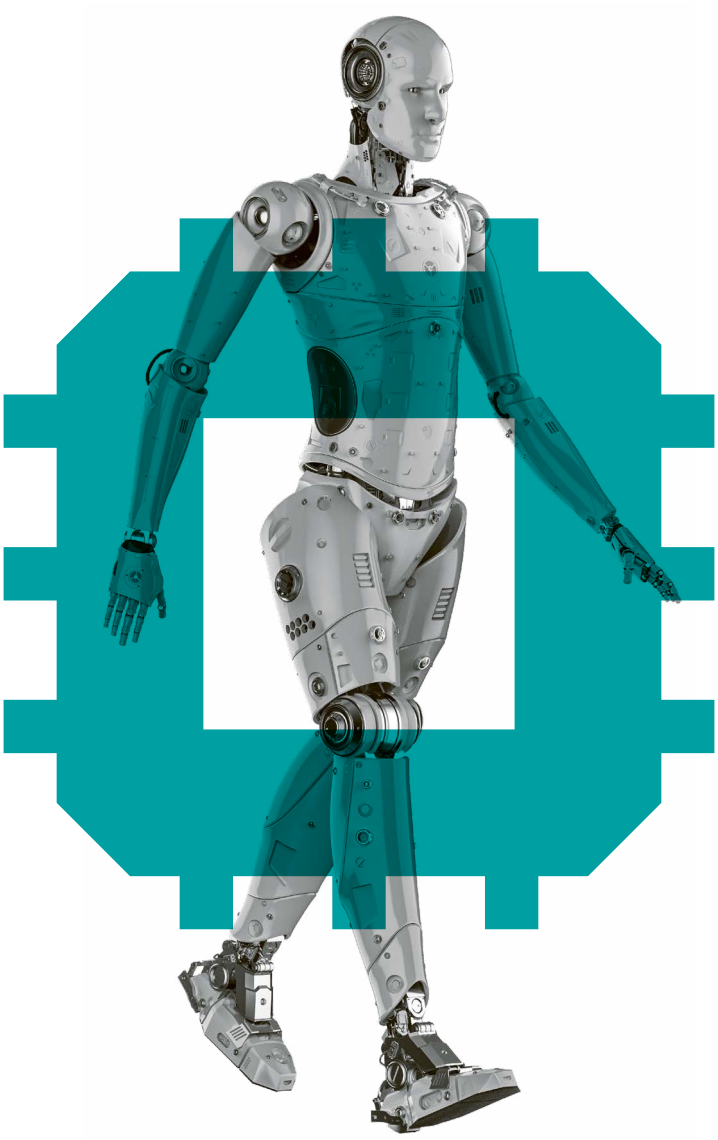
N

Newsletter
10/2019

Information and Communication Technology

Schellenberg Wittmer



Legal Aspects of "Artificial Intelligence" (AI)

Samuel Klaus and Claudia Jung

Key Take-aways

1.
AI-applications analyze unstructured data using an algorithm custom-tailored to the specific use intended, in order to draw conlusions based on such analysis.

2.
Regardless of its area of application and the purpose for which an AI application is put to use, legal questions arise regarding the creation, the parametrization and the use of AI applications.

3.
Since legislation does not (yet) account for the complexity of AI, the legal risks should be addressed by organisational measures and contractual provisions.

1 What is "Artificial Intelligence"?

1.1 Terminology

The term "**Artificial Intelligence**" (AI) does not refer to a specific technology. Rather, AI is a collective term for a multitude of methods which use mathematical-statistical models to simulate cognitive abilities.

1.2 Operating Principle

AI applications operate by analyzing a large amount of unstructered data (**Big Data**), using a custom-tailored algorithm in order to identify certain patterns in the data and to draw a conclusion therefrom. To do so, so-called **neural networks** are used, whose algorithms and structure are based on the functional principles of the human brain: Large numbers of individual algorithms work together in an intertwined and interdependent way, reflecting the functioning of the network of synapses in the human brain. Complex neural networks with several processing layers (i.e. with many algorithms connected in series and influencing each other) are referred to as **Deep Neural Networks**.

