Augsburger Rechtsstudien

94

Thomas M.J. Möllers | Kathleen van der Linde (Hrsg.)

On the Fourth Industrial Revolution

Legal Perspectives from Germany and South Africa

Nomos

Augsburger Rechtsstudien

Herausgegeben im Auftrag der
Juristischen Fakultät der Universität Augsburg von

Professor Dr. Arnd Koch
Professor Dr. Thomas M.J. Möllers
Professor Dr. Matthias Rossi

Band 94

Thomas M.J. Möllers | Kathleen van der Linde (Hrsg.)

On the Fourth Industrial Revolution

Legal Perspectives from Germany and South Africa

Nomos

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

ISBN 978-3-7560-1606-8 (Print)
978-3-7489-4525-3 (ePDF)

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 978-3-7560-1606-8 (Print)
978-3-7489-4525-3 (ePDF)

Library of Congress Cataloging-in-Publication Data
Möllers, Thomas M.J. | van der Linde, Kathleen (Eds.)
On the Fourth Industrial Revolution
Legal Perspectives from Germany and South Africa
Thomas M.J. Möllers | Kathleen van der Linde (Eds.)
395 pp.
Includes bibliographic references and index.

ISBN 978-3-7560-1606-8 (Print)
978-3-7489-4525-3 (ePDF)

Online Version
Nomos eLibrary

1st Edition 2024

Preface

With this fourth book emanating from the collaboration between the law faculties of the University of Augsburg and the University of Johannesburg, we would like to thank Charl Hugo most sincerely for his many years of friendship and intensive collaboration. He is a German-South African bridge builder par excellence and without his personal commitment the collaboration between the University of Augsburg and the University of Johannesburg would not be as intensive as it is. Thomas Möllers and Charl Hugo first met each other in 2001 when Charl Hugo was still a professor at the Faculty of Law in Stellenbosch. Thomas Möllers was on his first visit to South Africa, and he was part of the delegation establishing a formal cooperation agreement between the University of Augsburg and the Rand Afrikaans University – a predecessor institution of the University of Johannesburg. During the 23 years that the cooperation agreement has been in existence, Möllers has visited Johannesburg and the University of Johannesburg many times. In 2013, Charl Hugo joined the University of Johannesburg as a professor of banking law and director of the Centre for Banking Law. Together, Charl Hugo and Thomas Möllers edited the first three joint books, which were published in 2017, 2019 and 2020. While Charl Hugo still contributed, the Covid pandemic and a serious illness prevented him from taking a lead in this fourth project. Kathleen van der Linde has now taken over this task from Charl Hugo.

The fourth collaborative book combines topics "On the 4th Industrial Revolution – Legal Perspectives from Germany and South Africa" in an innovative approach as further explained in our introductory chapter. It follows the format of the previous books, this time with contributions on topics proposed by Augsburg authors, most of whom are also research associates of the University of Johannesburg, and responses by Johannesburg authors. To meet the requirements of the Department of Higher Education and Training in South Africa, the entire manuscript was subjected to a double-blind peer review process.

We would like to thank each colleague who contributed. A special word of appreciation is due to the Vice-Chancellor and Principal of the University of Johannesburg, Professor Letlhokwa George Mpedi, who greatly enriched the research meeting with his presence and expertise, and this

book with his contribution. Mpedi was instrumental in the intensified collaboration between our two faculties while he was still the Executive Dean of the Faculty of Law at the University of Johannesburg.

The research meeting in the Kruger National Park in October 2023 will remain an unforgettable memory for all participants. The fact that Charl Hugo and Kathleen van der Linde joined their colleagues from Augsburg for a few more days of collaboration was another highlight of the exchange between the two partners.

The cooperation between the Universities of Augsburg and Johannesburg makes a significant contribution to implementing the official strategies for internationalization of the respective institutions. The law faculties of both universities have always been pioneers as well as the engine of this cooperation. Thus, it should come as no surprise that a fifth Augsburg-Johannesburg research meeting and book is already being planned for next year. The fifth project will also focus on artificial intelligence and sustainability, some of the most pressing issues of our time. While the outlook of the previous volume expressed the hope for a separate Augsburg-Johannesburg publication series, the choice of UJ Press as the new South African partner publisher has already brought this goal closer.

Finally, we would like to thank the ACELR (Augsburg Center for Global Economic Law and Regulation) research assistants, Mr. Maurice Salm and Mr. Florian Giancaterino, who have been supporting the Augsburg - Johannesburg project for several years.

We are already looking forward to the next project!

The editors

Thomas M.J. Möllers (Augsburg)

Kathleen van der Linde (Johannesburg)

April 2024

Table of Contents

Introduction

I.

It was right after the successful third Augsburg-Johannesburg research meeting in 2019 that we started arranging a fourth project. The plan was to convene a collaborative session in Johannesburg in 2021. At that time no one could have imagined the fateful day of March 11, 2020.

In November and December 2019, the first outbreaks of a novel respiratory disease occurred in Wuhan (Hubei Province) in the People's Republic of China - an event that would normally be of secondary importance for academic collaboration between Faculties. Subsequently, however, this novel respiratory disease was to spread relentlessly and become an epidemic. This epidemic quickly developed into a pandemic. The first countries began to take measures against the spread of the virus, such as travel and entry restrictions. The joyful anticipation of the meeting gave way to concerns as to whether the meeting could take place at all considering the circumstances. The declaration of a global COVID-19 pandemic by the World Health Organization (WHO) on March 11, 2020, made clear that the fourth research meeting, and the book, would have to be postponed.

Despite its devastating impact, the COVID-19 pandemic was a powerful testimony to the relevance of the project topic: The Fourth Industrial Revolution - the digitalization of business and industry. The general wave of digitalization in all areas of private and public life, as well as in the economy, that accompanied the pandemic has not only impressively demonstrated what state and society are capable of in times of crisis, but also how close to current events and how far ahead of its time the research from Augsburg and Johannesburg is.

However, this pandemic-induced surge in digitization did not take place in a legal vacuum. It was embedded in a wide variety of existing regulations, as well as through the development of these regulations and the creation of entirely new ones. When the joint research meeting finally took place in October 2023, it became clear that not only the basic principles of digitalization in Germany and South Africa needed to be addressed, but also questions about the very specific effects of advancing digitalization, for example on labour law and employee data protection. The topic of

digitization was also taken a step further. While just a few years ago, artificial intelligence was considered a topic of the future, that future is now here. Like digitalization and climate protection, it is now a defining issue of this generation and (most likely) the next. These topics would be included in the fourth project, as the Fourth Industrial Revolution cannot be fully considered with a sole focus on digitization. Therefore, environmental and nature conservation from a climate change perspective, the ever-increasing use of artificial intelligence in all areas of life, and the ensuring of human rights in an increasingly globalized, digital, and climate-threatened world, were to be touched on as well.

In addition to the COVID-19 pandemic, the second major event of the 2020s that was at least as drastic and shattering would also be included in the book: the Russian invasion of Ukraine and the ongoing war between the two states.

This choice of topics demonstrates that the Fourth Augsburg-Johannesburg project is one that analyzes and discusses the major problems of the present. But it also shows how well the cooperation between the Universities of Augsburg and Johannesburg functions, despite the most adverse circumstances.

II.

1. How do legal scholars from different countries work together when the respective laws are different? Methodologically, comparative law comes to mind, but lawyers also work empirically and use the economic analysis of law. Within the framework of comparative law, a problem-oriented manner is widely agreed upon, by asking functionally how a factual problem is solved in a comparable way in another legal system.[1] Comparable are those contents, which perform the same function within the foreign law as in the familiar legal system.[2] The doctrine of legal spheres attempts to simplify comparative law by assigning several states to a legal style, according to their historical development, legal style, legal institutes (Rechtsinstitute), and legal sources, and thus to a legal sphere such as Roman, German,

1 *Möllers*, Legal Methods, 2020, Chap. 7 mn 81 ff.

2 On the principle of functionality, see *Esser*, Grundsatz und Norm, 1956, 31 ff., 349 f.; *Kötz*, RabelsZ 54 (1990), 203, 209 f.; Zweigert/*Kötz*, Einführung in die Rechtsvergleichung, 3. Aufl. 1996, 11, 33; *Junker,* JZ 1994, 921, 922.

Anglo-American, Nordic, etc.[3] Comparative law looks for similar regulatory tasks under comparable social conditions, without looking into isolated features of one system or another. Functional comparative law has been criticized for lacking a clear canon of methods. Allegedly, comparative law searches for similarities where none exist, while working from a standpoint of national preconceptions, thereby imposing a risk.[4] Additionally, the risk of circular reasoning cannot be disputed.[5] In our opinion, this is to be refuted by the fact that comparing facts and legal rules is part of the lawyer's daily business,[6] as shown by legal analogy and the comparative case method (Vergleichsfallmethode). The underlying question asks, how the respective legal systems meet the needs of the parties involved in a particular fact pattern.[7] Here the function constitutes a point of comparison, the *tertium comparationis*.[8] Thus, the functional method is independent of national legal doctrine, making it accessible to economic considerations, for example.[9] It considers the recipient.[10] The appeal of functional comparative law lies in the fact that the comparison is not limited to legal rules, but also includes social reality.[11] Similarly, legal anthropology calls for the identifica-

3 On the advantages and disadvantages of such a legal spheres doctrine see Zweigert/*Kötz*, Einführung in die Rechtsvergleichung, 3. Aufl. 1996, 62 ff.; *Pargendler,* 60 Am. J. Comp.L. 1043 ff. (2012); *David/Jauffret-Spinosi/* Goré, Les grand systèms de droit contemporains, 12e éd. 2016, S. 348; *Kischel*, Rechtsvergleichung, 2015, § 4 Rn. 1 ff.

4 On the state of the dispute see *Curran,* 46 Am. J.Comp.L. 43, 67 ff. (1998); *Husa*, RabelsZ 67 (2003), 419 ff.; *Piek*. ZEuP 2013, 60 ff.; *Reimann/Zimmermann/Michaels*, The Oxford Handbook of Comparative Law, 2nd ed. 2019, 346 ff.; *Kischel*, Rechtsvergleichung, 2015, § 3 Rn. 6 ff.

5 *Reimann/Zimmermann/Michaels*, The Oxford Handbook of Comparative Law, 2nd ed. 2019, 346, 374; Pistor, RabelsZ 88 (2022), 327 (349).

6 Likewise, already in *Kues*, De docta ignorantia, 1440, liber I cap. I: *Comparativa igitur est omnis inquisitio* – Jede Forschung ist also eine Vergleichende.

7 *Ebert*, Rechtsvergleichung, 1971, 29.

8 *de Cruz*, Comparative Law in a Changing World, 2nd ed. 1999, 230 ff.; Reimann/Zimmermann/Michaels, The Oxford Handbook of Comparative Law, 2nd ed. 2019, 346, 351, 386 f.

9 *Röver*, Vergleichende Prinzipien dinglicher Sicherheiten, 1999, § 7; *Pistor,* RabelsZ 88 (2022), 327, 328, 333 ff.

10 *Pistor*, RabelsZ 88 (2022), 327 (328, 350 f.).

