data protection laws as an expression of the constitutional right of self-determination in respect of information set high standards for collecting and processing of personal data. In general, the prior consent of the data subjects or another legal authorization is required. In addition, processing data is only allowed in the scope of a legitimate purpose to be determined beforehand. Use for other purposes, or even disclosure of the data to third parties, is always subject to the consent of the data subjects or a statutory authorization. If the data is to be processed outside of the EU and the EEA, appropriate data protection must be guaranteed.

The possibility that personal data can be processed further is therefore limited. This also affects the economic value added of Industrie 4.0 scenarios.

5 BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, p. 112..

Questions:

- When is data personal in nature? And where are the boundaries? Is the definition of what is personal absolute or relative?
- How can reliable and generally binding criteria for anonymising, pseudonymising and encryption of personal data be developed and quickly implemented? How can a risk-based approach be integrated into this process?
- How can the principle of data minimisation be quickly implemented? Are measures such as anonymisation, pseudonymisation or encryption sufficient or must efforts be made to create a regulatory framework for additional models (for example: data escrow models for Industrie 4.0 consortiums)?
- What priority do the rights of data subjects have over other rights to the data, for example those of data generators, and their economic interests?
- Under what conditions is it permissible to collect, process and disclose personal data in Industrie 4.0 scenarios? These conditions must be filled to a varying degree, according to risk to the data subjects (see the variations in risk in the foregoing examples).
- What should be considered in transborder data processing scenarios (involving personal data)?
- Are there specific requirements for platform operators, data aggregators and intermediaries that must be recorded more specifically than outsourcing data processing? How can accountability throughout the entire process chain be made transparent?

B: Legal Assessment

1. Broad scope of protection, consent and purpose limitation

Current data protection laws and the future European General Data Protection Regulation contain a very broad definition of the term personal data. This includes "any information relating to an identified or identifiable natural person". Accordingly, practically any data can become personal data if and as soon as it can be linked to a person.

This also applies to purely technical information, for example machine data or GPS coordinates, for example if they are collected to determine the location of a person or can be linked in any other way.

If personal data is used for commercial or research purposes, as can often be the case in Industrie 4.0 scenarios, this materially widens the scope of data protection law. Processing is only permitted if and to the extent that the data subject has given prior consent or of there is any other statutory justification. Consent can only provide a solid legal foundation if the purpose and scope of data use have been defined beforehand. For Industrie 4.0 scenarios in which it is not possible to define the intended use and scope of data use in advance, consent is accordingly not possible. Furthermore, data subjects may revoke their consent at any time with effect for the future. It is therefore advisable to factor in the "damocles' sword of revocation" when planning; accordingly, consent cannot be used in practice as an element of design in many cases.

If conditions for reliable data processing have not been met, any data subject may refuse to allow processing of any data related to his or her person. Furthermore, regulatory authorities and now also interest groups may take action against illegal data processing.

Any other possible legal foundations for data processing are subject to weighing the interests of data subjects, who in certain cases may also object to data processing. There is a risk that in certain cases the protection of personal data prevails over the economic interests of the data processors. The possibility of linking data to an individual therefore limits the possibilities of processing it, and in the same vein, often the economic value added.

Data that has been legally collected may be processed in the scope of the defined purpose or on a statutory basis. The limitation of purpose requires processing exclusively in the framework of the purposes for processing – whether loosely or expressly defined. Any data collected must always be immediately deleted after it has fulfilled its purpose. Use for any other purpose is only admissible under strict conditions. In many Industrie 4.0 scenarios, purpose limitation and data minimisation are at odds with creating extensive data stock and flexible processing of this data – this tension must be dealt with in particular by considering the factors of data richness, data diversity and second use.

In practice, companies need rules (also provided by appropriate guidelines, etc.) in order to comply with these requirements using smart "privacy by design" models and scalable technical and organisational protective measures, for example pseudonymisation, encryption and access rules.

Recommendation for action: The principle of data minimisation should be balanced out with strict rules for secure anonymisation and pseudonymisation technologies, in order to take turn data diversity, richness and secondary processing in the area of Industrie 4.0 to create flexible value added.

2. Anonymisation and pseudonymisation

Because the linkability of data to persons has a constitutive affect in the application of data protection law, anonymisation of data in Industrie 4.0 is very important. The requirements for successful anonymisation are very strict. This however, is one of the major problems. Several European data protection authorities feel that it is not only a matter of the horizon of the data processor, rather that all conceivable circumstances (including possible de-anonymisation by third parties) under which the direct link can be established must be factored in. Data protection authorities of other EU Member States seek to determine whether it is sufficiently probable that a processor can establish the connection to a person, or if this may be done on a regular basis. In addition, data that per se are anonymous could be combined with other data or background knowledge to establish a personal link, or this could take place over time. There is a risk of failure of anonymising processes, or that there might be an unforeseeable de-anonymisation process. If, acting on good faith, the anonymisation process is assumed to have been successful and no other data protection measures are taken, under certain circumstances unauthorized processing of personal data may ensue, with the following legal **recommendations for action**: In this situation it is advisable to continue to establish specific requirements for a legally effective anonymisation for Industrie 4.0 scenarios and to create guidelines and certification mechanisms. Furthermore, it is worth considering whether an authorised entity conducting anonymisation, in some instances according to instructions, is no longer responsible under data protection law if de-anonymisation by third parties is later possible.

The same shall apply for other measures, in particular pseudonymisation and encryption. They do not eliminate the personal link, however processing is substantially simplified and at the same time the privacy rights of the data subjects are ensured.

Regulations under current law on handling of pseudonymised data are underdeveloped. Recitals 26 and 28 and Article 6 (4(e)) of the General Data Protection Regulation indicate that European legislators aim to give clear priority and incentive to processing pseudoanonymous data (in particular Big Data solutions). However, there are presently no criteria yet for pseudonymisation and the specific requirements regarding admissibility of processing pseudonymised data. It would be good to not wait until the General Data Protection Regulation enters into force. Industrie 4.0 needs latitude, especially because processing of personal data in many situations connected with Industrie 4.0 is not the focus of value creation, rather at the most proves to be an undesirable by-product of process chains. Reliable and generally binding rules on pseudonymisation – including using encryption – will be especially helpful in making Industrie 4.0 a success.

C: Options and recommendations for action

1. Weighing interests and assessing impact using criteria regarding the degree of interference

To promote Industrie 4.0 wherever anonymisation or pseudonymisation is limited or cannot be applied, emphasis should be placed on suitable criteria and processes for carrying out simple weighing of interests or conducting a privacy impact assessment, which will be required in the future by the General Data Protection Regulation. To this end, regulators or, as will be required by the General Data Protection Regulation, the European Data Protection Board, will be called upon to develop rules and requirements. As a leitmotif, a risk-based approach should be used that focuses on the degree of interference caused by data processing. To safeguard the rights of data subjects to information regarding use of their data, data correction and deletion, as well the purpose of data protection, it will be necessary to clearly delineate in which cases weighing interests will, when in doubt, basically be decided to the advantage of well-defined Industrie 4.0 scenarios.

