AI, Machine Learning & Big Data

2019

First Edition

Contributing Editors:
Matt Berkowitz and Joshua Thompson

global legal group

Global Legal Insights

AI, Machine Learning & Big Data

2019, First Edition
Contributing Editors: Matt Berkowitz & Joshua Thompson
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS - AI, MACHINE LEARNING & BIG DATA

2019, FIRST EDITION

Contributing Editors
Matt Berkowitz & Joshua Thompson, Shearman & Sterling LLP

Production Sub Editor
Amy Norton

Senior Editors
Caroline Collingwood
Rachel Williams

General Consulting Editor
Alan Falach

Publisher
Rory Smith

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Matt Berkowitz & Joshua Thompson for all of their assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-912509-79-9
ISSN 2632-7120

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY
July 2019

CONTENTS

Switzerland

Clara-Ann Gordon & Dr. András Gurovits
Niederer Kraft Frey Ltd.

Trends

In Switzerland, the use of artificial intelligence, machine learning and big data continues to increase. It is a fact that digitalisation plays a key role in our daily life, and indirectly puts pressure on all economic stakeholders to follow development.

Artificial intelligence as a whole raises a lot of questions. Therefore, in Switzerland, different institutions are conducting studies to answer questions regarding topics such as ethics and the risks and opportunities of AI innovation.[1]

In addition, the Swiss federal government has funded research programmes on the effective and appropriate use of big data, and has incorporated a new federal working group specialised in artificial intelligence.[2]

According to the latest AI research, the majority of companies are not yet prepared for implementing AI into their businesses, nor do they know how to maximise the use of AI.[3] However, there are some leading tech/telecom companies headquartered in Switzerland that have already started implementing and developing their own AI.

For example, a leading Swiss telecom company is using chatbots in its customer support service, and is offering support for other businesses to implement the use of artificial intelligence, in order to maximise income and respond to market demand.[4]

Moreover, many companies already use intelligent wearables in order to help facilitate their employees' work and improve their results.

Hence, from a pragmatic point of view, the use of AI is trending; whereas from a regulatory perspective, there are still many questions left unanswered.

Ownership/protection

Copyright. Under Swiss copyright law, only works that are considered an intellectual creation with an individual character are protected by copyright (art. 2 para. 1 of the Swiss Copyright Act (CopA)). AI as software generally meets these requirements. However, works created by AI cannot be considered intellectual creations as they are not made by humans. These works currently cannot be copyrighted and the author cannot acquire copyright derivatively.

Copyrighted works are protected for 70 years after the death of the author (or 50 years in the case of computer programs).

Patents. Under Swiss law, patents are granted for new innovations applicable in industry. Anything that is obvious having regard to the state of the art is not patentable (art. 1 para. 1 and 2 of the Swiss Patents Act). AI may be patentable under Swiss law; however, there are issues regarding results created by AI. The assessment of whether these results are obvious,

and therefore patentable, should be carried out from a machine's viewpoint and not a human's one. Moreover, AI cannot be named the inventor, but it also does not act as a mere tool in order for its operator to be named inventor.

Data ownership. Under Swiss law, there are no property rights (in the sense of the Swiss Civil Code) to data, since data is intangible. The Federal Act on Data Protection does not convey ownership to data either, as it only regulates protection against unlawful data processing.[5] Protection of and factual ownership to data could therefore, e.g., come from intellectual property rights such as copyright. As a rule, data can be protected by copyright only if it is considered an intellectual creation with an individual character (see above). However, data generated by machines does not fall under the protection of Swiss copyright law, as it is not recognised as an intellectual creation (art. 2 para. 1 CopA).[6] On a more positive note, databases may be protected by copyright as collected works (art. 4 para. 1 CopA).

De lege ferenda, in doctrine various solutions have been debated for this problem. One solution could be the qualification of data as "*lex digitalis*".[7] Data would then fall under traditional ownership and possession rules, thus would be assigned to an owner who would benefit from all the proprietary rights. The second solution proposes the introduction of ownership protection specifically for data, whereas the last thesis proposes a new intellectual property for data.[8]

Antitrust/competition laws

Algorithms and big data. In Switzerland, protection against unfair competition is assured by the Competition Commission (ComCO) using the legal instruments provided by the Swiss Cartel Act (CartA). Swiss competition law does not contain specific provisions on algorithm-driven behaviour, ergo its general rules apply.

Thus, if, or when, machines collude, under Swiss law only explicit collusion is considered unlawful, unless there is tacit collusion as part of an abuse of market power.[9] Collusion (be it explicit or tacit) requires the subjective component of the "concurrence of will" or "consensus". This component distinguishes unintended mistakes of the algorithm from unlawful intended collusive restrictions of competition.

Under art. 5 para. 3 (a) CartA, agreements between companies on the same level of the production and distribution chain which directly or indirectly fix prices are presumed to eliminate effective competition and are thus prohibited. The same interdiction applies in the case of agreements between undertakings at different levels of the production and distribution chain (art. 5 para. 4 CartA). Therefore, if competitors agree to fix prices using algorithms, or even AI, these agreements are unlawful (i.e. hub and spoke cartel). However, if an algorithm is faulty and makes an unintended mistake, there is no consensus between competitors and there should be no sanction for the company.

Any abuse of a dominant position is unlawful, pursuant to art. 7 CartA. Because algorithmic computer programs can now store, collect and process a large amount of data, antitrust concerns relating to big data also have to be considered. Big data can put companies in dominant positions on the market. The Essential Facilities Doctrine is an example of how big data issues can relate to the abuse of a dominant position. Is data an essential facility to which the owner has to grant its competitors access?

Board of directors/governance

The are no AI- and big data-specific guidelines of which the Board should be aware. In general, Swiss companies need to be aware of the Swiss Code of Best Practices for Corporate Governance when they perform their corporate governance.

The board of a Swiss company (company limited by share or a limited liability company) is responsible for the overall supervision and management, with its duties listed in art. 716a CO. The members of the board of directors are jointly and severally liable for any damages caused by an intentional or negligent breach of those duties.

Regulations/government intervention

There are no specific regulations in relation to artificial intelligence, machine learning or big data. To our knowledge, so far, the Swiss federal government has founded research programmes and established specialised institutions in these fields, but no current or upcoming regulations have been announced.

However, based on a recent study[10] conducted by the Federal Office of Communications, a three-point strategy was proposed which, first, suggests the creation and maintenance of a national data infrastructure that would enable a nationally coordinated and internationally networked infrastructure. Second, the Office calls for stricter privacy and competition law rules for the internet sector in specific. And, thirdly, the implementation of the principle of personal data sovereignty is required as a long-term solution in order to empower data subjects to have better control over their data.

Implementation of AI/machine learning/big data into businesses

AI creates immense opportunities for businesses. However, there is also a great risk of the abusive use of AI.

Legal difficulties which companies would face when implementing AI/big data into their businesses are, in particular, data protection and financial trading rules, as well as regulating liability. Businesses need to plan for a budget for legal structuring of the use of AI/big data, as well as compliance. They should also implement a chapter on AI/big data into their codes of conduct.

Data protection. Big data and AI go hand in hand. On the one hand, AI needs a great amount of data to function and learn. On the other hand, big data techniques use AI to extract value from huge sets of data. Swiss data protection law, however, was not created with AI or big data in mind.[11] The Federal Act on Data Protection is only applicable to the processing of personal data. In particular, factual data and geo data do not fall within the scope of application. Data that is anonymised (meaning that no connection to a person can be established) does not fall under the Federal Act on Data Protection, either. However, since big data facilitates the identification of persons through the inclusion of huge amounts of data, