CATÓLICA LAW REVIEW

VOLUME VII \ n.º 3 \ novembro 2023

DOUTRINA

Marc Engelhart
University of Freiburg

João Pedro Barione Ayrosa
Mestrando em Direito pela Humbold-Universität zu Berlin (Alemanha). Advogado

Vítor Gabriel Carvalho
Mestrando em Direito pela Pontifícia Universidade Católica de Minas Gerais (Brasil). Bolsista CAPES/PROEX

Roberta de Paolis
Post-Doc Fellow in Criminal Law at Sant'Anna's School of Advanced Studies, Pisa, Italy

Sofia Cabrita
Doutoranda em Direito e Assistente convidada. Universidade Católica Portuguesa, Faculdade de Direito, Centro de Estudos e Investigação em Direito

COMENTÁRIO DE JURISPRUDÊNCIA

Manuel Monteiro Guedes Valente
Doutor em Direito pela Universidade Católica Portuguesa

RECENSÃO

Germano Marques da Silva
Professor Catedrático Jubilado da Universidade Católica Portuguesa

UCP EDITORA

CATÓLICA LAW REVIEW

Digital Compliance – Legal tech as a driver for better prevention

Marc Engelhart
University of Freiburg

SUMMARY

I. Introduction

Compliance and digitalisation are two aspects that have become an integral part of everyday business life today. Digitalisation has taken hold of a large number of business processes in companies and other organisations. In some cases, it is already the main focus of activity, such as high-frequency trading in investment banking.[1] These organisational changes are accompanied by the increasing digitalisation of the legal framework in which these entrepreneurial activities take place. This regulatory framework has become increasingly important over the last two decades as it has been increasingly and systematically linked to business processes in the context of compliance, corporate governance and risk management. More and more digital solutions are being sought for in order to achieve compliance with this regulatory framework.

The development of digital solutions for compliance as well as for corporate governance and risk management combines numerous developments and disciplines that have often been considered separately in the past, as it involves not only the most diverse fields of law (primarily corporate and criminal law) and their empirical basis in criminology, but also economics (including business ethics), sociology and psychology and, above all, information technology and its technical implementation. In addition, there are numerous national and international regulators and authorities in this field who issue specifications that are only partly to be considered as hard law, but often come across as soft law and thus raise the question of how and to what extent they should be taken into account.

In order to understand and implement this ultimately very far-reaching area, especially in larger corporate units, digitalisation offers approaches that are better able to grasp this complexity than a purely manual/personal system and also to integrate it into everyday corporate life. Digital compliance has thus become a key driver of legal tech development in corporate practice.

II. Compliance, Compliance Programmes and Digital Compliance

The field of compliance is a development that has been shaping legal systems all around the world for about three decades now.[2] It has its origins in the USA. There, in 1993, the introduction of sentencing guidelines at the federal level for corporate sanctioning (§ 8 United States Sentencing Guidelines – USSC) made compliance an essential element in determining the corporate penalty

1 Mozzarelli (2022), p. 259; Schemmel (2021), p. 166.

2 See, e.g., on the development in Germany, Tiedemann (2017), paras. 12 ff.

(association penalty):[3] The core of the regulation is that an effective compliance programme can mitigate the penalty; moreover, the creation or improvement of a compliance programme can be imposed as a compliance penalty in its own right.[4] This has created an incentive for companies to avoid or at least mitigate sanctions by establishing compliance measures. This motivation of avoiding sanctions has even gained in importance in the corporate context, as numerous regulations have adopted the approach of the sentencing guidelines and explicitly require such measures, at least in part, as is the case, for example, for combating corruption in the American Foreign Corrupt Practices Act (FCPA)[5] or the British UK Bribery Act[6], as well as generally numerous standards of corporate criminal liability in European and non-European countries. In addition, compliance efforts are now recognised in the practice of numerous authorities and courts as part of sanction considerations beyond the explicit stipulation. Also, numerous stakeholders are now demanding a more rule-compliant and ethical behaviour than in the past.

What is compliance about? Compliance in the narrower sense is the observance of the legal provisions applicable to a company and its employees. Usually, compliance does not refer to all legal provisions but only to the most important ones, mainly including the criminal or regulatory liability of the company and its employees (criminal compliance).[7] Beyond the legal regulations, compliance can also include adherence to other requirements such as ethical concerns, technical standards, etc. (compliance in the broader sense). In many cases, however, such requirements cannot be strictly separated from legal requirements, as they can be closely interwoven with them, for example, if a criminal negligence standard is specified by industry-typical best practice standards, ISO specifications or international soft law recommendations. Hence, the range of topics covered by compliance can be very extensive. Which topics apply to an individual company depends on the individual corporate structure and activity. Regularly, corruption, antitrust law and anti-money laundering as well as data protection law are of major relevance.[8] With the digitalisation of the corporate infrastructure, the area of cybersecurity has also become very important. Individually, however, environmental criminal law or product safety regulations can also be of central importance for the company.

3 In detail Gruner (1994-2022), chap. 14; see also Engelhart (2012a), pp. 162 ff.

4 Engelhart (2012a), pp. 162 ff., 188.

5 See Engelhart (2020), pp. 479 ff.

6 See Raphael/Phillips, pp. 461 ff.

7 Cf. the Sentencing Guidelines in the USA, which relate compliance to the detection and prevention of criminal conduct, § 8 B 2.1 Cmt. 1. United States Sentencing Guidelines.

8 See in more detail Sieber/Engelhart (2014), pp. 38 ff.

At first glance compliance refers only to a matter of course, since the legal system expects compliance with legal requirements by the company and its employees just as it does by any other person. However, legal compliance in a company is much more difficult to achieve than if the normative command is only addressed to a single natural person, since in a company a large number of persons with a variety of activities and interests are connected. Risks inherent in business activity and, above all, group dynamic risks that can lead to a corporate climate that is (in)faithful to the law shape the corporate environment here.[9] The state of compliance in a company is therefore not readily given, maintained or, in some cases, even to be achieved easily. It is this state of compliance most efforts in practice and also in theory try to achieve. Compliance thus becomes a synonym for comprehensive measures that a company can take to ensure legal compliance and to avoid or uncover violations.[10] Compliance measure refers to individual measures, while the term compliance programme[11] refers to a bundle of measures as part of a more comprehensive overall concept.

The most difficult question in this context is how a compliance programme should look like. In some sectors specific requirements exist,[12] yet there often is no general regulation for compliance. In the absence of general legal regulations, the requirements in § 8 United States Sentencing Guidelines. which define the main elements of a compliance programme, continue to be an important point of reference for the creation of a compliance programme.[13] These are supplemented by the guidelines of the U.S. Department of Justice for the U.S. prosecution authorities.[14] In addition to these legal guidelines, there are now several sets of

9 In more detail, Engelhart (2012a), pp. 610 ff.

10 See, e.g., Gruner/Brown (1995-96), p. 737; Hauschka (2004), p. 257; Schneider (2003), p. 646.

11 The term has become widely accepted with different variants: for example, the American sentencing guidelines for companies in § 8 USSG speak of a compliance and ethics programme. As a rule, a "Code of Ethics" (synonym: Code of Conduct) as a formal document on behavioural guidelines and standards represents a part of a more comprehensive compliance manual and is thus a part of a compliance programme.

12 E.g., in Germany, securities trading law provides for some guidance in Section 25a of the German Banking Act (KWG) and Article 22 (2) of Delegated Regulation (EU) 2017/565 (also in conjunction with Sections 63 et seq. of the German Securities Trading Act (WpHG)), which refer to a compliance function to be established. The necessary elements of such a compliance function are described in more detail by the German Federal Financial Supervisory Authority in the "Minimum Requirements for the Compliance Function and Other Conduct, Organisation and Transparency Obligations (MaComp)" BaFin, Circular 05/2018 (WA) – Minimum requirements for the compliance function and further conduct, organisation and transparency obligations – MaComp v. 19.4.2018, amended on 10.8.2021, reference WA 31 – Wp 2002 -2017/0011.

13 Engelhart (2012a), pp. 163 ff, 733 ff.

14 For more details, see "Principles of Federal Prosecution of Business Organizations" in the Justice Manual (JM), JM 9-28.300 as well as JM 9-28.800, available at https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations (last accessed on 31.03.2023); see also the U.S. Department of Justice/Criminal Division's guidance, Evaluation of Corporate Compliance Programs (Updated March 2023), available at https://www.justice.gov/criminal-fraud/page/file/937501/download (last accessed on 31.03.2023).

rules from recognised organisations for implementation in practice, such as ISO 37301 of 2021, which has replaced the (non-certifiable) ISO 19600 of 2014 and offers an international standard for best practice in compliance management.[15] In addition, there are more specific requirements such as ISO 37001 for anti-corruption management systems[16] and also some national standards exist.[17]

Central to all these approaches is that only an effective programme is relevant, i.e., one that actually serves to prevent and resolve breaches of the rules. The aim is not only to prevent window dressing (i.e., the formal fulfilment of criteria while at the same time materially deviating from the requirements in order to pretend to be a good corporate citizen). It is also intended to illustrate the necessity of a compliance programme tailored to the specific company, since the needs can diverge significantly depending on the type of activity, size of the company, etc. It is not enough to simply implement a compliance requirement, but this must be individually adapted to the conditions found in the company. This means that compliance requirements are basically only framework obligations that need to be concretised and filled out.

In detail, compliance programmes comprise numerous components from risk identification to sanctioning of violations.[18] The starting point and central to all further measures are risk identification and analysis in order to be able to determine in the first place which specific risks for rule violations exist in the company. The next step is the risk assessment in order to evaluate the (numerous) risks according to their significance, frequency, type, etc. Based on this, the compliance code can be developed, which includes a written record of the relevant requirements that apply in the company. Then, a corresponding structure (compliance structure) must be developed, which clearly assigns compliance tasks to qualified personnel (a compliance officer or a compliance department). In addition, and this is usually the most complex area (often referred to in practice as the compliance management system), organisational measures must be taken to create compliance procedures. This entails taking the appropriate measures for each activity and task to prevent rule violations. It includes the creation of special approval and reporting channels, the introduction of the four-eyes principle, special systems for accepting gifts, etc. Screening of applicants must be provided for new hires. In addition, there must be appropriate

15 International Organization for Standardization, ISO 37301:2021 – Compliance Management Systems, April 2021, available at https://www.iso.org/standard/75080.html (last accessed on 31.03.2023).

16 See at https://www.iso.org/iso-37001-anti-bribery-management.html (last accessed on 31.03.2023).

17 See, e.g., in Germany, the auditing standard 980 on principles of proper auditing of compliance management systems prepared by the Institute of Public Auditors in Germany (IDW) available at https://www.idw.de/idw/verlautbarungen/idw-ps-980/43124 (last accessed on 31.03.2023).

18 See, e.g., Engelhart (2012a) pp. 711 ff.; Kahlenberg/Schäfer/Schieffer (2020), pp. 811 ff.; Moosmayer (2021), pp. 35 ff.

communication and communication of compliance requirements, which include not only information through appropriate platforms or helplines, training, but also the continuous emphasis on compliance by superiors (in speeches, staff meetings, etc.) as a tone from the top with the creation of incentives for compliant behaviour.

These preventive measures are complemented by appropriate controls, both as unpredictable spot checks and as a permanent system. This includes a reporting system for possible violations (often referred to as a whistle-blower hotline). Such control measures are already elements of the repressive part of a compliance programme, which comprises investigative measures (compliance investigations or internal investigations) and procedures in the event of possible compliance violations as well as sanctions and criteria for sanctioning violations. Finally, the compliance programme must provide for continuous evaluation and improvement of the measures. A programme cannot be static (created and implemented only once), but must be dynamically adapted to new findings (new risks, new legal frameworks, identified ineffectiveness of measures, etc.).

Hence doing compliance is a complex task, especially in large corporate structures having business in multiple jurisdictions. And here digital compliance has become more and more important. Digital compliance is the digitalisation of compliance structures,[19] in particular individual measures of a compliance programme.[20] The goal is to improve the effectiveness and also the efficiency of a compliance structure through technical applications. Digital compliance is very much about supplementing or replacing the complex elements of a compliance programme with digital applications or even creating new ones in areas where no such effective or efficient measures were previously possible. In this respect, digital compliance is closely linked to the structure of a compliance programme. This also means that there can be no general solution for an individual company, but that digitalisation must be specifically tailored to that company.

What makes the task of creating an efficient compliance program even more complex is the close relationship of compliance to corporate governance (the factual and legal regulatory framework for the management and supervision of a company),[21] corporate social responsibility (aiming to ensure that a company

19 Digital compliance is not the same as compliance with regulations on digitalisation such as cybersecurity or cybercrime regulations. Such regulations may be part of a compliance programme but are not necessarily linked to digitalised compliance structures.

20 Cf. Bräutigam/Habbe (2022), p. 809; Burchard (2021), p. 741; Engelhart (2023), chap. 16, Neufang (2017), p. 249; Schemmel (2021), p. 166.

21 See v. Werder, Keyword "Corporate Governance", in Gabler Wirtschaftslexikon, as of 27.11.2018, available at https://wirtschaftslexikon.gabler.de/definition/corporate-governance-28617/version-367554 (last accessed on 31.03.2023). Details provide, e.g., the "German Corporate Governance Code (DCGK)", available at http://www.dcgk.de (last accessed on 31.03.2023), or the G20/OECD Principles of Corporate

assumes responsibility for society and the environment beyond the minimum legal requirements) and risk management[22] asking which risks can jeopardise the achievement of corporate goals a company is exposed to in its day-to-day business operations and how to react to them with appropriate (in practice often very complex) measures[23]. With regard to compliance, there are overlapping areas in these approaches, especially in the area of corporate structures and legal risks. Also, corporate ethics plays a major role in the implementation of efficient governance, risk and compliance structures. As these approaches overlap and often only view the various corporate and legal areas and corporate processes from different perspectives there is an initial development to take an overall approach. For example, the GRC (Governance, Risk and Compliance) approach attempts to ensure an efficient and effective process of corporate activities in compliance with the law.[24] The aim is to integrate the various measures from corporate governance structures, risk management structures and compliance programmes into one system in order to dissolve parallel structures in favour of a more effective (and often more cost-efficient) overall approach.[25]

III. Digitalisation of individual compliance measures

As the overview of the compliance development shows, today the decisive question is no longer whether a compliance programme should be established in the company, but only how. Yet, the complexity of such a programme requires a high level of financial and human resources, especially if the focus is on

Governance, 2015, available at https://www.oecd.org/daf/g20-oecd-grundsatze-der-corporate-governance-9789264250130-de.htm (last accessed on 31.03.2023).

22 For more details, see Gleissner (2022), pp. 101 ff.

23 For implementation in practice, there are numerous sets of rules such as ISO 31000:2018 on risk management, the auditing standard 340 prepared by the Institute of Public Auditors in Germany (IDW) on the audit of the early risk detection system (within the meaning of section 317 (4) of the German Commercial Code (HGB)) and auditing standard 981, which describes principles of proper auditing of risk management systems by the supervisory board in accordance with section 107 (3) of the German Stock Corporation Act (AktG). The German Institute of Internal Auditing (DIIR) has published its own auditing standard for the audit of the risk management system: DIIR Auditing Standard No. 2 – Audit of the Risk Management System by Internal Audit, November 2018, available at https://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard_Nr._2_Version_2.0.pdf (last accessed on 31.03.2023).