11 Zweigert/*Kötz*, Einführung in die Rechtsvergleichung, 3. Aufl. 1996, 45; Reimann/Zimmermann/Michaels (ibid.), 345, 386; *Kischel*, Rechtsvergleichung, 2015, § 3 Rn. 6 ff.

tion of *modes of thought* in individual cultures that lead to similarities or differences.[12]

Less clear, however, is the question of the scope of selection in comparative law proceedings, i.e. which legal systems can or must be considered. Here, the theory of legal spheres is used to search for similarities and differences in the social, economic, cultural, historical, and ecological background. Is it permissible to use the result of comparative law only if the precedent can be found in several legal systems or is it permissible to choose the best result even if it can only be found in one legal system?[13] If the result is the same in all legal systems, a compelling argument can be made that this legal solution is also the most convincing. In this respect, one can speak of *praesumptio similitudinis*, the presumption of the similarity of the practical solution.[14] Other authors call for common values as a prerequisite for comparative law.[15] Legal solutions often vary from state to state. In this case, courts tend to pick and choose the solution that suits them best.[16]

Such evaluative comparative law studies are permissible since foreign judgments generally function as a mere source of argumentation and do not constitute *persuasive authority*. The aim is to increase the weight of the judgment. A substantive examination of the arguments in the foreign decision is critical.[17] However, when it comes to the question of whether

12 Fundamentally, Fikentscher, Modes of Thoughts, 2nd ed. 2004; Fikentscher, Law and Anthropology, 2nd ed. 2016.

13 Leaving open the question Zweigert/*Kötz* (ibid.), 17.

14 Zweigert/*Kötz* (ibid.), 39; *de Cruz*, Comparative Law in a Changing World, 2nd ed. 1999, 232.

15 *Zweigert*, in: FS Schmitthoff, 1973, 403, 404 ff.; *de Cruz*, Comparative Law in a Changing World, 2nd ed. 1999, 235; *Mehren/Murray*, Das Recht in den Vereinigten Staaten von Amerika, 2008, 100 f.; *Rosenau*, in: FS Puppe, 2011, 1597, 1610.

16 Equally, *Bobek*, Comparative Reasoning in European Supreme Courts, 2013, 240: "cherry-picking"; BGH 27.2.1992 – 5 StR 190/91, BGHSt 38, 214 (230 f.) – Unterbliebene Belehrung.

17 *Reimann/Zimmermann/Smits*, The Oxford Handbook of Comparative Law, 2nd ed. 2019, 502, 522: "because of its inherent quality"; *de Cruz,* Comparative Law in a Changing World, 2nd ed. 1999, 280, 287; similarly *Kötz*, in: FG 50 Jahre BGH, 2000, 825, 835 f., whether the judgment gains "Substanz, Anschaulichkeit und Überzeugungskraft wesentlich gewinnt" (considerable substance, clarity and persuasiveness) in the critical analysis of the foreign decision; *Bobek*, Comparative Reasoning in European Supreme Courts, 2013, 247: "quality, not quantity".

such a *legal transplant*[18] is successful, an examination of the arguments of foreign judgments alone is not enough. Like the economic analysis of the law, the foreign legal situation can only provide additional support for the decision.[19] It is also crucial to answer the question of whether the foreign legal solution is compatible with the values of national law.[20]

2. South Africa and Germany are democracies that have established fundamental rights as a value system with a strong constitution and a strong constitutional court. This is the basis for intra-disciplinary work between civil law, public law, and criminal law. The approach of the cooperation is innovative, insofar that not only individual contributions on comparative law are included. The topics will be bundled, this year on "*The fourth industrial revolution - the digitalization of business and industry*". In addition, so-called tandems present individual topics from a comparative law perspective. Lastly, the format is also open to young scientists, who are given the opportunity to present their research.

III.

This book begins with *Buchner's* contribution, which outlines the importance of digital assistance systems and wearables, such as augmented reality glasses and smartwatches, in supporting employees at work. *Buchner* points out that the processing of personal data could raise privacy concerns and affect acceptance. The proposed solution is to set up data protection management systems to ensure control over data processing.

Building on this, *Mpedi's* response examines the legal perspective on the use of wearables in the workplace in South Africa, in particular the legal obligations of employers to provide a safe working environment and how wearables can be used to ensure health and safety in the workplace. The chapter also highlights the importance of employee privacy rights and the legal and ethical considerations that employers must consider when using wearables in the workplace.

---

18 *Watson*, Legal Transplants: An Approach to Comparative Law, 2nd ed. 1974, 21 ff.; *Kischel*, Rechtsvergleichung, 2015, § 2 Rn. 34 ff. utilizes the phrase "Rechtsübernahme" (the adoption of legislation).

19 *Kodek,* in: Gamper/Verschraegen, Rechtsvergleichung als juristische Auslegungsmethode, 2013, 23, 47; *Gamper*, in: Gamper/Verschraegen (ibid.), 163, 178.

20 *Kodek*, in: Gamper/Verschraegen (ibid.), 23, 47; *Gamper*, in: Gamper/Verschraegen (ibid.), 173, 178; *Wörner-Schönecker,* Rechtstransfers, 2022, 139 ff.; *Posner*, How Judges Think, 2008, 349: "similar values, traditions, and outlook."

The chapter by *Maties* deals with the different meanings of the term "working time" in German labour law. It primarily covers the contractually owed working time in contrast to the actual working time. In the case of additional work or overtime, the question arises as to whether this work was authorized and whether payment is due. Health protection under the Working Hours Act and the employment contract in conjunction with Section 612 of the German Civil Code (BGB) play a role here. *Maties* examines the particularly interesting question of whether an employer can stipulate in a contract that overtime is not to be paid, which would be a contractual deviation from Section 612 of the German Civil Code (BGB).

As a collaborator, *Koen* discusses overtime from a South African perspective. His article examines the regulation of overtime in South Africa and compares the historical dependence of general contract law with the contemporary framework of the Basic Conditions of Employment Act (BCEA). He examines the interplay between general contract law and labour law and discusses the criticism of a traditionally contract-centric approach that is said to insufficiently address power imbalances within the labour market. The BCEA is examined more closely, in particular its provisions on maximum working hours, the prohibition of overtime without agreement and wage rates. *Koen* also looks at the historical restrictions on overtime and discusses changes that allow for flexibility in working hours. Controversies surrounding the requirement of an agreement for overtime are highlighted, as well as the payment of overtime in comparison to the German model.

Fontana emphasizes within her contribution how numerous companies operate abroad to save costs, consequently risking the occurrence of human rights violations. Local standards for occupational safety, social security and environmental protection are often low. It is not advantageous for companies to produce abroad unless the protection of human rights is part of their business strategy. Thus, a shared responsibility exists to take action to prevent human rights violations which can be traced back to the home country, the host country, and the companies themselves.

Bilchitz responds from a perspective that considers both the Global North and the Global South. According to *Bilchitz*, however, globalization has created an accountability gap for corporations that make profits at the expense of basic human rights and environmental health in host countries. *Fontana* suggests that home and host states should take joint responsibility for addressing violations of fundamental rights. However, *Bilchitz* argues - in response to this - that corporations are directly responsible for fundamental rights in international law and not just states, which he demon-

strates on the basis of existing international treaties and arbitration awards. *Bilchitz* also looks at the trend in some home countries to adopt human rights due diligence laws and emphasizes the importance of recognizing corporate obligations for their effective implementation. He concludes by discussing why recognizing direct corporate obligations is better suited to address the accountability gap but points out the problem regarding a forum for enforcing these obligations, which needs to be resolved.

The following contributions address the topic of climate change and environmental law. *Kment* discusses the introduction of the Taxonomy Regulation by the EU as a new classification system to promote sustainable development. He emphasizes that this system aims to close financing gaps by mobilizing private capital. But he warns that the resulting classification could lead to considerable controversy, particularly in the case of nuclear energy.

Botha emphasizes that South Africa, as a signatory to the UNFCCC, had committed itself to making a fair contribution to tackling climate change. He highlights the EU Taxonomy Regulation, which aims to promote climate and environmental protection and create a standardized classification system for sustainable economic activities. South Africa has also introduced the Green Finance Taxonomy with the aim of achieving a net-zero economy by 2050. The article further discusses concerns about the transition from fossil fuels to a climate-neutral future, particularly in relation to nuclear energy and the environmental impacts of uranium mining.

In her chapter, *Weininger* addresses the problem that German environmental law, with its lengthy approval procedures, is slow to respond to the challenges of climate change and rapidly developing industry. She warns that the authorities could hinder the growth and development of the industry by maintaining their current course. Due to the binding provisions of European law, simple solutions such as shortening procedures are not possible. A conflict between extensive procedural requirements in environmental law and the necessary flexibility of the economy could cause considerable problems for the German economy. *Weininger* suggests examining innovative technological approaches and applying them to regulatory measures. It is being examined whether these approaches are compatible with the applicable law in Germany.

Ngcobo also sheds light on South Africa's lengthy environmental approval procedures and the challenges of balancing economic development with environmental concerns. She emphasizes the importance of environmental impact assessment (EIA) for sustainable development, while criti-

cizing the length and resource intensity of the EIA process. *Ngcobo* discusses the opportunities of using artificial intelligence to revolutionize the EIA process. Automation through AI could lead to greater accuracy, consistency, and faster processing times, which would improve the overall quality of the process. One challenge, however, can be seen in the lack of a regulatory framework for the use of AI within the EIA process.

The next contributions consider sales law, also from an ecological perspective. *Möllers* and *Wolf* focus on the tendency of South African legislators to import European and Anglo-American legal solutions that may not fit the existing South African legal system. Similar developments can be observed in German law, which is increasingly influenced by European law, particularly the German Civil Code. In 2019, directives on the sale of goods and digital content were adopted at the European level to ensure the "proper" functioning of the European single market. These directives lead to complete harmonization and create a uniform legal framework, as the member states are not permitted to adopt different provisions. The aim of their chapter is to combine sales law with questions on European legal methodology. The existing legal remedies under sales law do not take sufficient account of environmental concerns; consideration should be given, for example, to strengthening the right to reduce the purchase price compared to the right to withdraw from the contract.

The chapter by *Hugo* and *Lupton* provides an overview on how South African sales law should be developed. They argue that the development of substantive law, particularly in international sales, should be primarily through legislative means, while the courts should take a conservative and incremental approach. Legal developments should be based on comparative and international law, but consider different social, political, and legal backgrounds in different jurisdictions. They support the continued use of industry rules in contracts and see no need for comprehensive changes to substantive law. In contrast to the EU, consumer protection law only plays a minor role. They generally support the ratification of the CISG for harmonization but emphasize the urgency of legislation on electronic trade documentation and see the UNCITRAL Model Law as a useful role model. They agree with *Möllers/Wolf* regarding the economic consequences of high consumer protection and the environmental concerns of replacing goods rather than repairing them.

Sandhu's contribution highlights the importance of data as an indispensable resource of the fourth industrial revolution and emphasizes the increasing regulation of its flow and processing within the European Union.

The EU has established itself as a strong soft power in the area of data protection and has adopted numerous legal instruments to regulate the digital sector. Data, including non-personal data, is subject to a variety of regulations and guidelines. The EU is pursuing a digital transformation of national economies, governance structures, jobs, and education systems through a new form of governance. The article provides an overview of the proposed measures in European data protection law.

In their chapter, *Buthelezi* and *van Eck* examine South Africa's response to the Digital Industrial Revolution (DIR) based on the report of the Presidential Commission on the Fourth Industrial Revolution (PC4IR). They analyze the goals, strategies, and challenges of digital transformation in South Africa and compare them with those of the European Union. The article begins with an overview of the socio-economic situation in South Africa, highlighting challenges such as poverty, unemployment, and inequality, and discussing technology as a potential solution. The authors focus on digital literacy initiatives, infrastructure, data sovereignty, entrepreneurship, and business transformation. They note that the data governance environment in South Africa is fragmented, and regulatory structures are under pressure. The PC4IR's recommendation to reassess intellectual property and data protection laws gets a positive evaluation. The article emphasizes the need for a sound strategy based on the country's unique challenges, despite valuable insights from the EU.

Gutmann discusses the importance of medical data for innovation in healthcare and notes that its potential has not yet been fully realized in the European Union and specifically in Germany. In response, the European Commission has developed a concept for a new type of Europe-wide infrastructure for medical data, the European Health Data Space (EHDS). The aim is to create a unified infrastructure for health data, while complying with data protection standards. The paper examines existing regulatory deficits and their impact on the EHDS, including cross-border data exchange infrastructures and mechanisms for data processing in research. The EHDS remains an evolving framework with potential implications for data-driven healthcare and patient rights within the EU.

In their chapter, *Borges* and *van Eck* compare the development of the European Health Data Space and data protection law with the South African law on the protection of health data. They discuss the EHDS regulation as disruptive and emphasize the contradiction between the positioning of health data as a public good in the EHDS and data protection law. In South African law, the protection of health data is based on privacy

and confidentiality, but the authors consider the regulatory framework to be inadequate. They suggest that EU regulations could serve as a guideline for stricter data regulations in the South African healthcare industry.

De Villiers focuses on the major changes in legislation since the beginning of democracy in South Africa 30 years ago. The transitional constitution of 1993 and the final constitution of 1996 are examined. A central aspect of the contribution is the promotion of the right to information, in particular information held by the state. *De Villiers* points out that the right to information has received less attention in South Africa compared to other areas of law such as the right to privacy. The relationship between the right to information and the right to privacy is also discussed in this contribution.

The final chapter, by *Lorenzmeier* and *Strydom,* examines the legal and political implications of the ongoing war in Ukraine for the EU and South Africa. This shows that the war not only has an impact on legal systems, but also adversely affects Africa's grain supply. The first part assesses the situation in the European Union, which is closely linked to Ukraine through a comprehensive association agreement. This led to Ukraine's application for membership and the EU's restrictive measures against Russia. South Africa, on the other hand, faced problems such as the ICC's international arrest warrant against the Russian president and criticism of its neutral stance in the conflict.

Thomas M.J. Möllers

Kathleen van der Linde

April 2024

The Use of Wearables in Industry 4.0

Benedikt Buchner[*] *and Maximilian Schnebbe*[**]

Abstract: Digital assistance systems or so-called wearables, such as augmented reality glasses and smartwatches, can support employees in their work in many ways. However, the use of these wearables usually involves the processing of personal, and sometimes very sensitive, data in a variety of forms, which can give rise to data protection concerns on the part of employees and thus reduce the likelihood of them being accepted. One possible approach to increasing the acceptance of wearables and ensuring that they are used in a way that complies with data protection regulations is to establish privacy management systems which enable employees to make their own decisions regarding the use of wearables and control their data processing.[1]

I. Introduction

Globalization, demographic change and the demand for flexibility are just some of the challenges in industry and production that companies are facing today and will be confronted with in the future. To enable an appropriate response to the challenges posed by Industry 4.0, companies are increasingly equipping their employees with digital assistance systems ("wearables") designed to assist them in their work. There is a diversity of possible applications, functionality and design and this is, to a great extent, dictated by the type of wearable. From smartwatches to VR glasses,

* Benedikt Buchner, Dr. iur. LLM.; Professor, University of Augsburg Faculty of Law. Chair of Civil Law, Liability Law and Law of Digitalisation; Research Associate, University of Johannesburg.

** Maximilian Schnebbe, Dr. iur.; Managing Director of DataRight GmbH.

1 This contribution is based on the results of the joint project, "PersonA", which was funded by the German Federal Ministry of Education and Research (BMBF) and the European Social Fund (ESF) as part of the Future of Work ("Zukunft der Arbeit") program (promotional codes: 02L18B550 and 02L18B551).

a variety of wearables exists, each having different functions, and collecting and processing a wide range of employee data.

II. Data protection and acceptance

Through the use of wearables in day-to-day work, employee data can be processed in a number of forms and in significant volume. This includes, for example, not only employees' location data, but also video and audio recordings from their immediate work environment, and health data as defined by Art. 9 European General Data Protection Regulation (GDPR) (for example, heart rate and blood pressure).

As soon as wearables process personal data, data protection law comes into play. If data is processed in the workplace, it is employee data protection law that applies. This is characterized by the special hierarchical relationship between employer and employee, the sensitivity of the data processed, and the partly conflicting interests of the parties concerned.[2] Under the GDPR, employee data protection is still largely the domain of national legislators due to the opening clause of Art. 88 GDPR. Whereas in the past concerning German law, s. 26 Federal Data Protection Act (*Bundesdatenschutzgesetz* – BDSG) was the most important legal basis,[3] at present it is a mix of national and EU legal requirements, until the possible adoption of a new national employee data protection law. This is because the ECJ has implicitly stated that s. 26 (1) sentence 1 BDSG is incompatible with European data protection law.[4] Furthermore, according to Art. 88 General Data Protection Regulation, it is possible for collective agreements to regulate employee data protection.

In addition to the data protection challenges, the likelihood of employees accepting wearables is also an essential consideration when seeking to implement their use. Even if a wearable is compliant with data protection law, many employees will still be concerned about data security and monitoring, and even regard their jobs as being at risk. Employee acceptance and data protection therefore go hand in hand. If employees are concerned or resentful regarding wearables, (voluntary) consent cannot be considered as legitimizing the data processing involved.

2 *Gräber/Nolden*, in: Paal/Pauly, BDSG, s. 26 note 4.
3 *Schnebbe*, DuD 2020, 398 (398).
4 ECJ, Judgment of 30 Mar 2023, C-23/21, ECLI:EU:C:2023:270.

Wearables must be designed in such a way as to meet the requirements of data protection law and take into account possible employee concerns. To ensure that this is the case, one approach is to develop appropriate privacy management systems. In a digital control centre, the employees themselves can define the extent to which wearables collect and process data so as to increase their acceptance of them. At the same time, these privacy management systems should be aligned with the core principles of data protection law in general, and employee data protection law in particular, thus ensuring compliance with data protection requirements.