2. Transborder transfer of data

Connectivity and virtual reality are basic features of the digital transformation and therefore also of Industrie 4.0. Cloud computing is particularly important in this context. A reliable legal framework for transborder (that is, ex-EU/EEA) data transfer is essential to keep the German economy from decoupling from global supply chains and technologies. In addition to drafting a legally robust (as much as possible) EU-U.S. Privacy Shield, maintaining standard contract clauses and binding corporate rules, certification and quality labels will be very important. The European issuer of the ordinance created important prerequisites for ensuring an adequate level of protection for data transmission to third countries by means of certification of data processing (Art. 24, 42, 43, and 44 of the General Data Protection Regulation). Experience gained from the pilot project for certification to the TCDP standard (www.trusted-cloud.de) and creating a corresponding market environment are important contributions to preparing a legal basis, before the General Data Protection Regulation enters into force.

3. Platform administrators, aggregators and intermediaries

According to the usual data protection laws, all data processing steps take place between authorised entities ("data controllers") and sometimes data processors under their instructions and control. According to German law, the legal relationship for a "controller-to-processor" transfer ("C2P") is regulated by the "agreement for subcontracted data processing" ("ADV") and is subject to the complicated requirements of Sec. 11 of the Federal Data Protection Act. If however tasks are transferred, the ADV does not apply; at that point the standards for transmission to a newly authorized agent apply ("controller-to-controller", or "C2C"). This system will be retained by the General Data Protection Regulation, and creates the basis for a list of obligations for processors (Article 28). This poses special challenges to a number of processing operations, especially in the area of Industrie 4.0.

With the creation of a non-linear value-added chain or ecosystem, characterised by a multilateral exchange of data, the contours become blurred – it is increasingly difficult to identify who is, or could be, the "controller" and who the "processor". For this reason there are voices requesting that we no longer cling to the differentiation between "controller" and "processor", nor to the principle of accountability. The acceptance and specific regulation of authority to give directions is said to be reaching the limit of practicality and has no practical application.

Other authors recognize certain problems of categorization, however do not take the consequence that the respective accountabilities must be made all that much more transparent and comprehensible, across the entire process chain. They maintain that the information economy– especially in the area of Industrie 4.0 – will also require platform administrators, data aggregators, and intermediaries, to facilitate efficient and secure data exchange between the various participants. This calls for clear and transparent distribution of tasks and data protection obligations.

In this context, the goals of protection, processing transparency, data security (authenticity, integrity), client capability and portability and anchoring them with certificates are increasingly important or even of utmost importance to platform administrators, aggregators and intermediaries. These elements help the authorised entities to monitor compliance with data protection law and help safeguard the rights of the data subjects much better than defining abstract and specific authority would be able to – which the authorised entities or the affected individuals would hardly do, if at all.

Recommendations for action: In this case it would make sense to strengthen the data protection compliance of platform administrators, aggregators and intermediaries – which must be more specifically defined by statute – with framework regulations that, while ignoring the outdated ADV, ensure that the goals of processing transparency, data security and portability are achieved, by instituting corresponding certificates, as major elements of responsibility.

Product Liability

Violation of legal interests by (defective) products manufactured with Industrie 4.0 methods

A: Fact sheet

What is involved?

This topic deals with issues regarding the results of Industrie 4.0 manufacturing: smart, sometimes custom products stemming from Industrie 4.0 production enter the market as intended and thereby come into contact with users. Product defects resulting from the manufacturing process then perpetuate themselves though faulty product use, which may entail safety risks.

Questions and areas for action:

- Who is liable (also with respect to evidence) if the damage during use is clearly attributable solely to a product defect?
- Who is liable if it is not clear whether the damage was caused by the product itself or by a

B: Legal Assessment

- *Who is liable (also with respect to evidence) if the damage during use is clearly attributable solely to a product defect*

Here, contractual and non-contractual claims are to be considered. The Sub Work Group naturally focused on non-contractual claims. The provisions of Secs. 823 ff. of the German Civil Code[6] and Section 1 of the Product Liability Act[7] may be included as the basis for justifying claims.

There is no apparent need for additional legislation

Claims under contract law are to be considered on their merits any time the user is also the buyer of the product in the contractual sense.

Regarding claims for damages under Sec. 280 of the German Civil Code, in all other cases (also regarding evidence) culpability at the time of transfer is decisive, with the usual problems of liability based on fault. This can have various consequences, depending on the contractual arrangements (e.g. applying the UN Convention on Contracts for the International Sale of Goods).

6 Regarding difficulties in applying tort law: Bräutigam/Klindt, NJW 2015, 1137 (1139); Rempe, InTeR 2016, 17 (18).

7 Regarding the applicability of the Product Liability Act: Littbarski in Kilian/Heussen, Computerrechts-Handbuch, Teil 18, Rn. 24, 116, and regarding the product characteristics of software under the Product Liability Act: Wagner in § 2 ProdHaftG, MüKo, 6. Aufl. 2013, Rn. 13, 15

- *Who is liable if it is not clear whether the damage was caused by the product itself or by a mistake related to use (e.g. by an "intelligent peripheral")?*

  The non-contractual, that is, tort law bases for claims remain the same, if the manufacturer is involved. Any factors that interfere can generally be subsumed under the constituent element of the illegal action within the meaning of Sec. 823 of the German Civil Code, if applicable also in connection with a public protection law pursuant to Sec. 823 (2) of the Code. This will be the point of fact in each individual case.

  If however the technical root cause cannot be determined, under certain circumstances the injured party may have difficulty identifying the defending party. However, this does not structurally distinguish the situation discussed in the context of Industrie 4.0 from the legal risk in other situations with non-definable circumstances of cause.

C: Options and recommendations for action

If the damage is clearly attributable solely to a defect in the product, there are currently no regulatory gaps in German law. For non-contractual claims, both tort law and the Product Liability Act are suitable for solving issues related to Industrie 4.0[8].

However, proof of culpability for contractual claims represents a hurdle that is inherent in the German legal system. The same applies for proof that the product contributed to damage.

If the legal community should perceive this to be a regulatory gap, there should be a discussion regarding the approach of simple strict liability of one or several parties of the diffuse periphery, without any regard to culpability or contributory culpability. In any case, the Sub Work Group currently sees no need for taking steps in the direction of strict liability.

However, further developments should be carefully observed: at least regarding the use of autonomous or self-learning products, or to the extent that proof of culpability due to the particular characteristics of Industrie 4.0 is not possible, there could be a policy request further down the road for a statutory regulation of strict liability (e.g. similar to owner liability in road traffic).

Violations of legal interests in Industrie 4.0 facilities

A: Fact sheet

What is involved?

This topic deals with the issue of liability for the consequences of an accident occurring during a Industrie 4.0 process. Accordingly, this is an accident sustained at work (or damage to property) that occurred within an interconnected factory in which there are however no effects on the product being manufactured in relation to the sphere outside of the factory.

Questions and areas for action:

- Who is liable, if this accident was caused by a cyberattack from outside of the factory, which for example may have caused damage during individual process steps?

- Who is liable if the damage occurred without outside interference, yet there is no clear indication of a path of causality to a specific identifiable step in the process?

B: Legal Assessment

- *Who is liable, if this accident was caused by a cyberattack from outside of the factory, which for example may have caused damage during individual process steps?*

  A cyberattack can easily be subsumed as an intentional infringement of effective law as stipulated in Sec. 823 (1) of the German Civil Code. The attack basically inflicts damage just like any form of vandalism. Claims can be asserted against the identified attacker pursuant to Sec. 823 (1) (otherwise also pursuant to Sec. 823 (2) of the Code).[9]

- *Who is liable if the damage occurred without outside interference, yet there is no clear indication of a path of causality to a specific identifiable step in the process?*

  If the aforementioned claim relates to employee injury (industrial accident or damage to health), in Germany, the statutory occupational accident insurance fund covers this. On the other hand, whether the insurance fund

8 See Spindler, MMR 2008, 7 (12).

9 For a comprehensive treatment of liability issues arising from cyber attacks: Mehrbrey/Schreibauer, MMR 2016, 75 (76).

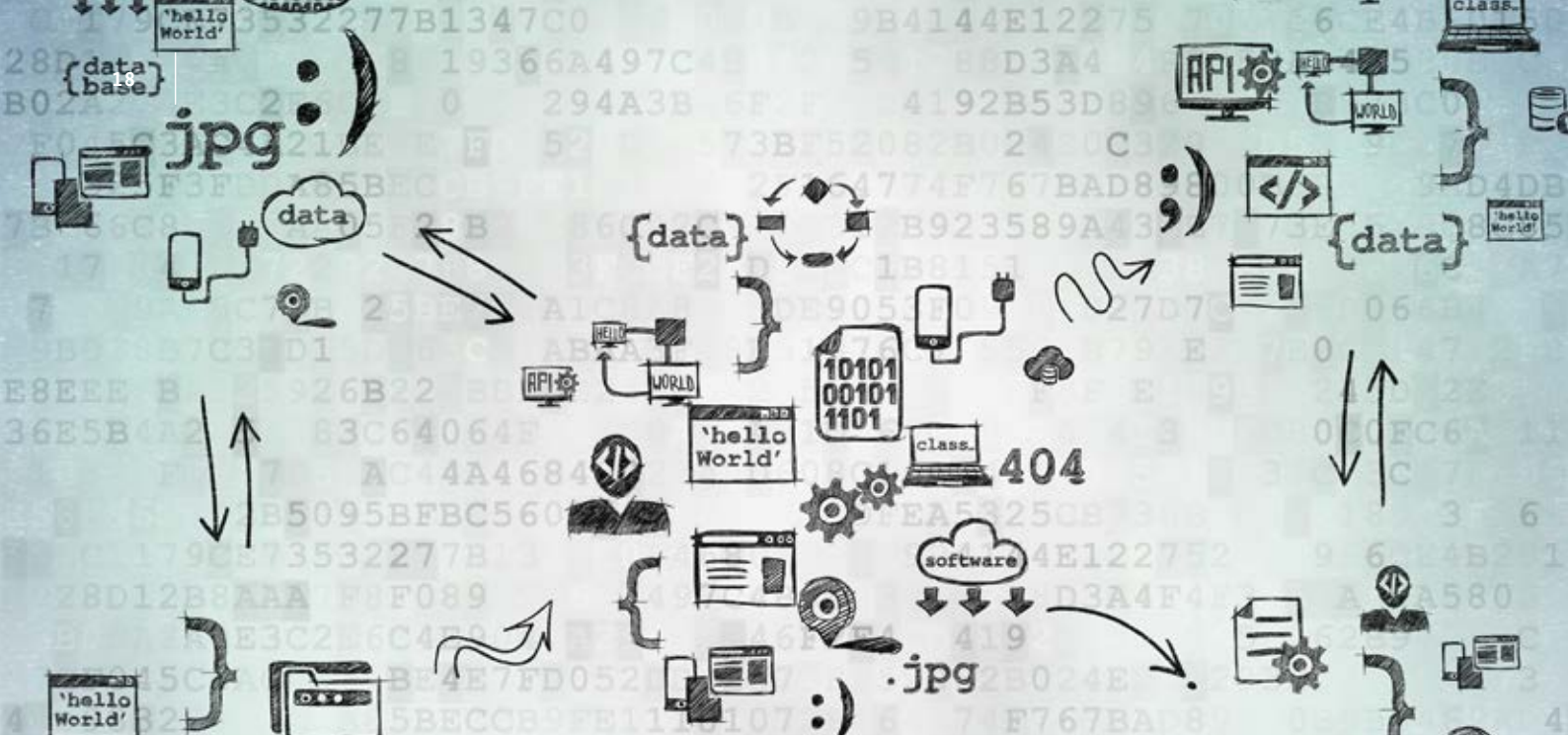
take recourse to an individual having the right to defend him – or herself, is questionable. The issue actually implies not identifying the specific offender.

However, for damage to property or other personal injury that does not involve employees (e.g. customers affected during an audit), the statutory fund system obviously provides no coverage. In such cases current laws can reach their limits.

C: Options and recommendations for action

The civil law assessment of cyber attacks outside the factory can already be conducted using available tort law instruments. Accordingly, there is no need for further development of the legal system in this aspect.

This could be different for claims in connection with the production process that occur without any definable contribution of fault by a participant. Any impetus to close any regulatory gap beyond the insurance provided by the employers' liability insurance association with respect to any other types of claims will need to consider a careful improvement on liability law.



IP Law and Data Ownership

Protecting knowhow

A: Fact sheet

What is involved?

The topic Protecting Know-How deals with questions arising from increasingly complex, and often automated creation, use and processing of company and machine data. This is particularly relevant, due to the interconnectivity across companies, for example in using cloud services, Predictive Maintenance, Condition Monitoring or Big-Data-Analysis by third parties in subcontract, or also simply during machine operation.

Questions and areas for action:

- Vast areas of manufacturing data are not linked to certain owners or protected by current legal institutions. Is this data sufficiently protected as “know-how” or as confidential business information (trade secrets)?
- What measures are necessary in order to assume that data is protected under trade secrecy (for example, contractual agreements and actual confidentiality)?

B: Legal Assessment

In the EU, national regulations on protection of business and industrial secrets differ greatly. They are often of civil law nature. In German law, business and industrial secrets are primarily protected by Sec. 17 of the Act against Unfair Competition. This is a norm in criminal law dealing with unfair competition. Civil law claims are based on Sec. 3a of the Act against Unfair Competition, or Sec. 823 (2) and Sec. 1004 of the German Civil Code. The information economy markets, from the very beginning international in nature, are not well served by the nationally fragmented legal landscape in Europe.

For this reason it would be welcomed if the EU directive on harmonization of know-how protection at least unified the law with minimum standards at the EU level. Trade secrets (meaning know-how, business secrets and technological information, Recital 14 of the Directive) are accordingly (1) information that is confidential, (2) information that has a commercial value because it is confidential, and (3) the trade secret holder should have made reasonable efforts to keep it confidential. National legal systems in the EU have up until now exhibited large differences regarding the requisite scope of confidentiality measures.

Because the directive is a minimum standard, the EU Member States could still set very different standards while transposing the directive into national law as to the required scope of confidentiality measures. The measures taken to maintain confidentiality in all legal systems are of contractual or purely factual nature:

- Confidentiality is legally regulated by the players in the economy in contracts (e.g. bilateral, multilateral or through pools or communities, for example in the form of confidentiality agreements or in user agreements or selling syndicates).

- However, confidentiality protection must also be ensured by actual separation, for example physically, from networks and server structures, as well as with cyber security measures (firewalls, regular software updates, data encryption, etc.), and by the use of hybrid or private clouds. In doing so, there must be various degrees of protection and concepts, depending on how sensitive the information is. A method for classifying information is provided by the publication "Technical Overview: Secure cross-company communication", issued by the Plattform Industrie 4.0.

C: Options and recommendations for action

The work group feels that the following aspects require action from the legislator, or that there is a need for legislative restraint, to enable the principle of freedom of contract to evolve:

- The EU directive on know-how protection should be implemented nationally as soon as possible. The work group suggests that the directive should be transposed as uniformly as possible in the various national legal systems, to create uniform conditions for the digital transformation of the economy and Industrie 4.0 in Europe. However, the Member States should not demand too much of the "reasonable efforts to keep information confidential", which are a prerequisite for legal protection of know-how under the EU directive. For example, the existence of confidentiality agreements between Industrie 4.0 partners should already suffice.

- In addition, business should quickly provide definitions for cyber security safety standards, also at the European level. These are not statutory obligations in the sense of "reasonable efforts to keep information confidential" as set forth in the directive, rather they form the basis for voluntary efforts to protect information in the context of Industrie 4.0. Uniform standards would also expedite the development of cyber security products and services (by both large companies and SMEs), promote export and help companies to be successful in the global cyber security market. In this context, export restrictions on products that provide cyber security by means of encryption technology should be sophisticated and be uniform throughout Europe, as much as possible.

- In the current situation, lawmakers should not interfere with freedom of contract regarding drafting confidentiality agreements. This allows the contracting parties to continue to either bilaterally or multilaterally define what they consider worthy of protection.

Joint ownership and "license chains"

A: Fact sheet

What is involved?

Industrie 4.0 encourages close cooperation among the participants in the various steps of production across traditional value-added boundaries. This cooperation then leads to more and more new discoveries, which may become the subject of industrial property protection, especially patents.

Accordingly, there will be more situations in the future in which the parties involved share industrial property rights to the same results (joint proprietorship). The current legal situation does not provide any clarity as to what extent, and in which cases, joint proprietors can forbid one another to exploit the rights, and in particular, to grant licenses to third parties , thereby blocking each other in the market. This deadlock will become intolerable at the point where the legal position of a joint proprietor is sufficient to allow it to block a business model or market segment in which it has no interest.

Because this has been a common problem in the past, especially in the area of patents, the need for new regulations within the framework of Industrie 4.0 is all the more acute.

Questions and areas for action:

- Is there any way to modernise the aforementioned constellations, to at least prevent participants at various market levels and with various interests from blocking each other?

- Furthermore, the question arises as to whether there is a similar need for action regarding other traditional types of intellectual property rights, such as copyright and database rights. This question also arises when considering new ancillary copyrights for data content, as has been discussed in the context of Industrie 4.0.

B: Legal Assessment

In **German intellectual property law**, and absent any diverging agreement, rights to joint proprietorship in intellectual property have often been assigned using general German Civil Code rules (see for example regarding the patent law rule on proportional proprietorship: Federal Court of Justice ruling BGH GRUR 2005, 663, 664 – Gummielastische Masse II). As a consequence – however the literature disagrees on this – it is possible that a joint proprietor would not have the right on its own to grant third-party licenses to joint rights (see for example in the area of patent law Benkard/Melullis, Patentgesetz, 11th ed. 2015, § 6, margin no. 67 with additional references). If a joint proprietor denies consent to granting a license, given the current legal ambiguity, an actual deadlock may ensue. In case of dispute, the affected party may resort to discontinuation of the joint proprietorship, including auctioning off the intellectual property right on which it is based (for patents, see Benkard/Melullis, aaO, Rz. 69). However, the patent may then end up with third parties, which does not improve the situation of the parties concerned regarding their intended exploitation of the patent.

Regarding this topic, the WG took a look at patent law in other legal systems. The following spectrum came to light, although this overview is not exhaustive:

- The most liberal is the solution offered in the U.S., where the logical consequence of the principle of "equal and undivided interest in the entire patent" is that each joint proprietor has free reign in exploiting the patent, and in particular, also in granting licenses to third parties, without having to obtain consent of co-proprietors. The only exception to this is for exclusive licenses.

  Besides that, this principle does not entail any obligation to monetary compensation of the other joint proprietors for the proceeds from patent exploitation. However, at least regarding this last aspect, German law has tended to go in this direction ever since the Federal Court of Justice decision "Gummielastische Masse II" (cited in the foregoing).

- **English law** provides a compromise: this legal system basically assumes that patent proprietors are not permitted to grant third party licenses without the consent of the co-owners, unless provided for otherwise. However, there is a remedy in the form of the "comptroller" (President of the British Patent Office), who may approve of third-party licenses if co-proprietors have created a deadlock among themselves. The comptroller is afforded wide discretion in the sense that his decision must be reasonable, appropriate and fair, taking into consideration all circumstances of each individual case, with the goal of finding a balanced economic solution, if the co-proprietors cannot agree. The reference case in this situation is the decision at the appeal level, Hughes v Paxman [2006] EWCA Civ 818; [2007] RPC 2, in which however no deadlock could be determined, and therefore no license was granted (see BL O/217/08).

- The **French approach** is relatively complex: each joint proprietor may grant non-exclusive licenses to third parties under its own name, however under the condition that appropriate compensation is paid to the other joint proprietors who do not exploit the invention themselves or have not granted any licenses. In addition, the draft licensing agreement must be transmitted to the other joint proprietors, accompanied by an offer of a specific price as compensation for their assignment of their respective joint proprietorship rights. Then, if the license opposes their own market interests, the other joint proprietors may object within a period of three months, under the condition that they acquire the joint proprietor share in question.

- And finally, **Chinese law** is based on the principle that, unless agreed otherwise, each joint proprietor may grant non-exclusive licenses to third parties without the consent of the other joint proprietors. However, this is linked to the obligation to "share" the "license fees" with the other joint proprietors according to statutory provisions.

C: Options and recommendations for action

- In particular, with regard to the topic of "joint proprietorship" or "license chains", it appears advisable to orient German patent law to a liberal model. According to this approach, proprietors of a (registered or granted) patent would in the future basically be allowed to grant third parties non-exclusive licenses to joint proprietorship rights without prior consent of joint proprietors – unless otherwise agreed – if necessary, within any other boundaries yet to be discussed (for reasons of equity, it may be advisable to not exclude compensatory payments, which however would be defined later by court rulings, if necessary). A solution, where possible by statute, should be addressed soon, to avoid deadlock situations which could otherwise become more frequent in the Industrie 4.0 environment in Germany.

- All other legal systems mentioned in Section B. have in common that they have a more liberal approach to this topic than German law; they are however either procedurally unreliable (English law, for example), or they stipulate the right to material compensation (for example in French or Chinese law), drawbacks that have justifiably been overcome in both U.S. Law and by German case law to date.

- These recommendations for action were compiled with an intentional focus on patent law. To the extent that this also applies to other classical areas of industrial property rights, the issues addressed in the foregoing should also be kept in mind, for example regarding copyright and database rights.

- Questions concerning the design of a new ancillary copyright for data content similar to ownership-rights with an associated injunctive relief do not arise as long as such an ancillary copyright is not created. If this type of ancillary copyright is considered, it should be discussed from the start whether creating these rights might magnify the complexity of potential joint proprietorship or license chains, and thereby also lead to corresponding deadlocks, to an extent making it impossible to create legal certainty, even with a regulation such as the patent law solution suggested here.

Data in the context of Industrie 4.0.

A: Fact sheet

What is involved?

For Industrie 4.0 applications, data is indispensable and a decisive factor for enhancing competitiveness. The matter at issue is data variety, coming from greatly varying sources and with greatly different meaning. Data regarding machines (e.g. from their parameterization) can be just as useful as data generated by machine use. In many cases, added value arises only when various data records are correlated (Big Data Analytics). Systematic evaluation holds the promise of new production knowledge and competitive advantage. In considering the legal aspects of data traffic, it is important to differentiate between "personal data" within the meaning of Section 3 (1) of the Federal Data Protection Act, and other data without a connection to a specific natural person (purely "machine data"). The treatment of personal data is subject to specific requirements stipulated by data protection law.

The analysis and evaluation of machine data will be the business models – some as yet undiscovered – of the future. Machine data can represent much more economic value added and be at the heart of changes in value creation. It is therefore a matter of the need for and the possibilities of legal security for the corresponding data. At present, there are no specific statutory provisions that assign machine data to a specific legal entity (data ownership).

In application scenarios in which the data being used is personal, complying with applicable data protection law is additionally a necessary condition, and is not specific to Industrie 4.0.

Questions:

- Does the law provide sufficient protection against third-party access to machine data in interconnected value-added chains?
- Are there any regulatory gaps in protection of machine data?
- What is the destiny of valuable elements of machine data in an insolvency?
- Would it be desirable to have a new law that assigns certain machine data to certain market participants in the manner of ownership?
- How can personal data be protected and at the same be made ready for use?

B: Legal Assessment

Data ownership

1.1 Situation under current law

Current law does not define comprehensive absolute rights to any data whatsoever. However, depending on the characteristics, certain constellations of data are even today – often indirectly – protected by a network of various national and international laws (copyright law, patent law, database protection law, business and industrial secrets, data protection law, criminal law, etc.).

It is interesting that statutory provisions often use meaningfulness to determine whether individual data is content worthy of protection. The individual sensor data "18 degrees centigrade", taken out of context, is by nature not protected. If however a temperature curve accompanied by time information is stored and linked to a measurement point in a certain system, this data becomes meaningful, and could represent for example a business or trade secret. Which protection applies to machine data is therefore usually determined by the particular context.

1.2 Possible regulatory need

In light of this, the work group explored the question of whether a new law is necessary that would assign certain machine data to clearly defined market participants in the manner of ownership (in turn, allowing these participants to dispose of the data).

According to the prevailing opinion among members of the WG Legal Framework, lawmakers should refrain from any further activity beyond the current legal structure and either not take any action at all, or at least not hastily. Furthermore, it appears questionable that the innumerable possible constellations of data assignment can be satisfactorily solved with abstract statutory provisions.

In addition, there is growing emphasis on the topics of data access, access authorization and data portability in the context of competition law in a variety of sectors and regulated areas. In the process of building the information economy in an open, innovation-friendly legal culture, these topics interact with the issue of any existing data ownership, or protection of data domains. Defining ownership and ownership-similar exclusivity rights to individual data too early in the game would run counter to this.

The discussion in legal science revolving around what interests in data are worthy of protection is ongoing and will remain dynamic, owing to the development of unknown possibilities and future, unknown business models. Hastily constructed definitions leading to protection of specific interests could hinder innovation and cause fragmentation of global markets.

Any assignment of data reaching beyond the current legal institutions, by means of legislative action to the benefit of certain "data stakeholders", could also harbour the risk of automatically impairing economic freedom and the level playing field for other stakeholders. On the one hand, this could prevent new business models from being developed in Europe – models on which we place new hope for desired growth and competitiveness over other global regions, for example in the are of data analysis. On the other hand, without adequate legal protection for access authorization, factual data domains and know-how, the companies operating these types of business models could be unfairly disadvantaged.

The actions of lawmakers and government agencies should be guided by the aim of fair assessments of the various interests involved. This means providing innovation with growing space and opposing undesirable developments only if they systematically infringe certain interests and equal opportunities for market participants – in particular, if they disturb the level playing field – or if there is the risk of this happening.

If at a later point in time a monopoly in the markets is created in favour of a few "data monopolies or data oligopolies", this should be dealt with using competition law. However, this type of market concentration by means of data exclusivity is not currently a foreseeable threat. In contrast to consumer business, there is no "one market participant in need of protection" in manufacturing.

The manufacturing industry is sufficiently sensitised to handling data relevant to trade secrets. In light of this, over the past few decades combining confidentiality agreements and agreements on restriction of use have provided not only a high degree of standardisation in industry, but has also led to high level of acceptance. This will equip the market well for self-regulation regarding the further development of sustainable data-use agreements, also in the context of eco-systems in Industrie 4.0. With regard to handling machine data, the companies involved in data exchange will therefore conclude agreements on data use or include such clauses in their contracts. This contractual solution is also possible without statutory assignment of ownership-type rights to machine data.

2. Protection of personal data in innovative business models

Wherever possible, lawmakers should try to achieve international harmonization of the regulatory framework.

If data is identifiable as being indirectly or directly personal data, the European General Data Protection Regulation will also attain relevance for Industrie 4.0 applications. It is therefore in the interest of developing innovative applications for Industrie 4.0 that this regulation be applied as uniformly as possible in all EU Member States. There is significant potential for finding technical solutions, such as anonymisation and pseudonymisation to protect personal data, while at the same time allowing for Big Data Analytics Services. The European Data Protection Board will be responsible for this in the future, and, with participation from industry – perhaps particular sectors – will draft guidelines or confirm and approve them, which will enable the economy to provide such services on a sound legal basis.

Choosing German law in standard form contracts

Instead of rigid assignment by statute of data ownership and access rights to certain categories of market participants, companies should preferably be in a position to organize such rights among themselves by contract. In order to strengthen freedom of contract in B2B transactions, lawmakers should remove existing legal ambiguities in German GTCB law. It can be assumed that the use of pre-formulated standard contracts in interconnected value-added chains in Industrie 4.0 will continue to gain considerable importance. At the same time, contracting parties can freely choose governing law in an internationalized world. The excessive application of restrictions on general terms and conditions in German law (GTCB law) to contracts between companies introduces an element of uncertainty regarding the reliability of German civil law, which is disadvantageous for contractual provisions, especially in innovative Industrie 4.0 business models. In order to survive in international competition, lawmakers should remove this competitive disadvantage, as best as possible.

Labour Law

Working hours in digitalised industry

A: Fact sheet

What is involved?

Working hours – both when worked and what duration – are determined by European and national regulations. European law stipulates that the number of hours worked during the week may not exceed 48 hours on a regular basis. In addition, resting periods that must be observed between work sessions are mandatory. National legislation in Germany has also determined that working hours may not exceed 10 hours per day. There are limited exceptions for certain situations. On the one hand, in the digitalised working world there will still be "traditional workplaces", yet on the other hand the need for employees to determine their own working hours will increase. Furthermore, it can be expected that the need for flexibility will increase and that working hours will not always be dictated by the employer, rather will be determined by external factors, for example end-customer-driven job assignments that trigger a short-notice procurement and production process.

Questions and areas for action:

- Are current statutory instruments for creating flexible working hours sufficient?
- Would it be helpful to liberate the 48-hour framework from the prescribed maximum daily working time for certain areas, so that for example, on certain days the employee may work more than 10 hours a day, if other days are then shortened accordingly?
- Would it make sense to shorten rest periods in order to distribute the daily working time over several time intervals during the working day?
- Should employees be given the right to individually schedule their working hours, comparable to Section 8 of the Act on Part Time and Fixed Term Employment?
- Should the works council have co-determination rights regarding work scheduling and duration of work hours, to avoid overworking? Is this a topic specific to Industrie 4.0, or is this a general issue?

B: Legal Assessment

Article 6 b) of Directive 2003/88/EC provides for more freedom of choice, stipulating only that an average maximum of 48 hours of work within 7 days must be complied with. Art. 16 b) of Directive 2003/88/EC stipulates a reference period of a maximum 4 months within which this maximum amount for hours of work must be complied with. There is no general prohibition on working Sundays or holidays. Employees may be accorded a greater degree of responsibility (Art. 17 (1) Directive 2003/88/EC) if their working hours cannot be recorded and/or determined beforehand due to the particular characteristics of their job, or if these hours are determined by the employees themselves.

C: Options and recommendations for action

It is possible to expand on the EU legal framework. For example, the limitation of daily working time to 8 or 10 hours should be revisited for certain areas of employment. Likewise, loosening the Sunday and holiday work prohibition should be given consideration. At the same time, greater flexibility also opens the door to greater risks of abuse, which could be dealt with by appropriate regulations. In this sense it is the job of the employer to strengthen and ensure compliance with working hours.

Giving employees the right to individually determine the scheduling of their working hours could underscore their individual responsibility.

The issue as to whether overworking can be prevented by giving employees co-determination rights to determine the number of hours they work or when they are scheduled should be decided after observing further developments. Collective bargaining partners already have the option of joint working hour agreements.

Occupational safety and health

A: Fact sheet

What is involved?

The digitalised work environment is increasingly causing boundaries to fall, such that in addition to the traditional job in a company, there are activities that are not bound at all any more to a work location or that can be carried out in the employee's home. Typical elements of occupational safety and health will no longer suffice to include such workplaces. Employees will increasingly work with their own equipment ("bring your own device"), over which the employer will no longer have sufficient influence regarding standards. As a result of changes in work rhythms, the demands placed on occupational safety and health could become more complex. Employment accessibility is changing, due to of e-mails, social networks, messaging service such as WhatsApp, etc., which may give rise to new health hazards.

Questions and areas for action:

- Are occupational safety and health regulations still sufficient for the altered structures found in Industrie 4.0, with relaxed limitations on hours and working location, or should existing regulations, such as the Ordinance on Working with Display Screens, or the Workplaces Ordinance, be expanded in scope, and perhaps new regulations created, for example for protection against overworking?
- Will more flexible working hours possibly create the need for a different type of protection?
- Can sufficient health protection still be maintained when employees take on more responsibility regarding their workplace, or will they need to be protected from themselves to a greater degree in the future?
- Are the protection mechanisms provided for by law still suitable for regulating the workplace, or are they in danger of being ignored in practice?
- Should there be technical precautions for avoiding "self-exploitation"?
- Should the employees' right of non-availability be more clarified?

B: Legal Assessment

Occupational safety and health is regulated by various laws, for example, the Act on Safety and Health at Work, the Occupational Safety Act, various statutory instruments, etc. Some of these rules on occupational safety are based on European law. This protection is accompanied by the rights of the works council, for example in Section 87 (1) no. 7 or Section 89 of the Works Constitution Act. Sometimes non-compliance is subject to a fine, for example under Sec. 22 of the Working Time Act, and Sec. 20 of the Occupational Safety Act.

C: Options and recommendations for action

The need to adapt existing regulations is already obvious in some areas, for example regarding the Ordinance on Working with Display Screens. In other areas there must be an assessment of whether the digitalised work environment will trigger a need to modify existing protection, or if we can assume that work in the Industrie 4.0 environment will not require any changes in occupational safety and health. If there is a recognizable need for change, current regulations will have to be adapted. It will be necessary to evaluate how to establish a balance between flexibility and protection from hazard.

It will be necessary to evaluate the technical possibilities and other options for creating better employee protection. This will be a continuous improvement process, in which the employer and works council will play an important role and take on special responsibility.

Employees already have the right to non-accessibility. Still, as there are frequent misunderstandings, this right should be clarified.

Rights of co-determination of the works council pursuant to Section 87 (1) no. 6 of the Works Constitution Act

A: Fact sheet

What is involved?

This topic deals with the co-determination rights of the works council in introducing and using technical devices designed to monitor the behaviour or the performance of employees. The Federal Labour Court is of the opinion that the objective possibility of monitoring is sufficient for requiring input from the works council. Modern work equipment is usually designed to check on employee behaviour. Time-intensive negotiations with the works council, it is feared, could lead to delays in introducing new technical devices.

Questions and areas for action:

- What are the possibilities for simplifying complex negotiations with the works council?
- Are new protection mechanisms necessary, or should available protection mechanisms be strengthened?

B: Legal Assessment

Section 87 (1) no. 6 of the Works Constitution Act grants the works council an enforceable right of co-determination in the introduction and use of technical devices designed to monitor the performance or behaviour of employees. The positive principle of consensus in this provision obligates the employer and the works council to reach an agreement. If this consensus cannot be reached, the conciliation committee will make a decision, and with a neutral chairman, may issue an opinion. As long as there is no agreement, the works council may request a cease and desist order, according to Federal Court of Justice case law, and may petition the court for temporary injunction.

C: Options and recommendations for action

Employer and employee representatives do not agree on this point: companies feel that, regarding technical changes relating to Industrie 4.0, consideration should be given to whether the employer should have a limited preliminary right to introduce these changes, under conditions yet to be specified for protecting the privacy rights of the employees affected by these changes. In this way the employer could introduce new technical devices at least to a limited extent and thereby no longer bear the risk of lagging behind competitors technically, or suffering other competitive disadvantages, due to any protracted negotiations with the works council.

However, employees' representatives reject a provisional right to introduce such devices. They perceive this to be a breach of the principles of co-determination in social matters under Section 87 of the Works Constitution Act. From their point of view, it is possible to ensure timely implementation of technical changes related to Industrie 4.0 by concluding company framework agreements that stipulate minimal technical standards for protecting privacy rights. Technical improvements can be implemented in due time without breaking with the tenets of co-determination.

Job security and skill development

A: Fact sheet

What is involved?

The prognoses for the effects of Industrie 4.0 on employment vary widely. For example, whereas the 2016 World Economic Forum held in Davos assumed that in the next five years 7 million jobs will be lost and only 2 million will be created, other forecasts predict the opposite. In Germany, a prognosis issued by the Institute for Employment Research (IAB) seems to be valid, with a projected loss of 60,000 jobs. However, the IAB assumes that by 2025 approximately 920,000 jobs will change with respect to required qualifications and will be shifted around between various occupational areas. Furthermore, companies will require qualified personnel for Industrie 4.0 tasks at short notice.

Accordingly, Industrie 4.0 will require new qualifications for employees. Even simple tasks will no longer be possible without experience in dealing with interconnected systems. Employees cannot fulfil the requirements of their jobs without continually updating their skills. On the other hand, companies that do not respond to the need to provide continuing education of their employees might fall behind their competitors.

Questions and areas for action:

- How can employees fulfil the demands put on them for further education?
- What type of government assistance is available for continuing vocational education and training?
- Should the employer grant employees eligibility for continuing education programs if the employer is planning or has already executed measures that alter the tasks of the affected employees, and render their professional knowledge and capabilities insufficient (Sec. 97 (2) of the Works Constitution Act)?
- Is it advisable to expand the rights of works councils in order to secure jobs and provide qualification, for example pursuant to Secs. 92A, 111 ff and 97 of the Works Constitution Act?

B: Legal Assessment

Labour Law provides neither for a statutory claim nor for a statutory obligation to continuing vocational training. Where there are no contractual obligations, the need for continuing education must be met with voluntary measures. The co-determination rights and cooperation rights of the works council are only meaningful at an administrative level.

C: Options and recommendations for actio

Government subsidies are an effective way to satisfy the need for continuing vocational training. It would therefore be helpful if the state stepped up this support.

The attitudes of employee representatives and industry organizations diverge regarding the issue as to whether co-determination rights should be expanded to deal with the issues of job security and professional education; employers feel that expanding such rights is not necessary and also raises constitutional issues regarding job security.

On the other hand, employees propose expanding works council rights, in particular regarding qualifications training and skill development, in order to ensure that requisite continuing training is available.

Employees should be granted the right to continuing vocational education and training. In this aspect, however, there is a controversy whether a statutory obligation for employees to submit to continuing training is reasonable. From the employees' point of view, collective bargaining agreements or employment contract clauses relating to training obligations are sufficient.

Works constitution principles in the context of Industrie 4.0

A: Fact sheet

What is involved?

There is no uniform legal definition of the term "shop". The Federal Labour Court defines operations as an organisational entity, within which the entrepreneur, alone or together with his or her employees, pursues specific work purposes on an ongoing basis with the help of tangible or intangible means to satisfy demand other than his or her own. The "shop" is the main point of departure for electing works council members, for example, as well as for exercising co-determination rights. It is the point of reference for numerous other statutory provision such as protection against dismissal for employees. Industrie 4.0 is characterised by flexible and decentralised organisational structures. Digital services are being shifted to Internet platforms, for example, and used by "crowd workers". Often a uniform management structure is lacking. In addition, demands on work in the company will continue to grow both quantitatively and qualitatively. Unions will find it increasingly challenging to communicate with employees, because "shop" as a point of reference will also change.

Questions and areas for action:

- Is the term "shop" still a useful classification criterion?
- Is the term "shop" suitable for decentralised organisational structures of Industrie 4.0?
- Should Section 3 of the Works Constitution Act – that is, the option of anchoring solutions in agreements – be expanded to include new company organisational structures?
- Should individuals in employment-like circumstances be included in the works constitution by amending Sec. 5 of the Works Constitution Act?
- Must the working basis of the works council also be improved due to digitalisation?
- Is it recommendable to modify union rights in view of changes in company structures due to digitalisation?

B: Legal Assessment

As a result of continuing digitalisation of the workplace, the term "shop", as used by the Federal Labour Court in its court decisions, is slowly becoming meaningless. This is already becoming apparent, for example, where traditional operations are only to be found where an entrepreneur pursues value creation in a more or less traditional division of labour.

For many future work relationships the term "shop" will no longer represent a suitable classification criterion. This however will cause business-related and plant-related co-determination rights to become largely unimportant and thereby working conditions will ultimately come under pressure. There is the risk that co-determination as a system will become meaningless.

C: Options and recommendations for action

In order to maintain the status quo of co-determination at shop level, Section 3 of the Works Constitution Act on establishing works constitutional structures will need to be adapted or expanded.

The number of individuals in employment-like circumstances will continue to rise as Industrie 4.0 progresses. These individuals are economically dependent on their employer, but not personally dependent. In this context, individuals in employment-like circumstances have up to now not been considered employees in the sense of the Works Constitution Act. In order to include this category of persons in coverage offered by the Works Constitution Act, these individuals should be included in Section 5 of the Works Constitution Act.

With regard to the substantial transformations brought about by digitalisation, the ability of employee representative bodies to have a say will also face new challenges.

The institution of co-determination at the shop level and corporate co-determination requires effective instruments of employee representation.

This is the only way for employee representation groups to fulfil their duties in the era of Industrie 4.0. To this end it would be helpful to make it easier for such groups to avail themselves of experts or to take a leave of absence.

In this vein, it would also be advantageous to provide unions with instruments for advertising and communication with employees that are similar to the traditional information and communication platforms (e.g. blackboards, flyers, employee meetings).

Modified hierarchies in the context of Industrie 4.0

A: Fact sheet

What is involved?

The employee is bound by the employment relationship to perform tasks delegated by others, and is personally dependent. The main characteristics of the employment relationship include in particular the aspect of subordination. The employee must always follow instructions received from the employer. In the context of Industrie 4.0, however, self-organization and autonomy take on increasing importance. For example, changes in the production line process are communicated directly to employees at the logistics contractor. Accordingly, instructions are issued not only be contractual employers, but also by customers of the employer, as in the example. Systems can also conceivably issue instructions.

Questions and areas for action:

- What are the consequences for the employment relationship if instructions are not longer given by the (contractual) employer, rather by a third party?
- Can autonomous systems (of a third party) give instructions under an employment contract?

C: Options and recommendations for action

Modified hierarchies in the context of working conditions in Industrie 4.0 can be reflected in current legal frameworks. It does not appear that there is currently the need for adapting legal frameworks.

Authority gives structure to the tasks to be carried out by employees. From a legal point of view, instructions are a unilateral declaration of intent that must be received. The fact that instructions may be issued by instances other than the actual employer (itself) is even today a common occurrence in business practice (deputies/temporary agency work). Instructions issued by machines are usually attributable to the “sender”, to the extent that they stem from the machines’ area of activity.

Employee data protection

A: Fact sheet

What is involved?

As digitalisation progresses, data processing will take on a new quality ("Big Data"). Due to Industrie 4.0, the amount of personal employment-related data will increase noticeably. This development, which will be taking place when the European General Data Protection Regulation enters into force on 25 May 2018, will lead to new challenges for reliable employee data protection (see pp. 8 ff regarding data protection).