In complex ("deep") neural networks, the way in which the individual algorithms interact with one another is no longer specified by the developer, as the number of parameters to be defined is far too large. Instead, suitable **training data** (i.e. training data specially selected and targeted for the intended use) is fed into the neural network (e.g. x-ray images with diagnosed tumor centers) to be processed in automated training cycles. The neural network uses **statistical optimisation processes** to identify the most appropriate settings (*parametrization*), e.g. in order to autonomously identify tumor centres on new X-ray images. This process of automated parametrization of the neural network is known as **Deep Learning**.

The quality of an AI application depends on its architecture, its training and the quality of the training data.

Both the structure of the neural network and its settings must be custom-tailored to the **specific purpose** that the AI application is targeted to fulfil (e.g. speech or image recognition, text generation, etc.). Ideally, the AI application should then be able to identify in a large amount of data (e.g. the data stream of a surveillance camera) the kind of pattern it has been trained for (e.g. faces, license plates, etc.) in a very short time. The actual success rate of the AI applications is largely dependent on the structure of the neural network, the way it has been trained and the quality of the training data used.

1.3 Scope of Application

AI applications are able to analyze highly complex or dynamically changing data for certain patterns (e.g. credit card data for the purpose of fraud prevention, real time voice and image recognition, orientation of autonomous vehicles based on their surroundings).

2 Legal Aspects

Regardless of the area in which and the purpose for which an AI application is being put to use, certain legal issues arise regarding the **creation** (cf. 2.1), **parametrization** (cf. 2.2) and **use** (cf. 2.3) of AI applications.

2.1 Creation

AI applications can be created in-house or by using third-party providers. In either case, questions regarding the protection of the AI application and its integration into physical products have to be addressed.

Software is protected by copyright, while algorithms and parametrizations are not. Although an AI application is implemented by means of a software, it is largely based on algorithms and their parametrization. The implementation usually lacks the technical character required for protection by a patent. The *heart* of an AI application can therefore **neither be protected by copyright nor patent**. The creator of an AI application should therefore implement alternative protective measures, e.g. contractual confidentiality obligations.

AI applications are often **integrated into physical products** (e.g. in "smart" devices, machines, robots) that are subject to laws on product liability (PrLA) and product safety (PrSA). In this case, the additional complexity resulting from the use of AI must be taken into account (e.g. regarding product monitoring if an AI-based product, after being put on the market, develops further through interaction with users).

Developers creating AI applications for third parties are confronted with the **usual issues related to ICT contracts**: A contract regarding the creation of an AI application is a contract for work, in which questions will have to be addressed such as - in particular - the definition of services and defects (how to define the requirements and specifications for an AI application, and how to identify a defect?) and liability. For example, the developer may be liable to the customer if the developer chooses an algorithm that is ill suited for the desired purpose of the AI application, or a structure of the neural network that is inadequate for such purpose. The parties are therefore well advised to specify in the contract the defined application purposes and other customer requirements. Detailed contractual provisions are also required if customers train the AI application themselves or provide the training data (cf. 2.2), wish to further develop the AI application themselves or intend to use it for purposes other than those originally specified.

2.2 Training (Parametrization)

The neural network of an AI application must be **parametrized ("trained")** using as much appropriate training data as pos-

sible. During the ‹training›, the AI application executes a number of optimization cycles until the optimal setting ("parametrization") of the individual algorithms making up the neural network is achieved. This process raises issues regarding the quality and legal protectability of the training data as well as regarding data privacy / data protection.

The selection and quality of the training data greatly influence the results that the AI application produces in productive use: If unsuitable data is selected or if it is of poor quality (e.g. if it is not similar to the later input data in structure, scope and informational content), then the AI application is unlikely to deliver the desired results in productive use.

In addition, the training data must be selected carefully in order not to transfer pre-existing (undesired) tendencies into the AI application. Experience has shown that this is particularly relevant with regard to **equality and discrimination**: If the training data is not well balanced (e.g. regarding gender or skin color), then the AI application trained with such ‹biased› training data will automatically adopt this imbalance (so-called "**machine bias**"). If a company uses an AI application with such a machine bias, it runs the risk of violating statutory equality requirements and non-discrimination laws (cf. Section 2.3).

When third parties are contracted for the training of an AI application, **contractual assurances** regarding the composition and quality of the training data and the appropriateness of the training should be obtained. Companies conducting the training of an AI application with their own data should verify the data's quality and appropriateness.

