gli
Global Legal Insights

AI, Machine Learning & Big Data

2020

Second Edition

Contributing Editor:
Matt Berkowitz

glg global legal group

CONTENTS

Austria

Günther Leissler & Thomas Kulnigg
Schönherr Rechtsanwälte GmbH

Trends

Artificial Intelligence (AI), Machine Learning and Big Data are still trending topics in Austria's tech and start-up scene.

AI and Machine Learning

The Austrian Council on Robotics and Artificial Intelligence (ACRAI) has summarised details, facts and figures on the status of AI and Machine Learning in Austria in a comprehensive study published in May 2019.[1] Here are the main takeaways of the study:

- The study identified more than 600 companies in Austria that are active in the area of AI, which is still only a fraction of all Austrian companies.
- Most AI-related companies are software developers, who offer data processing solutions, often in combination with consulting services.
- Approximately a quarter of all identified companies are active in the area of consulting services (business or market consulting), developing their own software solutions to analyse company information, stock prices, etc. Production companies (such as mechanical engineering, plant construction, electrical equipment, pharmaceutical products, sensors, etc.) represented 28% of the identified companies.
- There are further several institutions active in AI, including specific institutions (such as the the Austrian Research Institute for Artificial Intelligence of the Austrian Society for Cybernetic Studies[2]) and larger institutions, such as universities.
- Public subsidies, including Horizon 2020 projects, reached EUR 350 million.[3]
- R&D in AI is generally widely spread throughout Austria (with focus on Vienna, Graz, Linz/Hagenberg and Klagenfurt).
- Start-ups further play an important factor in the AI industry in Austria; they are generally considered as technology leader and competence centres, with AI-as-Service as a potential new business model for start-ups and other players.
- Lack of personnel, for instance neuronal network and software engineers, are one of the major constraints for AI, as well as the cost for obtaining/creating the relevant know-how and the implementation of innovation. Also, the current AI hype may create wrong expectations (and could trigger disappointments). General restraints and lack of data (in the required quality and quantity) are further hurdles and challenges to AI in Austria.

Further, from our perspective as market participants, we see more and more AI/Machine Learning activities by MedTech start-ups, aiming to create artificial doctors, such as radiologists, or automising the interpretation of medicinal test results or images (e.g. retina scans). This area of AI application has become significant recently, with telemedicine generally being on the rise (especially in the current Corona situation). Also, the combination between the distributed ledger technology (a.k.a. the "Blockchain") and AI is a trending topic in Austria (and overall) due to the importance of having tamper-proof databases and logs for the purposes of verifying decisions taken by AI algorithms, in particular when used by authorities or corporations.

By way of an outlook, in its 2020–2024 governmental programme,[4] the Austrian Federal Government promised to foster an eco-system for innovation through connecting start-ups, R&D institutions and public/private media houses to support, *inter alia*, AI technology, with the goal of strengthening the international competitiveness of Austria. It remains to be seen if the promises of the Austrian Federal Government will be kept.

Big Data

It comes with no surprise that in light of the world's data-based attempts to fight the Coronavirus that Austria has also reverted to Big Data and data exploitation mechanisms. As with many other states, Austria attempts to combat the spread of the virus by collecting and evaluating mass data. This approach is inspired by other countries such as, for example:

- Israel: Launch of a cellphone surveillance system. This system allows identifying whether someone has been in contact with a Coronavirus-infected person and to messages that person ("*You were near someone sick with the Coronavirus. You must immediately isolate at home [14 days] to protect your relatives and the public […]*").[5]
- South Korea: Contact tracing. South Korea goes beyond mass alerts in regions of suspected Corona infection. It believes in the efficiency of retracing the latest movements of individuals that have been positively tested for the Coronavirus and to isolate anyone who, according to his/her identified motion pattern, has been in contact with those infected individuals. Such contact tracing includes not only an analysis of the individual's cellphone location data, but also of his/her credit card records, CCTV footage and other available data sources.[6]
- China: China relies on a similar approach. Apps will alert individuals if they had been in contact with infected persons and ask them to stay at home and to contact the local health agency.[7]

Such concepts have proven their effectiveness. Most recent data has shown that the infection rate in South Korea has flattened and China has even announced a zero notice of new infections. The flip side of the coin, however, is a loss of people's privacy.

Austria has taken the middle ground by balancing the effectiveness of such preventive measures against data protection limitations. The outcome has been an amendment to the Austrian Telecommunications Act which entitles the government to request telecommunications providers to send nationwide or regional SMS mass alerts to their users if a public emergency (such as an outbreak of an infectious disease) occurs in that region.[8]

With this, Austria allows compulsory mass alerts but refrains from governmental tracking systems as they are in place in countries like South Korea or China. Instead, comparable systems are made available on a voluntary and non-governmental basis. For example, the Austrian Red Cross (an Austrian rescue service provider) has developed an app which provides several features, including "electronic handshake logs". Such log data shall allow alerts to contact persons of the app user as soon as the app user himself gets positively Coronavirus-tested. However, besides this app being a non-governmental app, it operates on a voluntary basis. In contrast to this, the tracing systems used in China or South Korea are operated on a governmental level and without allowing people to choose whether they want to participate. Also, under the Austrian model, contact persons will only be added to the user's handshake logs if they have agreed to being added. This means the system does not allow the tracing of each and every contact person; rather, only those contact persons who have given consent. In essence, compared to the Asian systems, the Austrian concept accepts lower system efficiency to the benefit of maintaining higher privacy standards.

Also, one of the country's largest telecommunications providers has, on its own initiative, provided the government with large-scale location data of its users in order to allow the government to verify people's acceptance of quarantine orders. However, in order to safeguard users' privacy, the data was anonymised before it had been provided to the government. This was done by creating movement clusters of at least 20 users so that no individual profiles of movement could be extracted from that data.

Ownership/protection

Computer programs may enjoy copyright protection under specific provisions on the protection of computer programs (Section 40a of the Austrian Copyright Act; UrhG). In accordance with the EU Software Directive (Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs), protection applies to the expression in any form of a computer program. However, ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright.

Under current legislation, only natural or legal persons can hold rights; a machine itself may not be the owner of a right. Thus, every intellectual property right must be allocated to a person. In respect to copyright and patent, only natural persons may be the creator or inventor. This can lead to interesting questions in the context of work products created by AI/Machine Learning systems. According to legal theory, either the owner of the algorithm or the person that applied the algorithm becomes the owner of its work products (or both). Alternatively, none of them becomes the owner if their contribution to the AI/Machine Learning system does not qualify as an "intellectual" or "spiritual" creation, and the creation was truly autonomously developed by the system.

Antitrust/competition laws

Current antitrust rules are flexible enough to deal with most competition law problems created by the use of AI/Machine Learning algorithms. There is uncertainty, however, as to whether future developments in digitalisation will necessitate broadening the extent of the cartel prohibition. This notwithstanding, competition authorities need to stay on top of technological developments and keep improving their expertise on algorithms.

Board of directors/governance

There is little discussion going on in Austria regarding whether management decisions of an Austrian company may be taken by AI. This is mainly because under Austrian corporate law, directors remain responsible for their decisions even if the decision is influenced, supported or even taken by an AI application. From a management liability's perspective, it remains to be seen to what extent managers can exculpate themselves on the argument that a decision was based on the results of an AI application. Managers are well advised to double check (at least for plausibility) whether the basis of their decision is adequate in the given circumstances, to avoid any personal liability caused by their decision. This will be particularly difficult in respect to AI algorithms due to the complexity of the underlying technology (e.g. the manager will have to ensure that the results of the application are not influenced by hidden or unwanted factors) and also because AI applications typically use large amounts of data (and it is quite difficulty to verify the quality of the underlying data). It also will need to be ensured that the results of the algorithm can be verified and reproduced, to be able to later audit the decision of the manager. As outlined above, a combination of AI and distributed ledger technologies could provide the basis for such criteria.

Regulations/government intervention

AI and Machine Learning

On 8 April 2019, the High-Level Expert Group on Artificial Intelligence – a supportive body to the European Commission – launched their "Ethics Guidelines for Trustworthy AI". According to the guidelines, Trustworthy AI has three components, which should be met throughout every AI system's lifecycle: AI systems should be (i) lawful, (ii) ethical, and (iii) robust. Thus, legal compliance ("lawfulness") alone shall not be sufficient anymore. Based on this theory, the guidelines aim to offer guidance on ethical and robust AI. These requirements will go through a piloting process expected to conclude with the presentation of a revised document in early 2020; to our understanding, the process is still pending. In Austria, no specific AI regulation has been implemented yet. However, this does not exclude applicability of other frameworks of relevance. Often, AI systems are typically based on the exploitation and the use of data. If such data counts as personal data, the limitations and requirements of the GDPR will apply. Thus, a key AI component is a valid anonymisation of the AI-related database.

Big Data

Features like the "electronic handshake log" (described above), or equivalent, are partly based on the processing of personal data in terms of the GDPR. This is because Art 4 Para 1 GDPR qualifies not only information as personal data that relates to identified persons but also where such data relates to persons that are identifiable. In its decision in the *Breyer* case, the CJEU took a very broad view on the question of whether an individual shall be deemed identifiable. In essence, the court took the view that data shall be deemed "personal" as long as it is not practically impossible or prohibited by law to identify the person the data relates to.[9] Features like the "electronic handshake tool" doubtlessly involve personal data processing. This is the case when the user gets positively Corona-tested and provides through this system this information to the Austrian Red Cross. Such information is not only personal data. In the context of the described system, it describes the health status of the app user and, as such, forms a special category of data in terms of Art 9 GDPR. Since the use of the app is voluntary its data processing requires consent as enshrined in Art 9 Para 2 lit a GDPR. Such consent needs to be freely given and in full knowledge of all the details of the data processing. This seems doable *vis-à-vis* the user of the app. So the Austrian Red Cross has provided comprehensive data protection information which shall form the basis for the app user's consent.[10]

However, things get trickier when it comes to people who get in touch with the app user. In other words, those "contact people" who provide their "electronic handshake" to the app user. Such contact people are identified by the system as soon as the app user discloses that he is infected by the Coronavirus because if the app user has been infected by the Coronavirus his contact people could potentially be infected as well. Therefore, they will receive alerts telling them to isolate themselves. From a data protection perspective, as soon as they become identified by the "relevant" handshakes, their personal contact data gets processed in context with their health status. This is because an indication of a potential COVID-19 infection is arguably information about an individual's health status. This leads to the consequence that such contact persons must declare their consent to their data being processed as personal health data (in case the app user turns out to be infected). The responsibility for obtaining such consent is with the app user, since he is the controller for the "electronic handshake".[11] However, it might be doubtful that the average app user indeed provides such comprehensive information to his/her contact person while performing the "electronic handshake" and that the contact person arguably understands all of the consequences arising from his/her allowance to get captured in the app user's "electronic handshake logs" – with the effect that such consent might potentially be insufficient.

The above shows the pitfalls of a voluntary tracking system. On the one hand, it is by its nature less effective because it does not apply throughout the entire population. On the other hand, for the above reasons, it is not legally sound in all its nuances. An alternative could be the establishment of such systems on a compulsory basis through statutory enactment. This approach has obviously been chosen by countries like China and Israel. Art 9 GDPR does not *per se* prevent states from doing so. In particular, Art 9 Para 2 lit i GDPR allows the processing of special data categories on the grounds of public health interests. However, such processing is only legitimate on the basis of national laws that provide suitable privacy safeguards. So here it is up to the legislator to balance the benefit of compulsory health data processing against the population's privacy interests.

For Austria, the outcome has been that the legislator (at least for now) has not taken any steps further than obliging telecommunications providers to send out SMS alerts to their users upon governmental orders (see above). So, obviously the legislator did not deem the threat of Coronavirus to be severe enough to deprive people of their privacy in such an intrusive manner as it would be the case with compulsory contact tracing. This, however, is merely a snapshot in time and the legislator's evaluation might change if the currently taken measures turn out to be not efficient enough in order to effectively combat the Coronavirus.

Criminal issues

Besides the government's ambitions to reduce the spread of the Coronavirus, there remains a strong element of self-responsibility with each individual. Not complying with quarantine orders or circumventing regional access restrictions might, depending on the case, trigger administrative fines. An even more serious consequence, however, is enshrined in Sections 178 and 179 of the Austrian Criminal Code whereby negligently or deliberately exposing the public to infectious diseases shall be sanctioned by up to one year (in case of negligence) and up to three years (in case of deliberate action) of imprisonment. This adds another consideration to the scenario: Does someone who denies or withdraws consent to the processing of his/her health data arguably impede the efforts to eradicate the Coronavirus and be deemed to be acting negligently within the meaning of the Criminal Code? On an overall view, it should be far off from any criminal liability if an individual refrains from contributing to a data mining process, as it would be the case with an individual denying consent to his participation in a voluntary tracing system. However, there might be scenarios where such liability comes closer than it initially seems. One might imagine a scenario under the discussed Red Cross app where a contact person first agrees to the electronic handshake, but immediately after his handshake was added to the app user's log data he realises that the app user is coughing or sneezing. If that contact person then withdraws his consent in fear of his upcoming isolation, this might come close to what is prohibited under the Austrian Criminal Code. Notwithstanding, of course, the burden of proof aspect since it would be with the state prosecutor to provide evidence for the discussed negligence.

Data anonymisation

The above considerations show that each type of tracing related to personal data processing has its limits. Voluntary tracing meets consent restraints, compulsory tracing means severe loss in privacy. A feasible compromise might be data anonymisation. Data is deemed anonymous if the data does not contain information about individuals. If data is anonymous it can be processed without the limitations of the GDPR, as it has arguably been the case with Austrian telecommunications providers when providing mass user data to the government to allow verification of people's quarantine acceptance. As stated, whether or not data shall be deemed personal depends on whether it relates to an identified or identifiable individual. The Austrian Data Protection Regulator has taken a somehow liberal view on that point. The authority was asked whether data anonymisation can be deemed valid data deletion under the GDPR and has accepted deletion through anonymisation. It is of particular relevance for the present context that in its decision the regulator has explicitly accepted that anonymised data might become identifiable again through future, more enhanced technical means.[12] At least for Austria it seems deducible from those considerations that data can validly be claimed to be anonymous if, for the time being, the data-related individual cannot be identified anymore although that individual's re-identification might become possible in the future. Under this perspective, data mining and data exploitation activities can arguably be carved out of the GDPR's applicability if it is sufficiently ensured that at the time of the processing the individuals' identities can arguably not be determined. This might be the case if data pools, or equivalent anonymisation tools, prevent individualised evaluations. By following the regulator's arguments, it seems not immediately harmful if such anonymisation does not ultimately prevent future de-anonymisation as long as the anonymisation is diligently done at its origin.

* * *

Endnotes

1. https://www.bmvit.gv.at/dam/jcr:abf0cdc3-bd4c-4335-aef9-8e5b0a33c119/ai_potenzial_oesterreich.pdf.
2. http://www.ofai.at/index.html.
3. Between 2012 and 2017.
4. https://www.bundeskanzleramt.gv.at/bundeskanzleramt/die-bundesregierung/regierungsdokumente.html.
5. https://www.npr.org/2020/03/19/818327945/israel-begins-tracking-and-texting-those-possibly-exposed-to-the-coronavirus?t=1585132364406.
6. https://www.nytimes.com/2020/03/23/world/asia/coronavirus-south-korea-flatten-curve.html.
7. https://abcnews.go.com/Business/china-launches-app-combat-coronavirus-spread/story?id=68907706.
8. Section 98a Telecommunications Act, as amended through the Second-Covid-19-Act: https://www.parlament.gv.at/PAKT/VHG/XXVII/A/A_00397/index.shtml.
9. CJEU 19 October 2019, C-582/14.
10. https://www.roteskreuz.at/fileadmin/user_upload/Stopp_Corona_App_DatenschutzInformation__OeRK_24.03.2020_V1.1.pdf.
11. This is supported by the Austrian Red Cross' data protection information which allocates the said controller responsibility to the user.
12. DPA's decision DSB-D123.270/0009-DSB/2018, dated 5 December 2018.

Günther Leissler
Tel: +43 1534 375 0276 / Email: g.leissler@schoenherr.eu

Günther Leissler is a partner with Schoenherr, where he specialises in data protection, telecommunications and life science regulation. Günther heads the Data Protection Group of Schoenherr.

Thomas Kulnigg
Tel: +43 1534 375 0757 / Email: t.kulnigg@schoenherr.eu

Thomas Kulnigg is a partner with Schoenherr, where he specialises in technology M&A and venture capital transactions, start-ups and digitalisation matters. Thomas heads the Technology & Digitalization Group of Schoenherr.

Schönherr Rechtsanwälte GmbH

Schottenring 19, 1010 Vienna, Austria
Tel: +43 1 534 37 0 / URL: www.schoenherr.eu