Questions and areas for action:

- Are new protection instruments necessary, or should available protection instruments be strengthened? Is it advisable to ensure data protection with measures in addition to legal provisions, by introducing technical precautions or certification, which would provide an incentive to IT manufacturers?
- Should an employee data protection law be introduced, in order to satisfy the particular need to protect employees?
- Should the works council be granted a co-determination right regarding data protection?

B: Legal Assessment

The constitutional right of self-determination in respect of information (see Article 8 of the EU Charter of Fundamental Rights on protection of personal data) must also be guaranteed, especially in the context of Industrie 4.0 scenarios.

Article 88 of the General Data Protection Regulation provides Member States the freedom to create their own rules, by law or collective agreements, for regulating data processing in the employment context.

According to Article 88 (2) of the Regulation, such rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

C: Options and recommendations for action

In addition to laws and regulations, technical precautions (access authorisation, deletion routines, etc.) and certifications appear to be a reasonable means of creating reliable employee data protection.

German legislation should make use of the opening clause of Article 88 of the General Data Protection Regulation, to avoid a deterioration of employee data protection in Germany. Particular regard should be given to ensuring that the employer and works council retain the scope for action previously accorded them. In addition to the law amending the General Data Protection Regulation, a stand-alone and comprehensive employee data protection law would be a measure that would not only serve the special need to protect employees, but also reflect the complexity of the matter.

Whether to grant the works council co-determination rights regarding data protection that extend beyond the facilities provided by Section 87 (1) no. 6 of the Works Constitution Act (see p. 26) is a controversial question that has not been decided.

Effects of Industrie 4.0 on employment terminology

A: Fact sheet

What is involved?

The platform economy in particular, which is gaining in importance for Industrie 4.0, is expected to cause a massive increase in the number of alleged self-employed individuals, growth that can already be observed. However, these individuals often require the same protection as employees.

Questions and areas for action:

- Can the traditional definition of an "employee" be retained, or must it be broadened?
- Do changes need to be made to the term "individuals in employment-like circumstances", and also to the Home Work Act?
- Is a law for economically dependent solo self-employed persons necessary?
- Should solo self-employed persons be accepted to a greater degree in the social-insurance system?

B: Legal Assessment

The issue of employee status, especially in the platform economy, is a frequent topic of discussion. According to current criteria, some of these individuals are in employment relationships, and others are self-employed, and yet others are in employment-like circumstances or home-based work. Provisions regarding social security are therefore widely different, even though, as already mentioned, the need for social protection is often the same.

The characteristic features of "traditional employment" and also for legal delineation such as "integration in the shop'" and "the employer's right to issue instructions to employees" lose much of their meaning in Industrie 4.0. Therefore, the issue is whether to provide a modified differentiation, for example as discussed in legal circles, that would give more emphasis to entrepreneurial activities and the actual alternatives provided by the market.

The Home Work Act is obviously outdated and hardly in a position to effectively cover modern working relationships.

Protection for the self-employed, in particular those without their own employees, is very rudimentary in the social security scheme.

C: Options and recommendations for action

The Home Work Act should be amended to include crowdworking. The concept of the individual in employee-like circumstances should be revisited, with consideration as to whether the amount of income as a definition of economic dependence should be lowered.

Solo self-employed persons should be included to a greater degree in social insurance schemes. This would provide them more security and could possibly reduce the burden on society, which would otherwise be required to close a possible gap due to poverty in old age.

Other than that, we should wait to see how things develop, and use empirical studies to evaluate areas requiring action.

Closing Comments

To close, two other topics should be mentioned briefly.

Digitalisation will also require changes at the European level. The rights to information and consultation set out in the European Works Council Directive and the EU Directive on information and consultation of employees to are too limited in view of transformation caused by Industrie 4.0. For example, the Directive on Information and Consultation of Employees does not contain any provisions regarding scheduling work time, data protection or occupational health and safety. The concepts shop, employer and employee should also be redefined. In the European Works Council Directive for example, data protection and occupational safety and health are not mentioned.

Another issue is individual rights in the company. Digitalisation will benefit greatly if employees are involved. Terms such as "the democratic company" describe how the company of the future will depend on independently-thinking, innovative employees who take the initiative and must actively contribute. The question to be examined is whether to strengthen or expand individual rights of employees, such as in the works constitution, for example regarding scheduling employee meetings pursuant to Section 43 (3) of the Works Constitution Act, or regarding the right to make complaints or to be involved in the work of the works council.

Outlook

The Legal Framework Work Group (WG 4) began its work in the summer of 2015, concentrating at first on identifying possible problem areas and finding legal assessments that could lead to solutions. This publication presents the work group's recommendations and options for political action regarding 17 topics. These recommendations will be discussed and verified during the next few weeks with various actors and initiatives with experience in these areas (e.g. Round-table discussions). In addition, other countries and legal systems will be analysed with a view to solutions for Industrie 4.0 applications. Then the results will be prepared for target groups in industry and communicated in the context of special functions.

AUTHORS:

RA Dr. Martin Ahlfeld, Weidmüller Holding AG & Co. KG (Head of sub-working group IP Law) | RA Till Barleben, ZVEI Zentralverband Elektrotechnik- und Elektroindustrie e.V. | RA Mathias Cellarius, SAP SE | RA Michael Dettmer, HDI Global SE | RA Verena zu Dohna-Jaeger, IG Metall | RA Dr. Alexander Duisberg, Bird & Bird LLP | Prof. Dr. Dr. Jürgen Ensthaler, Technische Universität Berlin (Head of sub-working group IT and Data Protection Law) | Dr. Bernhard Fischer, SAP SE | RA Christian Greger, TRUMPF GmbH + Co. KG | RA Dr. Philipp Haas, Robert Bosch GmbH | RA Florian Hilbert, Siemens AG | RA Elisabeth Höller, thyssenkrupp AG | RA Nils Hullen, IBM Deutschland | RA Dr. Marc Kaiser, AUDI AG | RA Dr. Ulrich Keil, Schaeffler AG | RA Dr. Thomas Klebe, Hugo Sinzheimer Institut für Arbeitsrecht | RA Prof. Dr. Thomas Klindt, Kanzlei Noerr LLP (Head of sub-working group Product Liability and Product Safety Law) | RA Dr. Jörg Kondring, Voith GmbH | RA Thomas Kriesel, BITKOM e.V. | RA Jenny Paschen, Vodafone GmbH | Thomas Schauf, Deutsche Telekom AG | RA Dr. Johannes Schipp, T S C Fachanwälte für Arbeitsrecht (Head of sub-working group Labour Law) | RA Dr. Hans-Jürgen Schlinkert, thyssenkrupp AG | RA Carmen Schmidt, Volkswagen AG | RA Tim Schwarting, Volkswagen AG | RA Martin Schweinoch, SKW Schwarz Rechtsanwälte (Head of sub-working group Civil Law and Civil Procedure) | RA Dr. Siegfried Schwung, KUKA AG | RA Christian Steinberger, VDMA e.V. | RA Daniel van Geerenstein, VDMA e.V. | RA Marc Wirwas, HARTING KGaA | Wolfgang Zeiler, Siemens AG

This publication represents the findings of the Working group on the legal framework (Plattform Industrie 4.0).

www.plattform-i40.de