The training of an AI application and the necessary training data are at least as relevant as the choice of the appropriate structure and algorithms. This raises the question of **how training data can be protected**. As a matter of Swiss law, pure data collections are not protected under intellectual property law. This makes contractual safeguards regarding the authorization, confidentiality and exclusivity of training data all the more important.

Furthermore, training data often contains personal data (e.g. people may be recognizable on pictures). If so, **data protection regulations** must be observed, i.e. the Data Protection Act (DPA) for matters limited to Switzerland and the General Data Protection Regulation (GDPR) for EU-related matters. If data is obtained from third parties, contractual assurances should be obtained. If own data is used, it should be verified whether this use is permissible: If no corresponding consent has been given by the data subject, the intention to create an AI application is generally not sufficient as a justification. Depending on the use case, anonymizing the training data might be an alternative.

2.3 Use

A company will be responsible for any **negative consequences of using AI applications** just as for any other tools and appliances. Even if the AI application is granted a certain degree of autonomy and causes damage as a result of an autonomous decision, the deploying company cannot rely on this in its defense: An AI application has no legal capacity, **any "action" by an AI application will be attributed to the company using it**. This raises issues regarding liability for AI-based decisions and the possibility of recourse.

If the use of an AI application leads to any damage, the question arises as to the reason: Was it the inappropriate structure of the neural network? Inadequately executed training? Or is the cause to be found in the training data? In these cases, the cause of the damage would be in the sphere of responsibility of the provider / creator of the AI application. However, if the reason was an error in operation (e.g. entering inappropriate data), or because the AI application was used for a purpose other than that for which it was originally designed, this would be the responsibility of the company using it. In any case, the prerequisite for identifying the source of the error is that the processing and decision-making process of the AI application is **transparent and traceable** (so-called "**Algorithmic Explainability**"). A company using AI applications created/trained by third parties should therefore be sure to obtain appropriate representations and warranties as well as comprehensive documentation.

Regarding liability, the traceability of the decision process of the AI application is of utmost importance.

An inappropriately programmed/trained AI application can lead to violations of statutory equality requirements and non-discrimination laws: If, for example, women are systematically disadvantaged by AI-based decisions due to a machine bias (e.g. regarding hiring or wages), there may be a violation of the Gender Equality Act (GEA).

In certain areas of application, **mandatory sector-specific regulations** must be observed (e.g. in road traffic for self-driving cars, in healthcare for AI-based medical products or in finance for automated portfolio management). An AI application must therefore be implemented in such a way that it always observes such regulations. Anyone procuring an AI application from a third-party manufacturer should obtain appropriate assurances in this regard.

If AI applications are used not only as a supporting tool, but for actual **automated decision-making** (e.g. for automatic approval/rejection of an application for a loan, based on an AI-based assessment of one's credit score), **data protection obligations** may also have to be observed: Within the scope of its application, the GDPR provides for a right not to be subject to a decision based exclusively on automated decision-making. This is not currently the case under the DPA, but a provision to that effect is expected to be introduced as part of its ongoing revision.

If AI applications are used for **creative processes** (e.g. for the design of new products), it is questionable whether and to what extent such results created autonomously by an AI application may benefit from legal protection. In the absence of a human *creator*, such work results **cannot**

be protected by copyright, and in the case of protection under the Designs Act (DesA) the question arises as to who is considered to be the *designer*: the manufacturer of the AI application, its trainer, the supplier of the input data, or the person who uses the AI application? This makes it all the more important to have suitable contractual regulations in place for the use of the AI application and for the use of the work results it generates.

3 Conclusion

AI applications are extremely versatile tools and have great potential, but they also entail numerous **legal risks**. Since legislation does not (yet) take into account the complexity created by AI applications and the specific issues associated therewith, the legal risks should be addressed by **organisational measures** and **contractual provisions** with the parties involved.

Roland Mathys
Partner Zurich
roland.mathys@swlegal.ch

Samuel Klaus
Senior Associate Zurich
samuel.klaus@swlegal.ch

Louis Burrus
Partner Geneva
louis.burrus@swlegal.ch

Olivier Hari
Of Counsel Geneva
olivier.hari@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P. O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.ch

Geneva
15bis, rue des Alpes
P. O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.ch

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg