6

Artificial Intelligence and Data Protection Law

THOMAS HOEREN AND MAURICE NIEHOFF

6.1 Introduction

Initial scientific research on artificial intelligence (AI) dates back to the 1940s.[1] Since then, technical development has made rapid progress. AI has become more and more important in recent years due to the rapidly increasing computing power of computers and the emergence of huge amounts of data, referred to as 'Big Data'.[2] The German Research Centre for Artificial Intelligence (DFKI) and the Fraunhofer Institute are conducting intensive research in this area.

This debate is being revived by the introduction of the General Data Protection Regulation (GDPR). Bitkom, the digital association of Germany, recently published a position paper[3] in which the topic was examined from an interdisciplinary perspective. The German Federal Government is also aware of the importance of the topic; for example, it organised Safer Internet Day 2018, the flagship event under the title of artificial intelligence.[4] In this context, the focus is increasingly on how technical progress can be made accessible in terms of data protection law. The GDPR, which aims to ensure that the data protection level for those affected is as uniform as possible, now joins this list. Among other things, this should be achieved by banning automated decisions and the associated information rights and obligations.

[1] Christian Honey, 'Künstliche Intelligenz – Die Suche nach dem Babelfisch' (2016) Zeit Online, www.zeit.de/digital/internet/2016-08/kuenstliche-intelligenz-geschichte-neuronale-netze-deep-learning, accessed 24 April 2019.

[2] Wolfgang Hoffman-Riem, 'Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht' (2017) 142 *Archiv des Öffentlichen Rechts* 6.

[3] DFK, Bitkom e.V., 'Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung' (2017), www.bitkom.org/sites/default/files/file/import/171012-KI-Gipfelpapier-online.pdf, accessed 25 April 2019.

[4] See www.saferinternetday.org/, accessed 3 March 2019.

https://doi.org/10.1017/9781108921923.010 Published online by Cambridge University Press

This chapter focuses on these automated decisions using algorithms and artificial intelligence uncovers their legal difficulties and offers solutions.

6.1.1 Algorithms

Algorithms are used to systematically solve a problem. They work with the help of (usually) deterministic, stringently followed, unambiguous and finite rules of action. The input of a certain value is followed by the output of a result, whereby the same result is always obtained due to the determinism with the same input values.[5] Classical examples in the analogue world are cooking recipes, for example, where a clear sequence of actions (recipe) is always followed by the same result (finished dish), that is, 'if …, then … processes'.[6] In the digital world, the rules of action are represented and processed by computer programs.

6.1.2 Artificial Intelligence

Artificial intelligence is also based on the algorithms described previously.[7]

Artificially intelligent applications also make use of rules of action, but they go far beyond that. The term 'artificial intelligence' generally refers to algorithms that are able to simulate human action.[8] In order to achieve the most human-like action possible, so-called artificial 'neural networks' are created. These correspond to the structure of the human brain.

A neural network consists of input and output neurons and intermediate layers, the so-called hidden layers.[9]

This construction is particularly capable for 'machine learning' and its sub-area of 'deep learning'. In addition to the linear 'if …, then … process', it includes the possibility of self-learning.[10]

Where pure machine learning is based on the ability to learn through human influence, the system learns contexts in deep learning without any

[5] Thomas Cormen et al., *Algorithmen – Eine Einführung* (4th ed. de Gruyter 2017), 5.
[6] Armin Barth, *Algorithmik für Einsteiger* (2nd ed. Springer Spektrum 2013), 2.
[7] Christian Ernst, 'Algorithmische Entscheidungsfindung und Personenbezogene Daten' (2017) 72(21) *Juristen Zeitung* 1027.
[8] There is still no scientific consensus on a definition; see DFK, Bitkom 'Künstliche Intelligenz', 28–31; Wolfgang Ertel, *Grundkurs künstliche Intelligenz* (4th ed. Springer Vieweg 2016), 1.
[9] Yann LeCun et al., 'Deep Learning' (2017) 521 *Nature Deep Review* 437.
[10] Jürgen Schmidhuber, 'Deep Learning in Neural Networks: An Overview' (2015) 61 *Neural Networks* 86.

human intervention. The system is trained using Big Data components, that is, large amounts of data. Based on the training data entered, the system recognises correlations and structures, questions the initial result and improves itself.[11]

This learning process leads to an increase in the layers between the input and output neurons, enabling increasingly complex decisions.

As a result, however, it is no longer possible to understand how the result is generated from an external point of view – we know that it works without knowing how it works.[12] The decision basis, the original algorithm, is also subject to constant change. The decision becomes a 'black box' for the person concerned.