24 See, e.g., Laufer (2016), p. 426; Laufer (2017), p. 417; see also Volkov (2013), pp. 1 ff.

25 See LegalHelix for a comprehensive approach that also includes foreign standards: https://legalhelix.com/ (last accessed on 31.03.2023); see also, e.g., SAP's integrated software, which offers a comprehensive governance, risk, compliance and cybersecurity solution, especially for the financial sector: https://www.sap.com/products/erp-financial-management/grc.html (last accessed on 31.03.2023) or the KPMG model to incorporate requirements from regulators, management and relevant stakeholders: https://home.kpmg/at/de/home/services/advisory/risk-consulting/risk-compliance.html (last accessed on 31.03.2023).

effectiveness. With digitalisation, there is the possibility of increasing effectiveness and at the same time being able to limit the invested resources.[26] This is particularly important where the duty of legality competes (or is seen to compete) with the generation of profits, especially when the focus (as often) is more on the more obvious preventive compliance costs than on the – sometimes considerably – higher repressive costs resulting from illegal behaviour.[27] Digitalisation offers opportunities particularly in the following areas of compliance programmes: in information management, in the dissemination of information, within the framework of the compliance structure, in control options and in documentation.[28]

1. Information Management

Digital information management has its first priority in digitising, as much as possible, existing information. This part of the digitalisation process is already well advanced ("paperless office"), although it depends very much on the industry sector. Only the digital capture and storage makes the information usable for further digital applications. This includes not only to have written documents available in digital formats, but also communication (e-mail and messenger services), as well as the recording of calls.

Digital creation or making documents digitally available (inevitably) requires an effective digital document management to make the information accessible. This task is by no means trivial, but it often does not really get much attention in practice. For example, different file formats (besides the common pdf, word and excel files, there are often specific data formats tailored for specific company usages) or different languages in the document can restrict or limit the information to be read and used for further digital usage. To that extent, the way information is digitised already has a decisive influence on the results of further document processing, etc. For basic access to the information, it is regularly not enough to store it digitally, it must be supplemented with context/reference information. In particular, summaries, tags, links, search modules, etc., enable a more effective use of the available information. If done properly, one main advantage is that information is accessible (especially via networks) to more people in different places than in the classic paper-based filing system.

26 See Rack (2016), pp. 16 and 58.

27 In any case, recourse to illegal behaviour for cost reasons is prohibited, but this must be emphasised again and again in practice. In the "grey area" of what is permissible, the question is often whether to invest in compliance measures or to accept possible repressive sanctions.

28 For a more comprehensive overview, see Engelhart (2023), chap. 16.

From a compliance perspective, this digitised company information is a decisive element on which to base digital compliance measures. But beyond this digital recording of work products another aspect of digitised information is of great importance for compliance: the (compliance) requirements to be met, especially the legal standards and legal obligations. The digital availability of these requirements is also necessary, to a large extent, for an effective corporate governance and (legal) risk management system. Yet, this task sounds much easier than it is in practice.

The starting points – and here the digital approach does not differ much from classic compliance approaches – are the legal and sub-legal requirements. Identifying the relevant regulations is by no means an easy task, as a large number of standards can apply to a company. A first step is to determine the relevant requirements for the company, which result from the basic risk analysis. In principle, this initial analysis can only be automated to a limited extent, but the digitalisation of company information is of great help here, as it enables an overall view of the company, its work processes and work products. Based on this analysis, many regulations that are not of greater relevance to the company can often be eliminated, but a large number of relevant compliance requirements still remain.

Such a collection of compliance requirements can only be effectively managed via database solutions and still remains a major challenge. For example, standards are often published in different organs, these are unsorted and must first be systematised. In addition, legal requirements in legislation are often rather general. In the case of abstract terms, general clauses, etc., the wording of the norm itself does not yet result in a clear and implementable requirement. Therefore, in many cases case law and its understanding of the norm is of great importance, especially if it defines relevant individual obligations. However, the inclusion of case law is not always unproblematic, as lower court decisions and sometimes even higher court decisions can only partially complement each other or even contradict each other in individual cases. Here, the inclusion in the database must already be carried out with great care.

In addition to the court decisions, there are numerous authority specifications which can be of importance, as guidelines or individual decisions such as in cartel and competition law often detail more abstract legal specifications. Finally, the legal literature can also be relevant; ranging from specific literature (for the company's industry) to general legal reading (such as the *Neue Juristische Wochenschrift* in Germany).[29] The literature can provide clues for interpretations and detailing (as well as valuable systematisation) of general specifications. In all these areas, development is constantly evolving, with innovations occurring

29 Rack (2016), p. 17, assumes approximately 56 scholarly legal articles per month are relevant for larger companies.

on a daily basis, resulting in a continuous effort to update the database. To that extent, a database is required that comprises not only the relevant legislation, but also timely legal updates from courts, relevant authorities and also from the literature.

A particular challenge in the legal field is the inclusion of regulations from several jurisdictions. Cross-border activities and a company/group structure that is anchored in several countries require the inclusion of numerous foreign (and possibly also supranational such as European) legal requirements. Since these requirements (e.g., for corruption, occupational health and safety, environmental protection) can vary from country to country, a compliance system must take this into account accordingly. In any case, the basis for an effective compliance is a sufficient recording of the requirements in a database. Here, again, the recording of legal standards alone is usually not sufficient, but the inclusion of judicial decisions or concretisations by authorities is required. This varies greatly from one legal system to another; in common law countries case law is more important than the actual legal text, in some countries such as China the legal text only becomes concretely applicable in practice through guidelines (e.g., from the supreme courts). In this area, a particular challenge is the timeliness of the system, but without regular updates ("global regulatory updates"), no effective transnational system can be established and operated. To that extent, the mere collection of such information with its updates is already a great challenge. Adding to this, various problems exist, such as linguistic: to make legal texts, etc., from national systems accessible to everyone in the company, translations (e.g., into English as a standard working language) are a first-choice solution. So, besides the original text, a database can provide a translation. Yet, and although translations are now possible by a variety of digital solutions such as Google Translate, DeepL, PROMT.One, MyMemory, babelfish.de or Bing Translator, translating legal texts remains a major problem. This problem is not new, but a general one in comparative law.[30] Yet, automated translation makes it easy to overlook a mistranslation of legal terms and can easily disguise important foreign legal concepts that might be of great relevance for conceptualizing the compliance program. To that extent, a thorough check by lawyers versed in comparative law remains essential in order to mitigate such translation risks.

In many cases, such a database provides a clear picture of the applicable regulations and the standards to be observed. However, there always remains a small number of rules from which no clear instructions for action can be derived (for example, because they are still too abstract without concretisation, unclear or even contradictory). These rules must be identified separately in order to be

30 See Engelhart (2012a), pp. 31 ff.; Schroeder (2005), p. 236; Weisflog (1996), pp. 20 ff.

able to establish an independent workflow for them, which, for example, provides for the observance of a certain procedure or the decision of a certain body such as the compliance department in individual cases in order to mitigate legal risks.

As such a legal database for a company is rather complex, it is worth considering whether several companies can share such a collection of law, i.e., whether it can be 'purchased' externally from a service provider.[31] This cannot be ruled out in principle, as specialised databases (such as juris or beck-online in Germany or Westlaw and Lexis Nexis for the U.S. and also other jurisdictions) already have a very comprehensive collection of case law and literature references (in some cases also literature is directly available electronically). Also, such information can be electronically imported into a company database, although this is often only possible to a certain extent as limitations for usage, copyright restrictions, etc., exist. However, such general external databases and solutions will only come into question to a limited extent, as effective compliance requires a solution that is truly tailored to the company, including a tailor-made legal database (with the selection of specific regulations and the determination of the concrete obligations for the company arising therefrom), as there is a danger that, on the one hand, a large number of regulations/standards that are not really relevant are included and, at the same time, the focus is not really on the central standards and behavioural requirements for the specific company, especially when legal changes occur.

In addition, only an internal solution really enables further and comprehensive reuse within the company. Information management only becomes a central element for the compliance structure when the information collected is processed and evaluated for company-specific purposes. This is the next step to go beyond recording and storing information and, thus, beyond the mere database function. In regard to the legal obligations it is closely connected to the collection of information, as knowing the purpose determines the search for the relevant regulations, etc.

The main step is to filter the legal information and specially to make clear what should be done by whom when and where. One of the first steps is to determine the scope of the obligation. This is necessary in many cases as the legal requirement often applies to several constellations and tasks within the company. At this stage it might be useful to make certain clusters for typical company tasks or products and link the requirement to these tasks and products. This question is also closely connected to whom the obligation applies, which might be senior management, just a group of people such as sales representatives, or

31 Rack (2016), p. 60 is generally in favour of this.

it might also apply to everyone. Often the obligation can be attributed to certain roles in the company, such as IT specialists, warehouse managers, research managers, plant doctors, etc. In many cases the obligation does not only affect one task or one person but also several, sometimes with a whole department behind it, so that the group of persons affected has to be determined. The main step here is to translate a legal requirement into the different tasks of a company. Within a dabase system, this can be done right from the start when a regulation is added to the database and this is especially valuable for legal updates as it enables the persons concerned or dealing with the task to directly have access only to the information relevant for them. The main asset, however, is not the possibility to have easy access to this filtered information, but the possibility to automatically inform the person about changes and, e.g., open an implementation workstream, assign implementation tasks, etc., for this specific new development.

The crucial aspect here is a reliable 'translation' of the general legal obligation into company tasks. For this step judicial expertise is needed as the regulation has to be evaluated and its scope has to be determined. An effective compliance structure can only be built if the legal obligation is understood correctly and broken down into manageable pieces for everyday work. In this field a special digital compliance service industry is in the making, supporting companies with the necessary legal expertise that is often not available within companies (as, e.g., when the company works in different jurisdictions but has no lawyer knowledgeable in the corruption laws of the different states). Therefore, external service can be useful when a service provider monitors the relevant regulatory sources and analyses them in regard to relevant changes. This means specifically that one has to identify new regulations (or the update of an existing one), to determine which of the regulations contain obligations. It can also be useful to differentiate according to the nature of legal regulations, e.g., between administrative and criminal obligations and thus consider the seriousness of consequences in case of a breach of the obligation. Also, external services can specify the obligation by determining (and adding this information to the data base) for what tasks and for whom the new regulation is of importance. The next step would be to determine exactly which department(s) within the company and which internal person(s) that have to deal with the changes; this is then best done by the company itself in cooperation with the external partner, merging the legal expertise with the corporate knowledge. In this regard digitalising implementation structures can be of great help and substantially reduce the number of occasions external expertise is required. An ideal cooperation structure would be a kind of permanent and automatic subscription service, where the service provider and the company have jointly determined for what tasks and fields the company needs legal updates

and then the service constantly and continually provides this information to the company. If desired, the service provider can upload the updates directly into the company's software system. In practice, such services already exist, yet are often still limited in scope (such as being restricted to the financial industry) and very often also in regard to the jurisdictions covered.[32] Especially the coverage of several jurisdictions has only recently come into focus.[33]

Covering the transnational dimension by digital means poses not only a great challenge but also offers new ways for a – what it is in substance – comparative law analysis. A solid analysis is the basis for programming compliance standards in a software to be used then in the corporate structure. Basing the programme code on just one legal system (be it the one with the highest requirements, the one of the parent company, etc.) – as often done – is an easy approach but leads to either over- or undercompliance, but not to really effective compliance. A clear picture of similarities and differences and, at best, a synthesis of the multiple rules, a transnational cross-section of specific norms and behavioural obligations (e.g., with regard to corruption norms, cartel requirements…) is necessary. This has always been the core business of legal comparison and such a comparative law analysis has always been a complex task.[34] Digital approaches can be of great value here. Scientifically and in practice, such digital comparative law is still in its early stages. But the changes in technology have triggered important developments: promising starting points have been laid by *Sieber* in comparative criminal law,[35] quantitative comparisons (especially in economic law) have been done with the approach of statistical comparative law[36] and last but not least the broader endeavour to analyse law and the legal field by quantitative methods and thus combine data processing and the law ("quantitative jurisprudence")

32 See, e.g., RADAR from the VÖB Service, that specialises on regulations from Germany, Austria, Swiss, Luxembourg and the EU for financial institutions, see https://www.voeb-service.de/informationsdienste/radar-produktfamilie (31.03.2023). See also the compliance-management-system "Recht im Betrieb" by Rack Rechtsanwälte that comprises a large number of mainly German administrative regulations (see https://rack-rechtsanwälte.de/seiten/compliance/compliance-management-system/compliance-management-system – last accessed on 31.03.2023).

33 E.g., LegalHelix is one of the few more comprehensive systems, see https://legalhelix.com/ (31.03.2023). A more complex system is also provided for by the LexisNexis® WorldCompliance™ Data that deals with collecting information worldwide on watchlist screening, financial crime compliance and anti-bribery requirements, https://risk.lexisnexis.com/products/worldcompliance-data (last accessed on 31.03.2023).

34 Just see Eser (2017), pp. 83 ff. on the various methodological problems and approaches.

35 For such early considerations on an information system for comparative criminal law, see Sieber (2006), pp. 78 (124 ff., 131 ff.) who has also initiated an online database, run as a test system, on the general principles of criminal law from up to 28 countries, which is accessible at https://infocrim.org/ (last accessed on 31.03.2023).

36 Siems (2008), p. 354. See also Kischel (2015), pp. 144 ff.

offers possibilities that go beyond the common normative legal interpretations.[37] The aim of all these approaches is to handle complex legal information and to get faster and better (or at least additional) results than by doing the analysis and comparison manually.

A database that includes the legal information and where the information is prepared in such a way that it is broken down to concrete tasks and people, is the ideal starting point for a direct link to the internal compliance structure. So, every regulation can be linked to the point in the company where it becomes relevant.

2. Digitalisation of the compliance structure

a) Basic compliance structure

The core element of a compliance programme is a comprehensive company-wide compliance structure. In a digital compliance structure, not only are process flows (largely) digitalised, but the relevant compliance aspects are also integrated into these tasks and processes: that is, for each process it is clear which regulations are relevant from a compliance perspective. The identified (legal) obligations are directly linked to the relevant processes and tasks. This also has advantages in the event of changes in (legal) requirements. Whenever changes occur (such as new legislation, new court decisions, new corruption risks in certain countries), these are first recorded in the information system. However, through the link to the process flows, this information can be immediately transmitted to the specific place and the task for which it is relevant. This also makes it possible to inform the respective employees immediately.

Beyond this aspect of digitalising company and legal information and timely updates about the legal situation other digital developments have become of great importance in practice. These developments often concern single measures and aspects and are therefore easier to implement than a comprehensive compliance approach. Among possible measures are automated document creation with specific workflows, automated approvals, e-signatures, etc., which all can be integrated into a more complex digital compliance structure.[38] In this way, the specification of certain contents for contracts, etc., individual modules or regulation types for documents can be designed in a compliance-compliant manner. It is also easy to set up requirements for special decision-making

37 See Coupette (2018), p. 379; Coupette/Hartung (2022), p. 935.

38 There are numerous providers on the market, e.g., Legito offers such a smart document approach, https://www.legito.com/ (last accessed on 31.03.2023).

processes, for example, if specific persons have to be involved or specific information has to be consulted in case of high-risk financial transactions (based on the high volume of the investment, etc.). The same applies to the area of anti-corruption in the acceptance of gifts and hospitality, which can be digitised with regard to admissibility checks, approval processes, etc. In a digitised environment, such processes can be made easily available at every place, so that for example smartphone appliances can enable corruption checks for managers on business trips, etc.