III. General requirements under data protection law

First, the use of wearables requires a legal basis as a prerequisite to data processing being lawful. Furthermore, wearables must fulfill the GDPR'S key data protection requirements. For example, data processed by the system must not be misused for the purposes of monitoring performance and conduct, or for other objectives (the purpose limitation principle). These and other data protection principles, such as data minimization, accuracy and storage limitation, should as far as possible be implemented and ensured through appropriate technology design ("privacy by design"). When implementing wearables, the constitutional requirements of the company must also be taken into account, both with regard to co-determination by the Works Council and company agreements as a possible legal basis for an employee obligation to use wearables.

1. Legal basis

According to both German and European data protection law, a general prohibition of processing personal data is enforced. Processing personal data is generally prohibited unless there has been given consent or there is a legal basis for processing (employee) data. The same basic principle can also be found in South Africa's *Protection of Personal Information Act 4* of 2013 (POPIA), which is closely aligned with the requirements of the GDPR.

a) Consent

If the use of wearables is to be implemented with a privacy management system in place to allow employees to control data processing, consent is the basis for permission, cf. Art. 6 (1) lit. a GDPR or the South African equivalent s. 11 (1) lit. a of POPIA. However, consent as a justification for data processing in the context of employment relationships is not uncontroversial.[5] There are generally concerns about the voluntary nature of consent because there is a power imbalance between employer and employee.[6] However, the German Federal Labour Court does not *per se* exclude consent as a possible basis for permitting data processing in the employment relationship.[7] The decision as to how employees wish to exercise their fundamental right to informational self-determination in an employment relationship is also up to them. The fact that employees are dependent on, and under the direction of, their employers does not preclude this.

In any event, consent can only be given voluntarily if there is a guarantee that employees will not experience any disadvantage as a result of refusing consent. According to legislative records relating to s. 26 German Federal Data Protection Act, when assessing voluntariness, "in addition to the type of data processed and the level of intrusion [...] the time at which consent is given is also decisive. Prior to the conclusion of an (employment) contract, employees will regularly be exposed to a greater degree of pressure to give consent to data processing."[8] This, in turn, means that consent to the use of wearables in an ongoing employment relationship is less problematic. However, in a situation in which the employees of a particular company use wearables regularly, the employer's expectation that all employees should use them increases and this should be taken into account. It is therefore possible that individual employees may be pressured into using wearables or release more data than they actually wish to.[9] Voluntary, and thus effective, consent can no longer be presumed in this case.

Section 26 (2) sentence 2 BDSG inexhaustively lists examples which indicate that consent has been given voluntarily. In particular, this also applies to the scenario where the employee gains a legal or economic advantage as

5 See *Bieresborn*, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, Chapter 4 C note 56.
6 See *Kort*, RdA 2018, 24 (27 et seq.).
7 German Federal Labour Court, Judgment of 11.12.2014 – 8 AZR 1010/13.
8 BT-Drs. 18/11325, id. 98.
9 *Kopp/Sokoll*, NZA 2015, 1352 (1354).

a result of the data processing, or where the employer and the employee pursue similar interests. The legislative records mention the introduction of a health management system or permission for the private use of company IT systems as concrete examples of this.[10] Similar advantages can also result from using wearables if the relevant employee is given assistance during certain periods of work according to their needs. By personalizing the assistance in user menus, employees can be supported in performing their tasks and work processes can be optimized. In addition, employers and employees can pursue the same interests through the introduction of personalized wearables. In general, the employer's need correlates with the employee's wish of work beig performed as efficiently and effortlessly as possible.

Another key point in the debate regarding consent as a basis for permission to process data is the issue of *informed* consent according to Art. 4 (11) GDPR or s. 1 subparagraph 5 POPIA. For this purpose, the data subject must be aware of any consequences of providing consent and be in a position to assess them. Employees must therefore be informed comprehensively about how and to what extent their data will be processed on the basis of their consent. Consent must be given in writing or electronically. "Electronically" means that the consent can be permanently stored and proven.[11] The declaration of consent must be in an understandable and easily accessible form, and in clear and simple language.[12]

If informed consent to using wearables is to be given within the framework of a privacy management system, a particular challenge will be to prepare information in such a way as to be complete, on the one hand, any yet remain clear and comprehensible on the other.[13] In addition to the actual design and presentation of the information, other factors and circumstances are decisive when assessing whether informed consent has been given. For example, it is important to consider that the typical work environment of a wearables user in industry and production is usually not stable - instead, the user is in a dynamic environment in which they can regularly be distracted by a number of external factors.

If the abundance and level of detail of the information provided are so extensive as to be unreasonable (information overload), the mere theo-

10 BT-Drs. 18/11325, id. 98.
11 In detail, *Thüsing/Rombey*, NZA 2019, 1399 (1401).
12 *Riesenhuber,* in: BeckOK Datenschutzrecht/BDSG, s. 26 note 45.
13 *Conrad/Treeger,* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, s. 34 marginal note 452.

retical possibility of obtaining an idea of the company's data processing procedures based on the actual information provided will not be sufficient for informed consent.

The right to withdraw consent to corporate data processing at any time is also problematic. Art. 7 (3) GDPR and s. 11 (2) lit. b POPIA expressly grant data subjects such a right. The consequence of withdrawing consent is that no further data may be processed. Corporate data processing systems based on employees' voluntary disclosure of data therefore always face the risk that the basis for further data processing will no longer apply if consent is withdrawn.[14] For this reason, it is sometimes debated in data protection law whether, in certain circumstances, the right to withdraw consent should be limited.[15]

b) Other options for permission

Although consent is the primary legal basis for using wearables, there are also scenarios in which other legal bases can be relied on to process employee data. The first scenario is where an assistance system is necessary for the performance of the employment contract pursuant to Art. 6 (1) lit. b GDPR and respectively in South Africa s. 11 (1) lit. b POPIA. In addition, the processing of employee data may be justified if this is permitted on the basis of a collective agreement, cf. s. 26 (4) sentence 1 BDSG or s. 32 (1) lit. f (i) POPIA.

Based on this, the evaluation of the legitimacy of processing personal data through wearables depends on whether there is a specific requirement for this form of data processing in the course of the performance of an employment contract. However, one can argue that the term "assistance system" suggests that it is solely designed to *assist* the employee and is not yet *necessary* in the strict sense for the performance of the work.

Take the example of smart glasses that support employees in their work for a specific maintenance or repair process: Whilst these glasses may simplify this work process, shorten the time required, and reduce the likelihood of errors, they are obviously not absolutely necessary but only considered merely "helpful" to perform the work. However, it is debatable whether this legal analysis alters if a company, for instance, has no other alternative but to use wearables to save time and costs in order to remain

14 See *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, Chapter D note 532.
15 In detail, *Stemmer*, in: BeckOK Datenschutzrecht/DS-GVO, Art. 7 Rn. 93.

competitive. In any case, it is up to the company to decide how to arrange its work processes as efficiently as possible. This may lead to a scenario where the maintenance process can only be executed using data glasses in the future - thus rendering the associated data processing legally necessary.

As far as location tracking functions are concerned, these may also be necessary for an employment contract to be performed. For example, this could be the case if firefighters or employees on an oil rig are to be secured through their GPS location.[16] It may also be necessary for an employer to coordinate the work assignments of employees out in the field.[17] However, a pure tracking device is not necessarily a wearable in the sense of a personal assistance system. On the other hand, there are numerous assistance systems that have an inherent tracking function. If, for example, VR glasses have a tracking function, this function may in itself be necessary for performance in an employment relationship and the processing may thus be justified. However, for additional functions, another basis for permission must be relied on.

According to s. 26 (4) sentence 1 BDSG, a collective agreement can also justify the processing of employee data. For example, it could be agreed that the employer must provide assistance systems to support employees in their work. The data processing required for this purpose can then also be permitted. If assistance systems actually support employees and do not monitor them, such an agreement will even be appropriate.

If assistance systems are intended to monitor employee conduct and performance, the Works Council has a right of co-determination in accordance with s. 87 (1) (6) Works Constitution Act (*Betriebsverfassungsgesetz - BetrVG*)[18] in any event.[19]

Finally, in specific cases, the processing of employee data through wearables can also be justified on the basis of detecting criminal acts in the workplace. However, justifying the use of wearables exclusively on this basis is not permitted. Even if wearables that have an inherent GPS or video recording function, for example, can assist in uncovering criminal acts in the workplace, their original use must first be justified in some other way. If an employee uses wearables and has only released certain data for pro-

16 *Wedde,* in: Däubler et al., BDSG, s. 32 note 108.

17 *Beckschulze/Natzel*, BB 2010, 2368 (2373).

18 The *Betriebsverfassungsgesetz* (BetrVG) is the German Works Council Constitution Act, which regulates the cooperation between the employer and the employees' elected representatives.

19 *Wisskirchen/Schiller/Schwindling*, BB 2017, 2105 (2105 et seqq.).

cessing by consent, or if another legal basis applies, the employer can also access and process other unreleased data (provided that this is technically possible) to solve a crime in the workplace. The prerequisite for this is in any event that there must be concrete indications of a criminal offense. A mere suspicion is insufficient.[20] Furthermore, the interests of the employee and the employer must be weighed against each other in accordance with the principle of proportionality.[21]

2. Further data protection requirements

For wearables to be used in compliance with data protection law, the other GDPR requirements for processing personal data must also be observed. The backbone of these requirements is found in Art. 5 General Data Protection Regulation, which lays down the principles relating to the processing of personal data. Section 26 (5) German Federal Data Protection Act again explicitly emphasizes the particular relevance of these requirements and requires the controller to design the data processing, and the technology introduced for it, in such a way as to comply with these principles. The core tenets are privacy control (employee-determined privacy) and privacy by design (legally compliant data collection and processing through the appropriate design of the technology). Furthermore, the GDPR grants a whole range of data subjects rights, cf. Art. 12-23 GDPR or by comparison in South Africa s. 5 (1) lit. a – I POPIA, that the controller must ensure through technical and organizational measures.

To integrate this collection of data protection requirements into a privacy management system and design it accordingly, these requirements must first be categorized and classified. For this purpose, a sound approach is to take the goals of the so-called standard data protection model[22] as a guide, which proposes suitable mechanisms for translating the legal requirements of the GDPR into technical and organizational measures. It thus serves to support the design of a privacy management system by transforming

20 *Maschmann,* in: Kühling/Buchner, BDSG, s. 26 note 59.

21 *Schnebbe*, DuD 2020, 398 (399 f.).

22 This is a method adopted at the conference of the independent data protection supervisory authorities of the federal and state governments for data protection advice and verification on the basis of uniform guarantee objectives. Available online: https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode_V20b.pdf (last visit: 14.03.2023).

the abstract legal requirements of the GDPR into concrete technical and organizational measures.[23]

In addition, the standard data protection model also serves as a framework for verifying the extent to which the relevant data protection requirements have been complied with. Within this model, seven performance objectives are identified. These can be used as a guideline for structuring the data protection requirements for the processing of personal data by a privacy management system. The protection goals are data minimization, availability, integrity, confidentiality, unlinkability, transparency and intervenability.

The technical design of the wearable, which can vary depending on the type, model and area of application, is then particularly decisive for the data protection analysis of a privacy management system based on these assurance goals. Monocular and binocular data glasses, for example, can use an integrated camera to record images, videos and sounds, which may also record third parties. Smartwatches, for example, can record a wide range of very sensitive data categories, from GPS coordinates to health data such as blood pressure and resting pulse.