In order to protect the rights of those affected, the GDPR contains various regulations, in particular the articles on automated decisions that are important for algorithms and AI. Automated decisions concern Arts 22 and 13–15 of the GDPR. These open up obligations to provide information or rights. There is a broad discussion on the content of this topic. Those affected are interested in receiving as much information as possible, and those responsible must be protected within the framework of trade secrets. For those affected, effective protection must be provided against automated decisions. You must not be left helplessly at the mercy of the AI's decisions.

In a first step, the chapter explains the applicability of the prohibition standard of Art. 22 GDPR in the case of automated decisions. On this basis, the rights of information and obligations according to Arts 13–15 of the GDPR will be discussed. In this context, the question arises: what specific requirements have to be placed on the information duty of those responsible? For this purpose, the present legal situation on the issue of dispute will be explained – whether a disclosure of the algorithm formula is required in the context of the information, or whether the mere principle behind it is sufficient.

Based on this, specific requirements for the type and scope of the information are developed: what does this mean in practice for those responsible? What standards are necessary for this? How does a company explain itself today if it decides against an applicant or a supplier?

[11] Ibid.

[12] Oliver Stiemerling, 'Künstliche Intelligenz – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge' (2015) 12 *Computer & Recht* 764; Ertel, *Grundkurs künstliche Intelligenz*, 308–10.

In a further step, the question is raised as to how the requirements for the justification of an automated decision will develop in the future.

This is where the peculiarities of AI-based decisions come into play. The differences to linear algorithms are worked out and the problem is raised that, due to the deep learning process, the responsible persons themselves may not be able to understand or represent either the algorithm or the principle behind it. How can the uncertainty be represented in enterprise applications when machine learning techniques only give probability indications? How can you make them understandable to the user? What is required by law?

Accordingly, the relationship between GDPR and the national law of the new Federal Data Protection Act (BDSG-New) will be examined in particular. It deals explicitly with the relationship of Section 31 BDSG-New to Art. 22 GDPR. To what extent does GDPR include scoring in the BDSG-New? Is there a priority of the GDPR or does the BDSG-New substantiate the GDPR?

Finally, aspects related to the topic are dealt with, such as the obligation to carry out a data protection impact assessment in accordance with Art. 35 (3) (a) GDPR, the right of objection according to Art. 21 GDPR, the obligation to appoint a data protection officer (Art. 37 GDPR) and the possibility of imposing a fine under Art. 83 GDPR.

The chapter ends with a view on the challenge that the legal system faces with the development of artificial intelligence.

6.2 Lion's Share

Artificially intelligent applications are also finding more and more applications in automated decisions. Since they are particularly suitable for large amounts of data, the application areas of image and speech recognition can be mentioned above all; for example, most citizens are familiar with Google image search or the speech assistant Siri.

Even in the banking, insurance and government sectors, algorithm-based decisions are increasingly being used.

Article 22 of the GDPR wants to take this into account by banning automated decisions.

6.2.1 Article 22 (1) GDPR

The model for Art. 22 GDPR is Art. 15 (1) of the Data Protection Directive. According to the Directive, every person has been granted the right not to be subject to a decision which is detrimental to him or her and which is

https://doi.org/10.1017/9781108921923.010 Published online by Cambridge University Press

based solely on automated processing of personal data for the purpose of assessing individual aspects of this person. Article 22 GDPR goes beyond Art. 15 of the Directive, which only concerned disadvantageous or weighty measures.

Article 22 (1) of the GDPR prohibits the persons concerned from excluding a 'decision based solely on automated processing'. This means a procedure that is carried out without human intervention from the data acquisition up to the decision making.[13] Thus the question arises when a decision is considered to be exclusively automated.[14]

This is clearly the case when decision-making processes are carried out from beginning to end without any human influence.

It is unclear whether Art. 22 GDPR also includes those processing operations where the algorithm completely prepares a decision, but where a person ultimately implements the decision without wanting to influence the decision content. This is the case, for example, with a mere confirmation of the result.[15] In this respect, the mere decision making (pressing the 'OK' button) of the human being is not to be taken into consideration. This would ultimately render the standard useless. Further, human intervention in the neural network to improve decisions, such as supervised learning,[16] does not constitute sufficient human action. It has no influence on the content but is comparable to maintenance. It must therefore be based on whether the person who is involved in the decision-making process also deals with the content of the decision. This argument goes beyond mere consent.[17]

This can be derived from the purpose of Art. 22 of the GDPR. The purpose of the prohibition regulation of Art. 22 (1) GDPR is to protect the parties concerned from an exclusively computer-based decision. At the end of every decision there must be a human being.[18] The background is the fundamental rights protected under Art. 2 (1) of the Basic Law and Art. 2 (1) in conjunction with Art. 1 of the Basic Law, the general freedom

[13] GDPR, Recital 71 explicitly states so.

[14] Mario Martini 'Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling' in Boris Paal and Daniel Pauly (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2nd ed. C. H. Beck 2018), DS-GVO Art. 22 ref. 16–18.

[15] Wolfgang Hoffman-Riem, 'Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht' (2017) 142 *Archiv des Öffentlichen Rechts* 36.

[16] Hereto Jürgen Schmidhuber, 'Deep Learning in Neural Networks: An Overview' (2015) 61 *Neural Networks* 89–91; Stiemerling, 'Künstliche Intelligenz', 763.

[17] Martini DS-GVO Art. 22 ref. 16–18.

[18] Mario Martini, 'Algorithmen als Herausforderung für die Rechtsordnung' (2017) 72(21) *Juristische Zeitung* 1019.

of action and the right to informational self-determination. For those affected, it must remain transparent whether they have been the target of a fully automated decision; otherwise, a 'feeling of helplessness'[19] arises. Furthermore, an exclusively algorithm-based decision concerns the identity and right of self-determination of each person concerned. The algorithm processes the acquired personal data on the basis of predefined criteria and weightings, draws conclusions and correlations and comes to a result. The affected person is nothing more than a collection of input data; the individual personality of the person is not taken into account.[20]

Ultimately, however, the prohibition in Art. 22 (1) GDPR turns out to be isolated and a blunt sword. Due to its paragraph 2, there are numerous exceptional possibilities, which will probably become the norm in practice.

In this respect, the legal focus does not lie on the prohibition in accordance to Art. 22 (1) GDPR. Consideration should be given to the rights and obligations which result from the references in Arts 13–15 of the GDPR to Art. 22 of the GDPR. Indeed, if the door is already open for the application of automated decisions, there must in any case be rules that guarantee the effective exercise of the rights of those concerned.

6.2.2 Rights and Obligations under Articles 13–15 GDPR

Articles 13–15 of the GDPR are therefore relevant due to the prohibition of automated decisions.

6.2.2.1 Description

Articles 13–15 GDPR are preventive means of protection.

Article 13 (2) (f) and Art. 14 (2) (g) of the GDPR establish a duty of information for those responsible as soon as persons are affected by automated decisions according to Art. 22 of the GDPR. At the same time the data subjects shall also be granted a right to information pursuant to Art. 15 (1) (h) of the GDPR.

6.2.2.2 The Purpose of the Provisions

Following the purpose of the prohibition standard of Art. 22 of the GDPR, Arts 13–15 of the GDPR are intended to enable those affected to take

[19] Christian Ernst, 'Algorithmische Entscheidungsfindung und Personenbezogene Daten' (2017) 72(21) *Juristen Zeitung* 1030.

[20] Ibid.

effective measures against decisions that are exclusively automated. This is already explained in Recital 63, p. 1, which gives the person concerned the right to 'verify the legality'. The person concerned must be given a fair and transparent insight as far as possible. This includes, in addition to the information on the existence of a processing operation of personal data, its circumstances and purpose.[21] An 'effective enforcement' is only possible if the person concerned has a comprehensive insight into the decision. Only then can he or she raise specific concerns about the processing process and effectively raise his or her own objections.

6.2.2.3 Requirements for Article 13 (2) (f), Article 14 (2) (g) and Article 15 (1) (h) GDPR

However, the precise scope of the disclosure obligation is controversial.

Article 12 (1) of the GDPR confirms the requirements for the greatest possible disclosure obligation of those responsible towards the persons concerned.

This places the following requirements on the disclosure obligations of the responsible persons according to Arts 13–15 of the GDPR: 'Precise, transparent, comprehensible and easily accessible form in a clear and simple language'.

For this purpose, in Recital 58, p. 3, it is clear that 'the complexity of the technology required for this purpose makes it difficult for the data subject to recognise and understand whether, by whom and for what purpose personal data concerning him/her are collected'. The EU therefore recognised the conflict threatening those affected and tried to counteract it with the aforementioned obligations.

The Union also recognised that automated decisions have a special feature, namely their lack of transparency. For this reason, Arts 13–15 of the GDPR respectively impose the following requirements in their second paragraphs f) and g) and h) on the duty of the responsible persons to provide information: significant information on the logic involved must be provided.

Which leads to the question: what is behind the concept of the involved logic? What exactly do those responsible for automated decisions have to communicate?

[21] Boris Paal and Moritz Hennemann 'Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person' in Boris Paal and Daniel Pauly (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2nd ed. C. H. Beck 2018) Art. 13 ref. 4.

6.2.3 The Scope of the Information Obligations in Terms of Content

The algorithm may need to be disclosed in a second step, taking into account the peculiarities of AI-based decisions.

6.2.3.1 Disclosure Algorithm

One possibility would be to have to disclose the operating algorithm behind the processing. This would fulfil the requirements for a disclosure obligation that is as comprehensive as possible and would also get to the bottom of the 'involved logic'.

This contradicts the prevailing opinion of literature. According to the latter, it is only the principle behind the decision, not the algorithmic formula itself, that should be explained.

On the one hand, this would result from the interpretation of Recital 63, p. 3, to Art. 15 of the GDPR. In its German version it is still not very productive. It merely repeats the wording of the standard by declaring: 'Every person concerned should therefore be entitled to know … the logic underlying the automatic processing of personal data'.

However, the French language version explicitly states that only the basis of the logic is revealed. This is also the case for the Dutch language version.

On the other hand, Recital 63, p. 5, should also be used. Accordingly, the disclosure is explicitly intended not to impair the business secrets of other persons. Sentence 6 restricts this to the extent that the person concerned may not be denied access to all information due to the protection of trade secrets. This entails weighing the interests of the parties responsible for business secrets against the interests of the parties concerned in providing the information.

Exactly this consideration had to be decided by the Federal Supreme Court (BGH) in its judgement of 28 January 2014,[22] in the so-called SCHUFA judgement. In this, the plaintiff brought an action against SCHUFA for disclosure of the score formula that was used. This score formula is exactly such an algorithm that uses personal data to determine whether a person is creditworthy or not.

At that time the BGH ruled, still on the basis of Section 34 BDSG-Old, that the plaintiff was not entitled to this claim. The reason for this was that SCHUFA's trade secrecy prevailed over the plaintiff's right to

[22] Federal Supreme Court (BGH), judgement of 28 January 2014 – VI ZR 156/13.

https://doi.org/10.1017/9781108921923.010 Published online by Cambridge University Press

transparency of the decision. This takes up the prevailing opinion in the literature and transfers it to the application of the GDPR.

As an interim result, it can be stated on the basis of this argumentation that the disclosure obligation does not have to include the algorithm formula.[23] The Higher Regional Court of Nuremberg, as a preliminary instance of the Federal Supreme Court, explained in its decision of 2012 that 'comprehensible' does not mean 'recalculable for the person concerned'.[24]

Recital 63, p. 6, may be used to disclose the algorithmic formula. The latter explicitly states that the protection of trade secrets in accordance to Recital 63, p. 5, should not lead to a refusal of information to the person concerned. The responsible persons must not hide behind their secrecy because otherwise there would be no effective information. It must always be weighed on a case-by-case basis. In individual cases, this can also lead to the publication of the algorithm. In this respect, it is questionable to what extent the definition of the algorithm affects the trade secret at all. It is important to note that the disclosure of the algorithm does not represent a factual threat to the business secrets of the responsible person. This does not mean that the data subject or third parties can exploit or misuse this information just because the relevant regulations and program procedures are explained to the data subject with the appropriate weightings. In order to do this, the source code has to be released, which translates the algorithm into working, usable software.

While the prevailing opinion may have now spoken out against the publication of the algorithmic formula,[25] the question of AI-based decisions must be completely reiterated. Following this controversy, the special feature of AI-based decisions has to come into play.

6.2.3.2 Special Features of the Right to Information in the Case of AI

In contrast to 'normal' algorithm-based decisions, the problem with AI-based decisions is that AI decisions are based on the deep learning process. AI systems correspond to neural networks; they are not programmed according to a linear model of a line of code but continue to program themselves. This means that the algorithm is self-developed – it learns by itself.

[23] Paal and Hennemann, DS-GVO, Art. 13 ref. 31.
[24] Higher Regional Court (OLG) Nuremberg, judgement of 30 October 2012 – 3 U 2362/11.
[25] Paal and Hennemann, DS-GVO, Art. 13 ref. 31.

Therefore, it is not possible to perform an ordinary linear control. Usually, the developers themselves do not know how the AI system works and how it is decided.[26] The developers only know that it works.[27] The algorithm could not be published at all, as it is constantly evolving.

Looking at the GDPR, it quickly becomes clear that the authors did not consider this. The GDPR is far too one-dimensional: it does not take into account the possibility of non-transparent, self-learning processes. All too superficially, the regulation speaks of automated decisions, logic and a fair and transparent procedure, without considering the complexity of self-learning AI processes.

For this reason, GDPR must be specially designed with regard to AI decisions. When interpreting the requirements of Arts 12 and 13–15 GDPR, it is important to observe the constant leitmotif of the information rights. The person concerned must receive the necessary transparency so that he or she can raise objections effectively and decisively against automated decision-making. The requirement of Art. 12 of the GDPR is to be considered thereby. The information must therefore be provided in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language'.[28]

How should this be done with AI, even if the developers do not know how the AI system works and the algorithm is not transparent?[29] The impending 'black box character' must therefore be dissolved. This is done in a way that allows the person concerned to understand the outcome of the decision:

> 'Every far-reaching decision should be verifiable by a human being'.[30] This does not necessarily require an explanation of how the neural network works, it is sufficient to understand how the decision was made.[31]

[26] Joshua Kroll et al., 'Accountable Algorithms' (2017) 165(3) *University of Pennsylvania Law Review* 638; W. Nicholson Price II, 'Black-Box Medicine' (2015) 28(2) *Harvard Journal of Law & Technology* 432–33.

[27] Stiemerling, 'Künstliche Intelligenz', 764; Ertel, *Grundkurs künstliche Intelligenz*, 308–10.

[28] See Art. 12 (1) GDPR.

[29] Kroll et al., 'Accountable Algorithms'.

[30] Gianclaudio Malgieri and Giovanni Comandé, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7(4) *International Data Privacy* 246; Finale Doshi-Velez and Mason Kortz, 'Accountability of AI under the Law: The Role of Explanation' (2017) 18-07 Harvard Public Law Working Paper, 1–2.

[31] Sandra Wachter et al., 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31(2) *Harvard Journal of Law & Technology* 850–51; Doshi-Velez and Kortz, 'Accountability of AI under the Law', 2–3.

One possibility would be to publish the output algorithm, the basic construct of the neural network. This could at least provide an indication of how the automated decision came about. In this case, the objection of the prevailing opinion that the trade secret is contrary to this should have far less weight. After all, it is not the working algorithm in the status quo that is issued, but a 'predecessor version'. However, depending on the developmental progress of the neural network, the output algorithm may not have much in common with the algorithm at the time the decision is made. In this respect, this will not help the person concerned to effectively assert her or his rights as an affected person. The requirements of Recitals 63 and 71 and the meaning and purpose of the right to information would not be respected. The logic behind the decision would no longer have been revealed. The algorithm in the predecessor version most likely has significantly different weightings, criteria and structures than the decisive AI algorithm. Thus, it does not help the affected person to find out possible decision criteria of the output algorithm if the later algorithm has created new criteria for itself through the self-learning process.

Another possibility would be to provide the person concerned with information about the training data. The input neurons, that is, the input data of the system, are known to the responsible persons. However, this leads to the same problem: the hidden layers, which are relevant for decision making, are not easily visible and develop independently from the original training data. Again, it would not be possible to provide information that meets the requirements.

One way to make these hidden layers visible is the so-called Layer-Wise Relevance Propagation (LRP). Here, the decision-making process of a neural network is played backwards through a complicated mathematical procedure. It is visualised for the human eye using a heatmap. On this heatmap, positive and negative decisions of the hidden layers are made visible with the help of different colours and thus the decision is explained. Until now, this method has been particularly successful with image recognition software. This variant solves the problem by not releasing the algorithm. Nevertheless, the reason for the decision is worked out. It is questionable to what extent this is technically applicable to non-visual decisions.

A similar solution is to make artificial intelligence explainable.[32] By means of so-called Local Interpretable Model-Agnostic Explanations

[32] Joshua A. Kroll et al., 'Accountable Algorithms' (2017) 165 *University of Pennsylvania Law Review*, 650–52; Christin Seifert et al., 'Visualisations of Deep Neural Networks in Computer Vision: A Survey' in Tania Cerquitelli, Daniele Quercia and Frank Pasquale (eds), *Transparent Data Mining for Big and Small Data* (Springer 2017), 123–25.

(LIME), predictions of a neuronal network are made comprehensible for the affected persons. Using a technical procedure, the relevant word fields around the decision are recognised. This may not encompass the complete decision of the neural network as given as only the local, neuronal activities around the decision are recognised. In the event of a refused creditworthiness check, the criteria 'unemployed', 'debt' and 'SCHUFA entry' might be identified as relevant for the result.[33] These results are therefore verifiable and comprehensible for the affected person. Each interested party may use this information to assess whether the decision is based on criteria that are correct and appropriate or not.

However, this is only an approximate value, albeit a very reliable one. The possibility that in the depths of the neural network other criteria – which may possibly be factual and discriminating – may have led to the decision cannot be completely ruled out. In order to understand the logic behind the decision, it is necessary for the person concerned to be informed about this imponderability. Automated decisions remain statements of probability.

This should also be kept in mind while contemplating the disclosure obligations of users. In practice, users must ensure that they present the automated decision to the affected parties in such a way that it can be explained in a verifiable and comprehensible manner. The fact that from a technical point of view (as of today) there is no way to fully implement decisions of neural networks must be taken into account. In this respect, technical innovations must not be blocked by data protection legislation. There is a need for an appropriate balance between promoting innovation and safeguarding the rights of those affected. This line of thought should also lead the interpretation and application of the GDPR. The illustrated possibility to explain automated decisions by means of an approximation test which complies with the technical standards and which is as close as possible to reality is sufficient.

6.2.4 Scoring According to BDSG and GDPR

Another fragment for standardisation in the area of AI is Section 28b BDSG-Old and Section 31 (1) BDSG-New with their regulations on scoring. There is a new criterion for the evaluation of information gathering

[33] See Marco Tulio Ribeiro et al., 'Why Should I Trust You? Explaining the Predictions of Any Classifier' (2016) 2 ff, https://arxiv.org/abs/1602.04938, accessed 27 June 2018.

methods, namely the basis of a 'scientifically recognized mathematical-statistical method' for calculating the probability value (No. 2).[34]

This classification has far-reaching consequences for the Big Data scene. In accordance with Section 31 (1) No. 2 BDSG-New, the mathematic standards must be 'verifiable' for calculating probability. The reference to 'verifiability' shifts the burden of presentation and proof to the users and allows the data protection supervision to keep informed about the parameters for verifiability in the case of the use of personal data within the framework of Section 40 (4) sentence 1 BDSG-New.

To this end, it must be explained to what extent the BDSG-New will be used in addition to the GDPR.

6.2.4.1 Definition Scoring

Section 31 BDSG-New defines scoring as 'the probability value of a certain future behaviour of a natural person for the purpose of deciding on the establishment, execution or termination of a contractual relationship with that person'.[35]

This means that a forecast for the future is created on the basis of collected data of a person.

6.2.4.2 Applicability of Section 31 BDSG-New Compared with Article 22 GDPR

The GDPR does not mention scoring in any way. Nevertheless, the application of scoring under Art. 22 of this regulation can be argued for.

For this purpose, the ranges of the respective standards must be determined and compared with each other.

The scope of Section 31 BDSG-New is unclear. It can be interpreted in such a way that it is also applicable to automated decisions in accordance with Art. 22 of the DS Regulation, in addition to the narrow scope of financial scoring. This is supported by the explanatory statement of the Federal Government's bill: 'Scoring is a mathematical-statistical procedure that allows the probability of a certain person showing a certain behaviour to be calculated'. There is no evidence anywhere that the scoring procedure must be limited to credit checks. The only limitation contained in the provision is the indication that scoring should be used to 'decide on the establishment, performance or termination of a contractual relationship

[34] See Section 31 (1) No. 2 BDSG-New.

[35] See Section 31 (1) BDSG-New.

with the party concerned'. The term used to describe the collection of probabilities goes far beyond the usual methods of credit scoring. For all business transactions, therefore, the decision to conclude a transaction will inevitably be influenced by forecast assessments. Similarly, many AI processes are based on scoring, which is incorporated into the design of differentiated business models.

In this respect, the wording is consistent with Recital 71 to Art. 22 of the DS Regulation, which inter alia reads as follows: in sentence 1, 'automatic rejection of an online credit application'; in sentence 2, 'analysis or forecasting of aspects relating to … economic situation'; and in paragraph 2, 'appropriate mathematical or statistical methods'.

With regard to Art. 22 GDPR, a differentiation must be made as to whether the scoring method is directly related to the final automated decision or whether scoring is merely an upstream method by external credit agencies. This differentiation can also be seen in the wording of Section 31 BDSG-New. Paragraph 1 refers to 'probability values … for the purpose of the decision', and paragraph 2 explicitly mentions the 'use of a probability value determined by credit agencies'. The criterion here, as in the interpretation of exclusivity, is whether a human decision has been made in the meantime.

Article 22 GDPR therefore covers internal scoring. The collection of probability values is immediately followed by an automated decision without human intervention. In this respect, the term scoring meets the requirements of a 'decision based exclusively on automated processing'. It is subject to the requirements of Art. 22 GDPR.

The GDPR is regarded as a European ordinance in accordance with Art. 288 (2) sentence 1 Treaty on the Functioning of the European Union (TFEU), which comes into force immediately and bindingly for all member states. It takes precedence over contradicting national regulations. However, priority is limited by the extent of contradiction through national law. Interpretations and concretions by national law are possible. An example of concretion can be found in Section 31 (1) BDSG-New, substantiating the term 'involved logic' of the GDPR for the benefit of the concerned parties as a 'scientifically recognized mathematical-statistical procedure'. The added value of concretion compared with the wording in Recital 71, p. 2, lies in the aforementioned shift in the burden of proof. In accordance with Section 31 (1) BDSG-New, suitable mathematical and statistical methods must be demonstrated.

However, external scoring, which also includes classic credit scoring, cannot be covered by Art. 22 of the DS Regulation. The upstream

collection of probability values, which does not yet lead directly to a decision, constitutes an upstream measure and merely prepares a decision. This remains unchanged by Recital 71, which sees 'online credit applications' of Art. 22 of the DS Regulation specifically covered. In relation to Art. 22 GDPR, the purpose of the standard, as outlined earlier, must be taken into account. Article 22 GDPR protects the persons concerned from a completely mechanical decision without regard to human individuality. It does not protect against being affected by surveys of probability values. Their legality is thus judged according to the general requirements of the GDPR. Therefore, the GDPR requires an opening clause for external scoring to open up the possibility for the national legislature to create specific, supplementary or deviating regulations from the GDPR.

The relevant opening clause can be seen in the summary from Art. 6 (4), 23 (1) lit. e) GDPR. Here, the national legislature is granted derogations to the 'protection of other important objectives of the general public interest of a member state, in particular an important economic or financial interest'.[36]

This goal was set in the legal justification of the Bundestag. In this, the Federal Government declares that it wants to adopt the 'material protection standard of Sections 28a and 28b BDSG-Old'.[37] This results out of efforts to protect the economy. Among other things, economic transactions are based on protecting consumers from excessive indebtedness by means of credit checks. Scoring is therefore 'the foundation of the German banking system and thus of the functioning of the economy'. Hence, the German Federal Government remains true to its policy of adhering to national scoring regulations. The German government already presented this justification in the DSAnpUG-EU draft.[38] The objection of it being merely a private-sector purpose which does not serve the public interest of the member state and leads to an undervaluation of the GDPR system does not apply. On the one hand, the functioning of the economy is indeed a public interest of the state. On the other hand, the GDPR as a system with innumerable opening clauses is intended to be put into practice in this manner by the member states.

Scoring, being directly related to the automated decision, is thus covered by the provision of Art. 22 of the DS Regulation. The GDPR is made

[36] See Art. 23 (1) lit. e) GDPR.

[37] See Deutscher Bundestag: 18. Wahlperiode (2017) Drucksache 18/11325, 101, http://dipbt.bundestag.de/doc/btd/18/113/1811325.pdf, accessed 24 June 2021.

[38] Ibid.

more specific for the benefit of those affected by Section 31 BDSG-New such that the verifiability of the mathematical-statistical methods of probability calculations is imposed on the users.

6.2.5 Follow-up Aspects of Automated Decisions

Automated decisions in accordance with Art. 22 GDPR are accompanied by further rights and obligations.

6.2.5.1 Data Protection Impact Assessment, Article 35 (3) lit. a GDPR

Article 35 (3) lit. a GDPR subjects the processor to a data protection impact assessment with systematic and comprehensive evaluation of personal aspects of natural persons. In accordance with paragraph 1, it is necessary to assess the consequences of the processing operations envisaged for the protection of personal data. In analogy to the previous remarks, this is particularly problematic for AI-based decisions, since the extent of the self-learning process of neural networks is hardly or not at all predictable for those responsible.

6.2.5.2 Right of Objection, Article 21 GDPR

In addition to the right of information under Art. 15 GDPR, the data subject is entitled to a right of objection in accordance with Art. 21 (1) GDPR.

6.2.5.3 Obligation for Data Protection Officer, Article 37 GDPR

If authorities should carry out automated decisions, a data protection officer shall be appointed in accordance with Art. 37 (1) lit. a GDPR. The same applies to private individuals in accordance with lit. b) for extensive, regular and systematic monitoring of persons affected.

6.2.5.4 Fines, Article 83 GDPR

Violations of the prohibition standard of Art. 22 GDPR as well as the information rights and obligations under Arts 13–15 GDPR are sanctioned with fines of up to €20,000 or up to 4 per cent of the total annual turnover achieved worldwide (Art. 83 (5) GDPR).

6.3 Conclusion

Algorithm-based, and above all AI-based, decisions continue to pose major problems for the legal system. These problems will not be solved by

https://doi.org/10.1017/9781108921923.010 Published online by Cambridge University Press

the introduction of the GDPR. On the contrary, further questions arise. Particularly in view of the increasing social significance of such decisions, a review of the legal assessment is required.

The justification requirements of the rights and obligations under Arts 13–15 GDPR must be fulfilled by users to the extent that the parties concerned must be given the opportunity to effectively defend themselves against an automated decision. This is achieved by explaining the decision to the person concerned in a way that is as coherent and comprehensible as possible. To this end, the criteria leading to each decision must be disclosed to the parties concerned.

This is put into practice by means of a state-of-the-art procedure which determines the criteria for finding results with the highest possible validity. However, errors in the deep, (still) impenetrable neural networks cannot be entirely eliminated. The person affected must also be informed about this.

Since automated decisions are increasingly making important social decisions, it remains to be seen whether further regulatory measures are appropriate in addition to disclosure obligations. Martini proposes these at various levels for preventive as well as supportive self-regulation and *ex post* regulation while warning about the dangers of over-regulation.[39]

In addition, Section 31 BDSG-New, which constitutes a legally binding specification for Art. 22 GDPR in the context of automated decisions, imposes the burden of explanation and proof for the verifiability of the mathematical standards on the users.