An advantage is that digital solutions are largely independent of the structure of the company, whether it follows a strongly hierarchical horizontal division of labour, a vertical division with emphasis on the difference between leadership and execution of work, or relies on lean management. The only thing that matters is that process flows and the tasks of individual process participants are clearly defined, that the necessary digitalisation of the process flows is in place and that these processes and tasks are linked to compliance requirements (and hence the legal background). In this structure, managers are generally involved with more comprehensive tasks and more far-reaching competences, and they also receive more compliance-relevant information. This corresponds to the approach under company law and criminal law of the special management responsibility of managers.[39]

In this digital compliance structure, a delegation (or assignment) of duties can also be easily done and is clearly evident: the comprehensive compliance programme of the company is specifically broken down into to specific tasks and assigned to individual (or several) responsible employees. Duties can be personalised with this assignment. In this way, relevant changes in compliance requirements can be specifically assigned to certain tasks as well as persons, so that an immediate implementation of changes is possible.

Digitalisation also makes it easy to record which compliance information was held by whom at which time and which compliance tasks were performed by whom during which period. These aspects can be stored and thus also be proven by this documentation if, for example, compliance with certain (legal) duties is questioned in civil, administrative or criminal proceedings. Knowledge of legal obligations, responsibilities and measures taken is thus clearly traceable. This is especially true for the aspect of information exchange. With digitalised processes, an exchange of information between certain levels, persons, departments, the head office and foreign subsidiaries is thus clearly recognisable and can be

39 For example, under German law the lack of organisational measures to prevent crime can constitute a breach of the duty of supervision according to sec. 130 OWiG (Ordnungswidrigkeitengesetze) and is one of the most important triggers of corporate liability according to sec. 30 OWiG. See Engelhart (2012b), p. 166 and for details Engelhart (2017) pp. 1161 ff.

documented. Digitalisation also makes it possible that not only the result of a work process or a task is visible and communicated, but also that the current processing status is recorded, retrieved or displayed (in real time). This enables managers, for example, to see whether a task has been tackled in time, has been sufficiently processed or is overdue. The different tasks and the current status can thus also be displayed in real-time for supervisory purposes, e.g., for the compliance department or also for the responsible executive on the board of directors, etc.

The clear definition of tasks and processes necessary for compliance also promotes the analysis of redundancies or superfluous task assignments, which, when optimised, can make a compliance programme not only more effective but also more efficient overall.[40] For example, it should be regularly checked to whom exactly a certain compliance task is assigned/delegated, whether there are still possible standardisations and/or typifications of tasks and processes and, above all, whether the technical possibilities for the digitalisation of various facets of the task, etc., are known or actually used. It will regularly become apparent that numerous legal compliance requirements demand parallel processes, checks and audit results, so that multiple labour-intensive audits, etc., can be avoided through a systematic compliance approach.[41]

b) In particular: digitalisation of decision management

With the digitalisation of internal processes as well as control measures, there are also more comprehensive possibilities (especially for supervisors at all levels) to make decisions based on informed and up-to-date information.

In this way, not only can relevant information be made available in real time, but the responsible office can also be informed about relevant changes and events by means of a corresponding information system. These can be indications of legal changes (at this point the system is connected to the legal updates), but also other digitally based information sources such as conspicuousness during digital (automated) document review, indications of possible criminal offences via the whistleblowing system, etc. The indications can be prioritised (automated alerts for specific important incidents). Also, the information can be prioritised (automated alerts with "yellow or red flags") and sent to the responsible persons (compliance department, management, etc.) depending on the type and urgency. With corresponding confirmation requirements (read confirmation, etc.), it can also be proved that information has been received and

40 See Rack (2016), p. 19.

41 See, e.g., Rack (2016), pp. 19 f.

when, which can often be relevant for civil and criminal proceedings. All in all, digitalisation can make an important contribution to ensuring that the company management in particular makes an informed decision, which is for example required by German company law (see section 93 (1) sentence 2 of the German Stock Corporation Act – AktG).

Furthermore, this information function can be used for an ongoing risk analysis of the identified core risks, as the compliance system is oriented precisely towards these risks. The digital possibilities to obtain and analyse relevant information here facilitate the necessary evaluation of whether the established system is working and how it should be adapted if necessary. This achieves a monitoring of the system as such (which, in addition to an external evaluation, can make a significant contribution to permanent further development).

Beyond the information function, AI can be established as an aid in forecasting decisions. By their very nature, these are forward-looking business decisions in which there is a great deal of leeway on the basis of the business judgment rule. Nevertheless, these decisions are relevant to the question of compliance, especially retrospectively, when a risk has materialised and led to the commission of a crime, for example. The question then arises as to whether the decision should have been made in this way (or has exceeded the limits of discretion). In this regard, it is not only about the aspect of an informed decision at management level, but also about the factual correctness of this decision. And in this area of decision-making, AI can provide valuable input as an additional decision-making aid; however, the complete delegation of these decisions to an algorithm, i.e., comprehensive decision outsourcing, will not be permissible.[42] The advantage of AI is that it has comprehensive capacities (and possibilities) to analyse (vast sets of) data, to evaluate them in self-learning processes and to show concrete proposals or options for action (or to exclude certain actions). It is even discussable if there is an obligation to use algorithms as this may often be a way (or maybe the only way) to include a "neutral" opinion (not guided by human interests of purpose and power) for critical decisions.[43]

A special area for extensive digitalisation in companies is also that of a group structure that often extends beyond national borders. Different national legal requirements, management cultures, etc., make it difficult for the parent company to manage the group accordingly. Contrary to what is sometimes assumed, a group structure also does not exempt subsidiaries from (criminal) legal

42 See on this aspect of the digitalisation of board duties in corporate law Möslein/Lordt (2017), p. 793, and Möslein (2018), p. 204. See also Spindler (2018), p. 17.

43 See Möslein (2018), p. 209; Spindler (2018), p. 43; Wagner (2018), p. 1099.

responsibility.[44] This applies not only to German law, but also to transnational or extraterritorially applicable regulations such as the FCPA or UK Bribery Act. Therefore, in these areas it is particularly important that there is a corresponding flow of information from the subsidiaries to the parent company, that risks are recognised there at an early stage and that they are responded to. Global group structures therefore require a global compliance programme, for which digital approaches are particularly suitable.

This topic is sometimes closely connected to supply chain management, where an increasing number of regulations as hard and soft law require a clear picture of the legal and actual situations of other entities a company works with (see also below). Often the foreign subsidiary (and not the parent company) has the contacts and agreements with entities in the respective state, so that the compliance measures of the parent company must also consider any connections of the subsidiary in the state the subsidiary is located (and of all states where business of the subsidiary is done). This makes compliance from the perspective of the parent company even more complex.

c) In particular: digitalisation of 'evidence'

Digitalisation can also be used and often is already used to record, control and document, above all, those processes for which certain proofs are necessary. This includes "classic" forms of access control, when only certain persons should have access to certain rooms or devices, but also to certain documents or information. For example, it can be of great importance which devices, information, etc., are currently in which place, or who has or has had access to these items (which can be relevant in internal investigations, for example). This not only helps to secure certain valuable assets, but also ensures that such items do not fall into the hands of unauthorised persons who should not have access, e.g., for antitrust reasons or to protect business secrets.

In certain areas, complete and uninterrupted proof of communication or transactions is also important. For example, for effective prevention of money laundering or corruption, it is often necessary to record donors, payment channels and recipients transparently and completely. Similarly, the complete recording of communications (whereabouts) for a particular project or product can provide the transparency needed to avoid even the appearance of corrupt behaviour. In addition to compliance with legal requirements, transparency and proof of a certain use of funds for certain stakeholders can also be a central motive, such as in the case of donations for a specific purpose, where all stages

44 See explicitly Schemmel (2021), pp. 166 ff. as well as in more detail Kress (2018), pp. 44 ff.; Minkoff (2016), pp. 64 ff.

from the payment to the concrete use of the project can be traced.[45] In these areas, the blockchain process opens up new possibilities for proof.[46]

A particularly important area of complete verification has arisen as a result of supply chain management requirements. Former soft law or just self-regulatory rules are more and more put into hard law, such as those now provided for in the German Supply Chain Sourcing Obligations Act (LkSG) of 2021.[47] These legal obligations extend far beyond the company's own sphere of business; as a rule, suppliers worldwide are involved, who must fulfil certain criteria (such as compliance with basic human rights, environmental and production standards) and the company as a business partner must monitor the contractual partner. Here, digital systems offer solutions for an effective and efficient implementation of these requirements that go far beyond on-site monitoring.[48]

d) In particular: digitalisation of prevention

A digital compliance structure also opens up the possibility of evaluating the information collected in real-time not only with regard to compliance with the tasks and processes as they were initially defined. Additionally, especially on the basis of self-learning algorithms, a continuous and continuously improved risk analysis can also be carried out, which identifies emerging breaches of rules and thus also may make them preventable.[49] For such an analysis, sufficient and relevant data must be aggregated, modelled and evaluated.[50] In particular, relevant information can be collected with behaviour-relevant data such as GPS tracking, telephone recordings, tracking of the use of electronic devices as well as the overall use of electronic performance monitoring (which can go as far as the implantation of computer chips).[51] Collection and analysis raise difficult questions about the legal borders of such use of data; especially in the case of personal data, this is only possible within the limits permitted by (European) data protection law.

45 See for example the SmartAid software from Datarella: https://datarella.com/smartaid-traceable-donations/ (last accessed on 31.03.2023).

46 See for the example of the fight against corruption: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (2020).

47 See Gesetz über die unternehmerischen Sorgfaltspflichten zur Vermeidung von Menschenrechtsverletzungen in Lieferketten – Lieferkettensorgfaltspflichtengesetz (LkSG) of 16 July 2021, BGBl. I p. 2959.

48 See, e.g., Prewave that offers monitoring of supply chain partner by screening information from social media of the partners and offering risk warnings, see www.prewave.com (last accessed on 31.03.2023).

49 See Neufang (2017), p. 249 for a detailed discussion.

50 Neufang (2017), pp. 251 ff.

51 Burchard (2021), p. 747.

The approaches for such future predictions are still in the development phase, but in further development they could use predictive and prescriptive analyses of complex data to identify the future commission of crimes in real time, or at least at an early stage and thus also help prevent them.[52] In this area, the approach overlaps with state predictive policing developments, which in the area of police authorities attempt to predict the commission of crimes through digital analyses.[53] In the corporate context, the focus has so far been mainly on combating money laundering and corruption.[54]

e) In particular: digitalisation in recruitment

Compliance also regularly includes checking those persons who are to work for the company, whether as employees (often referred to here as "onboarding") or as business partners. Here, a digitalised check of these persons with regard to previous relevant criminal activities, their listing on sanctions lists, PEP lists,[55] blacklists, watchlists, etc., has become an established practice;[56] in some cases, information and certificates of relevant degrees, experience and activities are also checked. Especially in the case of the screening of business partners, it is not only a one-time check at the beginning of the cooperation, but also a continuous (periodic or permanent) monitoring, as in the case of inclusion on sanctions lists, which are constantly updated.

3. Digitalisation of control

Finally, digitalisation offers an optimal area of application for the monitoring of internal company processes. To the extent that the compliance system is digitised and internal company processes are assigned to specific compliance requirements, it is possible to monitor whether and to what extent certain tasks are really being carried out. This control aspect complements the information,

52 See Schemmel (2021), pp. 166 ff., as well as Neufang (2017), p. 252, who refer to preparatory acts for insider trading and market abuse as examples of application. See also Burchard (2021), p. 747; Mazzacuva (2021), p. 150.

53 On predictive policing in the workplace, see Rudkowski (2019), p. 72 and also Dzida (2017), p. 541. On predictive policing in general, see Heilemann (2021), p. 49; Rademacher (2017), p. 366.

54 See Mazzacuva (2021), pp. 150 f.; Simões Agapito/de Alencar e Miranda/Xavier Januário (2021), p. 87.

55 This concerns politically exposed persons (PEPs), which in essence refers to politicians or a person working in the immediate environment of a politician who may be subject to heightened requirements with regard to money laundering and terrorist financing.

56 ComplyGate, for example, offers solutions for such background checks, cf. https://www.complygate.co.uk/ (last accessed on 31.03.2023).

the documentation and the risk assessment function already mentioned. Control measures can be implemented digitally as a query on demand, as a display when certain events occur (display of alerts with red or yellow flags) or, for particularly important issues, as a live display, so that continuous monitoring is opened up. This makes it possible to identify, clarify and, if necessary, eliminate discrepancies in a timely manner. Various escalation levels can be implemented here (also with a strict need-to-know principle for certain critical events, so that secrecy can be maintained to a large extent); control messages can also be automatically evaluated and linked to automatic remedial measures (or procedures). In particular, in decentralised structures such as corporate groups, the separate and often globally distributed entities such as the parent company, headquarters, subsidiaries, etc., can be connected and automatically involved in an overall control system.

Concrete control measures include, for example, who has access to certain sensitive areas, when and how which is, for example, important for the protection of business secrets. Such access controls might comprise video surveillance/face recognition or chip card/smartphone access also documenting which person had access at what time. In addition, access to certain documents and files/folders can be recorded in detail.

Another tool that can be implemented digitally without any problem concerns whistleblowing systems. In principle, these are possible as a simple hotline by telephone or by setting up a special email address. However, in order to protect the whistleblower, the company and also incriminated persons, a more complex workflow can be set up, which efficiently enables (also anonymous) communication with the possibility of asking questions back, etc.

Particularly extensive and intensive control measures are possible when analysing existing digital data. In contrast to paper-based file management and archiving, these data are much more easily accessible and can thus also be analysed with regard to special incidents. The analysis can be done on an ongoing basis, for example, to identify anomalies in transactions that deviate from regular operations. Without a digital solution, the time-critical detection of possible violations and security breaches is hardly possible. In addition to this ongoing analysis, there are many possibilities in the context of concrete suspicions within the framework of compliance/internal investigations, whereby the search (for corrupt processes, for example) can be much more specific than during a general/permanent screening.

The use of AI plays a significant role here, especially with self-learning algorithms. Here, AI can recognise patterns that would not have been seen during a manual check, as basically only 'known' patterns are searched for. In addition, going through large amounts of data is much faster than doing it manually (and

sometimes is only possible in a digital way when the amount of data is large). In day-to-day operations, this has often meant that only spot checks could be carried out. With the digitalisation of these tasks, a wide area can now be monitored continuously. In compliance/internal investigations, a large number of legal experts were previously employed to review and evaluate relevant materials (such as communications and working documents). This review can be achieved to a large extent through a digital solution, which can not only reduce the extensive use of external consultants significantly but also provide for a much more comprehensive research.

A special area of IT forensics is emerging for such screenings in regard to the handling of large amounts of data (big data).[57] The technical challenge in compliance applications (as in many other areas of big data analysis) is the handling of large, complex and diverse types of data, most of which are of varying quality and come from different sources. In the company, however, there is a certain advantage in that self-generated data basically follow uniform specifications. If this is not yet the case, data collection and processing can be designed within the framework of the digitalisation of compliance in such a way that these data can then also be used for high-quality big data analysis in terms of content and technology. Of course, such measures themselves must remain within the framework of the applicable requirements (first and foremost those relating to data protection).

4. Digitalisation of the documentation

An essential advantage of digitalisation (which has already shone through several times in the previous aspects) is the comprehensive possibility of documentation and archiving.[58] The obligation to document is legally provided for in some areas (such as in tax law), in other cases documentation is prescribed internally or is a factual necessity, as it is required for auditing, for example (audit-proof documentation). In addition, from a sanction's perspective, documentation is often the only (or at least the most reliable) way to provide evidence of a certain behaviour (fulfilment of certain obligations, etc.). In this respect, "not documented, not done" often applies.[59] The digital (automatic) recording of the

57 On the term and its use, see De Mauro/Greco/Michele (2015), p. 97. More detailed for the use in the corporate context Meier (2016), pp. 105 ff.