When creating a privacy management system, it is essential to ensure that data processing is appropriate, relevant and limited to what is necessary.[24] In addition, employee data may only be stored for as long as necessary for the purposes of processing.[25] The restriction to the necessary extent is particularly relevant if the data is to be consolidated into a personality profile.[26]

In the interests of effective rights for the data subject, it should be possible for the processed data to be accessed directly through the privacy management system. In particular, specific data must be retrievable immediately when needed. Databases, data management systems and parallel search functions are suitable for this purpose.[27] In addition, it must be ensured that data can be restored in the event of any kind of system malfunction.

Furthermore, the system must be designed so that the employee data processed remains complete, correct and up-to-date.[28] Any deviation from

23 Standard-data-protection-model, id. 6.
24 *Roßnagel,* in: Simitis/Hornung/Spiecker, Datenschutzrecht/DS-GVO, Art. 5 note 118.
25 Standard-data-protection-model, id. 26.
26 *Martini,* in: Paal/Pauly, DS-GVO, Art. 25 note 50.
27 Ibid.
28 *Frenzel,* in: Paal/Pauly, DS-GVO, Art. 5 Rn. 39; Standart-data-protection-model, id. 26.

this must be detectable immediately so that the corresponding data can be corrected.[29] Technical and organizational measures must also be taken to ensure the appropriate security of personal data,[30] including that unauthorized persons do not have access to the data or the assistance system.[31]

In particular, if one wearable is used by several employees (for example, as part of shift work) the system must be designed so that personal data is not merged unless this is absolutely necessary.[32] This applies in particular if the merged data was collected for different purposes.

When giving consent and using the system, employees must always be able to understand which data is being collected and processed, when, and for what purpose.

IV. Conclusion

The use of digital assistance systems in industry and production is one of the many innovations that characterize technological progress in the context of Industry 4.0.[33] At the same time, this development also contributes to the fact that the workplace is becoming increasingly integrated into an environment of ubiquitous data processing. The introduction of privacy management systems can increase the acceptance of wearables and ensure that they are used in line with data protection requirements so that assistance systems can be integrated into Industry 4.0 on a long-term basis and in a legally compliant manner.

Bibliography

Astrid Auer-Reinsdorf and *Isabell Conrad*, Handbuch IT- und Datenschutzrecht, (C.H. Beck, 3rd ed., Munich 2019).

Martin Beckschulze and *Ivo Natzel*, "Das neue Beschäftigtendatenschutzgesetz", Betriebs-Berater (BB) 2010, 2368.

Wolfgang Däubler, *Peter Wedde*, *Thilo Weichert* and *Imke Sommer*, EU-DSGVO und BDSG (Bund-Verlag, 3rd ed., Frankfurt/M 2023).

29 *Standard-Datenschutzmodell*, S. 27; see *Dix* in: Simitis/Hornung/Spiecker, Datenschutzrecht/DS-GVO, Art. 5 note 20.

30 *Schantz,* in: BeckOK Datenschutzrecht/DS-GVO, Art. 5 note 36.

31 Recital 39 GDPR.

32 Standard data protection model, id. 26.

33 See *Hofmann*, ZD 2016, 12 (12).

Nikolaus Forgó, *Marcus Helfrich* and *Jochen Schneider*, Betrieblicher Datenschutz (C.H. Beck, 3rd ed., München 2019).

Kai Hofmann, "Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0 – Datenschutzrechtliche Besonderheiten und Herausforderungen", Zeitschrift für Datenschutz (ZD) 2019, 12.

Reinhold Kopp and *Karen Sokoll*, "Wearables am Arbeitsplatz -Einfallstore für Alltagsüberwachung?", Neue Zeitschrift für Arbeitsrecht (NZA) 2015, 1352.

Michael Kort, "Neuer Beschäftigtendatenschutz und Industrie 4.0", Recht der Arbeit (RdA) 2018, 24.

Jürgen Kühling and *Benedikt Buchner*, Datenschutz-Grundverordnung, BDSG (C.H. Beck, 4rd ed., Munich 2024).

Boris Paal and *Daniel Pauly*, Datenschutz-Grundverordnung/Bundesdatenschutzgesetz, (C.H. Beck, 3rd ed., Munich 2021).

Peter Schantz and *Heinrich Wolff*, Das neue Datenschutzrecht, (C.H. Beck, Munich 2017).

Maximilian Schnebbe, "Digitale Assistenzsysteme in der Industrie und Produktion", Datenschutz und Datensicherheit (DuD) 2020, 398.

Spiros Simitis, *Gerrit Hornung* and *Indra Spiecker*, Datenschutzrecht (Nomos, Baden-Baden 2019).

Gregor Thüsing and *Sebastian Rombey*, "Die 'schriftlich oder elektronisch' erteilte Einwilligung des Beschäftigten nach dem neuen Formerfordernis in § 26 II 3 BDSG", Neue Zeitschrift für Arbeitsrecht (NZA) 2019, 1399.

Gerling Wisskirchen, *Jan Peter Schiller* and *Jan Schwindling*, "Die Digitalisierung – eine technische Herausforderung für das Mitbestimmungsrecht aus § 87 I Nr. 6 BetrVG", Betriebs-Berater (BB) 2017, 2105.

Heinrich Wolff and *Stefan Brink*, BeckOK Datenschutzrecht/BDSG, (C.H. Beck, 45th ed., Munich 2023).

Heinrich Wolff, *Stefan Brink* and *Antje v. Ungern-Sternberg*, BeckOK Datenschutzrecht/DS-GVO, (C.H. Beck, 45th ed., Munich 2022).

Register of cases

ECJ, Judgment of 30 Mar 2023, C-23/21, ECLI:EU:C:2023:270 – Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium vs. Minister des Hessischen Kultusministeriums.

German Federal Labour Court (BAG), Judgment of 11 Dec 2014 – 8 AZR 1010/13.