Attention must also be paid to the side effects, which should not be underestimated. Data sequence estimation, for example, presents the user with problems that he or she already has in relation to the obligation to provide information: he or she needs to assess the range of his or her AI-based system.

There is probably also the obligation of a data protection officer.[40] Otherwise, there is a risk of substantial fines for violations.[41]

The introduction of the GDPR will in practice require users of automated AI-based decisions to replace them comprehensively with their systems. In order to comply with the disclosure obligations and the data impact assessment, it is de facto assumed that users of AI can trace the basis of their decision – at least to the core criteria. This must be verifiable on the part of the users. The application of the law must always take place

[39] Martini, 'Algorithmen als Herausforderung für die Rechtsordnung'.
[40] See Art. 37 (1) GDPR.
[41] See Art. 83 GDPR.

in step with technical development. In no way must technical innovation be blocked by excessive regulation.[42] At the same time, the rights of those affected must be protected. The goal must be to dissolve the black box character of AI without hindering its development.

This is a major task for the future.

Bibliography

Arel I, Rose D and Karnowski T, 'Deep Machine Learning – A New Frontier in Artificial Intelligence Research' (2010) 5(6) *November IEEE Computational Intelligence Magazine* 13–18.

Barth A, *Algorithmik für Einsteiger* (2nd ed. Springer Spektrum 2013).

Cormen TH, Leiserson CE, Rivest R and Stein C, *Algorithmen – Eine Einführung* (4th ed. de Gruyter 2017).

DFK, Bitkom (eds), 'Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung' (2017), www.bitkom.org/sites/default/files/file/import/171012-KI-Gipfelpapier-online.pdf, accessed 25 April 2019.

Doshi-Velez F and Kortz M, 'Accountability of AI under the Law: The Role of Explanation' (2017) 18-07 Harvard Public Law Working Paper.

Ernst C, 'Algorithmische Entscheidungsfindung und Personenbezogene Daten' (2017) 72(21) *Juristen Zeitung* 1026–36.

Ertel W, *Grundkurs künstliche Intelligenz* (4th ed. Springer Vieweg 2016).

Hall P, Phan W and Ambati S, 'Ideas on Interpreting Machine Learning' (2017), www.oreilly.com/ideas/ideas-on-interpreting-machine-learning, accessed 15 March 2017.

Hoffman-Riem W, 'Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht' (2017) 142 *Archiv des Öffentlichen Rechts* 6–36.

Honey C, 'Künstliche Intelligenz – Die Suche nach dem Babelfisch' (2016) Zeit Online, www.zeit.de/digital/internet/2016-08/kuenstliche-intelligenz-geschichte-neuronale-netze-deep-learning, accessed 24 April 2019.

Kroll JA, Huey J and Barocas S et al., 'Accountable Algorithms' (2017) 165(3) *University of Pennsylvania Law Review* 633–705.

LeCun Y, Bengio Y and Hinton G, 'Deep Learning' (2017) 521 *Nature Deep Review* 436–44.

Malgieri G and Comandé G, 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation' (2017) 7(4) *International Data Privacy* 243–65.

[42] Martini, 'Algorithmen als Herausforderung für die Rechtsordnung'.

https://doi.org/10.1017/9781108921923.010 Published online by Cambridge University Press

Martini M 'Algorithmen als Herausforderung für die Rechtsordnung' (2017) 72(21) *Juristische Zeitung* 1017–25.

Paal B and Pauly D (eds), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2nd ed. C. H. Beck 2018).

Price II N, 'Black-Box Medicine' (2015) 28(2) *Harvard Journal of Law & Technology* 419–67.

Ribeiro M, Singh S and Guestrin C, 'Why Should I Trust You? Explaining the Predictions of Any Classifier' (2016), https://arxiv.org/abs/1602.04938, accessed 27 June 2018.

Schmidhuber J, 'Deep Learning in Neural Networks: An Overview' (2015) 61 *Neural Networks* 85.

Seifert C et al., 'Visualizations of Deep Neural Networks in Computer Vision: A Survey' in Cerquitelli T, Quercia D and Pasquale F (eds), *Transparent Data Mining for Big and Small Data* (Springer 2017), 123–25.

Stiemerling O, 'Künstliche Intelligenz – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge' (2015) 12 *Computer & Recht* 762.

Sydow G, *Europäische Datenschutzgrundverordnung* (2nd ed. Nomos 2018).

Wachter S, Mittelstadt B and Russell C, 'Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31(2) *Harvard Journal of Law & Technology* 841–87.

Wolff H and Brink S, '*Beck'scher Online-Kommentar Datenschutzrecht*' (27th ed. C.H. Beck 2019).