58 For various offers, see, e.g., the automated documentation system of various types of communication from proofpoint, https://www.proofpoint.com/us/solutions/modernize-compliance-and-archiving (last accessed on 31.03.2023).

59 See Rack (2016), p. 64.

processes enables a longer-term storage and thus also the retrievability and traceability of the respective process at any time.[60] In this way, accusations of inactivity (which from the perspective of criminal law can be regarded as an act of omission and, e.g., under German law, can constitute an administrative offence of a breach of supervisory duty according to sect. 130 OWiG) can be refuted. Of course, in individual cases, this documentation can also create evidence that internal investigators and state prosecutors can access to prove violations (which might not be provable without documentation).

5. Information transfer

Lastly, digitalisation is a vital means for communicating compliance-relevant information. and has substantially improved the situation compared to the pre-digital age. Compliance requires that every employee in the company is aware of the regulations that must be observed. It is particularly important that the individual employee knows, understands and can apply the regulations that are relevant to him or her. The more specialised the field of activity, the more specific (but usually also more limited) are the regulations to be complied with. In order to be able to determine the regulations relevant to the individual workplace, it is necessary to have a concrete job description of which activities are carried out by which persons.

When teaching compliance requirements, it is often important to include other concerns such as ethical considerations (and thus approaches to corporate ethics, business ethics, etc.), since ultimately the goal is not formal compliance with rules, but the correct action in terms of content. Here, the teaching of compliance requirements often overlaps with the equally important aspects of corporate governance and corporate social responsibility.

Digitalisation offers extensive possibilities for communicating the relevant compliance content. These include 'classic' query options in the databases, but also more modern communication offerings such as helpdesks and helplines with the compliance department. Chatbots, for example, can also be used for simpler compliance enquiries.

In addition to these classic access options to information sources, the (more modern) focus is primarily on active knowledge transfer. This concerns the extensive field of digital training (compliance training), which can be individually tailored to individuals.[61] The starting point is of course the communication of

60 See Burchard (2021), p. 746.

61 See for example ComplyGate's E-learning offerings in the areas of anti-corruption, data protection, antitrust law and money laundering prevention, https://www.complygate.com (last accessed on 31.03.2023).

the regulation, but it must be done in a way that makes clear what the scope of application and the concrete significance for the activity of the respective individual are. This means that, for example, a genuine transfer of knowledge and a real understanding of the norms should be achieved with case constellations, etc. beyond the mere text of the law. Digital approaches offer possibilities that go far beyond classical ways of imparting knowledge, such as group trainings, with not only an addressee-appropriate recording of the state of knowledge and the possibility of an addressee-appropriate presentation (which can be adapted depending on the state of knowledge, field of application, etc.), but also with defining and implementing individual learning objectives. Individualised digital training is flexible and can be taken at any time at the workplace and can be done also on a permanent basis (e.g., the achieve certain learning goals over a longer period of time). The same applies to the integration of checks to see whether the learning objectives have been achieved. With self-learning elements, a modular learning programme can be established that is designed for repetition and can be adapted to the individual learning pace. Achieved goals can be clearly documented (with certificates, etc.) and thus also serve as clear proof of the company's communication of the compliance requirements.

IV. Conclusions

Digitalisation enables measures in compliance programmes that are significantly more comprehensive, effective and efficient than classic compliance approaches and go beyond them both qualitatively and quantitatively.[62] In this respect, the dynamic development of legal tech has substantially advanced compliance efforts to adopt preventive measures, in particular to prevent criminal offenses. At present, the full potential of digitalisation is not yet being fully exploited. Current practice tends to focus on digitising single compliance elements. However, the path to a comprehensive digital compliance programme is no longer in the distant future, as the technical capabilities are already largely in place. Overall, the digitalisation of compliance allows a company and its employees to (once again) focus on their core concern, namely the pursuit of the company's goals.

However, when implementing digital compliance, it is important to remember that what is technically possible can only be within the bounds of what is also legally permissible. This means that when implementing digital compliance, great importance must be attached to issues such as data protection (especially

62 Burchard (2021), p. 748.

when processing personal data) and – from a more general perspective – the rights of those affected by the compliance measures. In particular, the inclusion of employees' personal data is only permitted to a limited extent under the European data protection law, even if this is sometimes permitted to a much greater extent abroad.[63] This is where digital compliance dovetails with privacy tech. In addition, neither employees nor partners of companies want to be transparent, so data security must also be sufficiently guaranteed. Furthermore, copyright issues can be relevant when data from other providers are included for the purpose of internal big data analysis.[64]

Such reservations apply in particular to control measures, where it must be ensured that only legally permissible analyses and measures are carried out. The application of compliance measures must not itself lead to a breach of the law. This means that in the case of (especially secret) monitoring measures, the personal rights of the employees concerned or even of third parties must be sufficiently taken into account.

However, even if the legal framework for compliance measures is observed, not everything that is legally permissible and technically possible is also entrepreneurially opportune. The level of control that compliance measures enable can also be counterproductive. Compliance basically shall thrive on a positive, law-abiding attitude on the part of those involved. However, the kind of comprehensive monitoring that is now possible, especially through digitalisation, may indicate a fundamental mistrust of those involved (the employee is seen as a risk) and can make them an object of mechanisation.[65] It is therefore important to strike a balance between the possibilities of positively communicating compliance relevant content and reinforcing adherence to norms on the one hand, and monitoring elements on the other. After all, more monitoring does not necessarily mean more compliance.

63 Most striking and far-reaching is probably the social credit system in China, which also places special compliance requirements on companies with regard to the 'screening' of their employees, see Kowallik (2021), p. 252.

64 In the case of big data analyses, digital compliance, as with other such procedures, is based on data quality and the choice of algorithms must be made carefully. See Hoeren (2016), p. 8 for a general discussion of these aspects.

65 Cf. Neufang (2017), p. 254: "The individual degenerates into a data set."

Bibliography

Bräutigam, Peter & Habbe, Julia Sophia (2022). "Digitalisierung und Compliance – Rechtliche Herausforderung für die Geschäftsleitung", *Neue Juristische Wochenschrift*, 809-814.

Burchard, Christoph (2021). "Digital Criminal Compliance", in *Digitalisierung, Globalisierung und Risikoprävention: Festschrift für Ulrich Sieber*, Engelhart, Marc/Kudlich, Hans/Sieber, Benjamin (eds.), Duncker & Humblot, Berlin, pp. 741-755.

Coupette, Corinna and Fleckner, Andreas M. (2018). "Quantitative Rechtswissenschaft", *Juristenzeitung*, Vol. 73, 379-389.

Coupette, Corinna & Hartung, Dirk (2022). "Rechtsstrukturvergleichung", Rabels *Zeitschrift für ausländisches und internationales Privatrecht*, Vol. 86, 935--975.

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (ed.), *The potential of distributed ledger technologies in the fight against corruption* (2020). Available at https://www.giz.de/de/downloads/Blockchain_Anticorruption-2020.pdf (last accessed on 31.03.2023).

Eser, Albin (2017). *Comparative Criminal Law*, C.H. Beck, Munich.

De Mauro, Andrea, Greco, Marco & Grimaldi, Michele (2015). "What is Big Data? A Consensual Definition and a Review of Key Research Topics", *AIP Conference Proceedings*, Vol. 1644, pp. 97-104, https://doi.org/10.1063/1.4907823 (last accessed on 31.03.2023).

Dzida, Boris (2017). "Big Data und Arbeitsrecht", *Neue Zeitschrift für Arbeitsrecht*, 541-546.

Engelhart, Marc (2012a). *Sanktionierung von Unternehmen und Compliance*, 2nd ed., Duncker & Humblot, Berlin.

Engelhart, Marc (2012b). "Corporate Criminal Liability and Compliance in Germany", in *Corporate Criminal Liability and Compliance Programs, First Colloquium,* Fiorella, Antonio and Stile, Alfonso Maria (eds), Jovene Editore, Napoli, pp. 167-206.

Engelhart, Marc (2017). "§ 130 OWiG", Wirtschaftsstrafrecht. Kommentar, in: Esser, Robert/Rübenstahl, Markus/Saliger, Frank/Tsambikakis, Michael, Otto Schmidt, Köln, pp. 1161-1178.

Engelhart, Marc (2020). "Vereinigte Staaten von Amerika", in *Antikorruptions-Compliance*, Busch, Markus/Hoven, Elisa/Pieth, Mark/Rübenstahl, Markus (eds.), C.F. Müller, Heidelberg, pp. 479-507.

Engelhart, Marc (2023). "Digital Compliance", in *StichwortKommentar Legal Tech*, Ebers, Martin (ed.), Nomos, Baden-Baden.

Gleissner, Werner (2022). *Grundlagen des Risikomanagements*, 4th ed., Vahlen, Munich.

Gruner, Richard (1994-2022). (loose-leaf), *Corporate Liability and Prevention*, LexisNexis.

Gruner, Richard & Brown, Louis (1995). "Organizational Justice: Recognizing and Rewarding the Good Citizen Corporation", *The Journal of Corporation Law*, Vol. 21, 731-765.

Hauschka, Christoph E. (2004). "Compliance, Compliance Manager, Compliance Programme – Eine geeignete Reaktion auf gestiegene Haftungsrisiken für Unternehmen und Management?", *Neue Juristische Wochenschrift*, 257--261.

Heilemann, Julia (2021). "Click, Collect and Calculate: The Growing Importance of Big Data in Predicting Future Criminal Behaviour", *Revue Internationale de Droit Penal* (RIDP), Vol. 92, 49-68.

Hoeren, Thomas (2016). "Thesen zum Verhältnis von Big Data und Datenqualität – Erstes Raster zum Erstellen juristischer Standards", *MultiMedia und Recht* (MMR), 8-11.

Kahlenberg, Julia, Schäfer, Simon & Schieffer, Anita (2020). "Allgemeine Bausteine eines Compliance Management Systems", in *Antikorruptions-Compliance*, Busch, Markus/Hoven, Elisa/Pieth, Mark/Rübenstahl, Markus (eds), C.F. Müller, Heidelberg.

Kischel, Uwe (2015). *Rechtsvergleichung*, C.H. Beck, Munich.

Kowallik, Andreas (2021). "Compliance in einer digitalen Welt: Das neue Sozialkreditsystem in China", *Der Betrieb* (DB), 252-257.

Kress, Sonja (2018). *Criminal Compliance und Datenschutz im Konzern*, Nomos, Baden-Baden.

Laufer, William (2016). "Compliance and Evidence: Glimpses of Optimism from a Perennial Pessimist", in *Die Verfassung moderner Strafrechtspflege: Erinnerung an Joachim Vogel*, Tiedemann, Klaus/Sieber, Ulrich/Satzger, Helmut/Burchard, Christoph/Brodowski, Dominik (eds.), Nomos, Baden-Baden, pp. 423-442.

Laufer, Willam (2017). "A very special regulatory milestone", *University of Pennsylvania Journal of Business Law*, Vol. 20, 392-428.

Mazzacuva, Federico (2021). "The Impact of AI on Corporate Criminal Liability: Algorithmic Misconduct in the Prism of Derivative and Holistic Theories", *Revue Internationale de Droit Penal* (RIDP), Vol. 92, 143-158.

Meier, Stefan (2016). *Digitale Forensik in Unternehmen*; available online at https://d-nb.info/1123802726/34 (last accessed on 31.03.2023).

Minkoff, Andreas (2016). *Sanktionsbewehrte Aufsichtspflichten im internationalen Konzern*, C.F. Müller, Heidelberg.

Mösle in, Florian (2018). "Digitalisierung im Gesellschaftsrecht: Unternehmensleitung durch Algorithmen und künstliche Intelligenz?", *Zeitschrift für Wirtschaftsrecht* (ZIP), 204-212.

Mösle in, Florian/Lordt, Arne (2017). "Rechtsfragen des Robo-Advice", *Zeitschrift für Wirtschaftsrecht* (ZIP), 793-802.

Moosmayer, Klaus (2021). *Compliance*, 4th ed., C.H. Beck, Munich.

Mozzarelli, Michele (2022). "Digital Compliance: The Case for Algorithmic Transparency", in *Corporate Compliance on a Global Scale – Legitimacy and Effectiveness*, Manacorda, Stefano and Centonze, Francesco (eds), Springer Nature Switzerland, Cham, pp. 259-284.

Neufang, Sebastian (2017). "Digital Compliance – Wie digitale Technologien Compliance-Verstöße vorhersehen", *Zeitschrift für Internationale Rechnungslegung*, 249-254.

Rack, Manfred (2016). "Die Digitalisierung des Compliance Managements zur Senkung des Aufwands", *Compliance-Berater*, 16-20 & 58-64.

Rademacher, Timo (2017). "Predictive policing im deutschen Polizeirechts", *Archiv des öffentlichen Rechts,* Vol. 142, 366-416.

Raphael, Philip Monty & Phillips, Tom (2020). "United Kingdom", in *Antikorruptions-Compliance*, Busch, Markus/Hoven, Elisa/Pieth, Mark/Rübenstahl, Markus (eds), C.F. Müller, Heidelberg, pp. 461-478.

Rudkowski, Lena (2019). "'Predictive policing' am Arbeitsplatz", *Neue Zeitschrift für Arbeitsrecht*, pp. 72-79.

Schemmel, Alexander (2021). "'Effective Corporate Governance' by Legal Tech/Digital Compliance", in *Rechtshandbuch Legal Tech*, Breidenbach, Stephan and Glatz, Florian (eds), 2nd ed., C.H. Beck, Munich, pp. 166-182.

Schneider, Uwe H. (2003). "Compliance als Aufgabe der Unternehmensleitung", *Zeitschrift für Wirtschaftsrecht*, 645-650.

Schroeder, Friedrich-Christian (1996). "Probleme der Übersetzung von Gesetzestexten", *Zeitschrift für die gesamte Strafrechtswissenschaft*, Vol. 117, 236-244.

Sieber, Ulrich (2006). "Strafrechtsvergleichung im Wandel. Aufgaben, Methoden und Theorieansätze der vergleichenden Strafrechtswissenschaft", in *Strafrecht und Kriminologie unter einem Dach*, Sieber, Ulrich/Albrecht, Hans-Jörg (eds), Duncker & Humblot, Berlin, pp. 78-151.

Sieber, Ulrich & Engelhart, Marc (2014). *Compliance Programs for the Prevention of Economic Crimes*, Duncker & Humblot, Berlin.

Siems, Mathias (2008). "Statistische Rechtsvergleichung", *Rabels Zeitschrift für ausländisches und internationales Privatrecht*, 354-390.

Simões Agapito, Leonardo/de Alencar e Miranda, Matheus/Xavier Januário, Túlio Felippe (2021). "On the Potentialities and Limitations of Autonomous Sys-

tems in Money Laundering Control", *Revue Internationale de Droit Penal* (RIDP), Vol. 92, 87-107.

Spindler, Gerald (2018). "Gesellschaftsrecht und Digitalisierung", *Zeitschrift für Unternehmens- und Gesellschaftsrecht* (ZGR), 17-55.

Tiedemann, Klaus (2017). *Wirtschaftsstrafrecht*, 5th ed., Vahlen, Munich.

Volkov, Michael (2013). *The Impact of New Technologies in Corporate Governance, Risk Management and Compliance Programs*, 2013.

Wagner, Jens (2018). "Legal Tech und Legal Robots in Unternehmen und den sie beratenden Kanzleien", *Betriebs-Berater*, 1097-1105.

Weisflog, Walter E. (1996). *Rechtsvergleichung und juristische Übersetzung. Eine interdisziplinäre Studie*, Schulthess, Zurich.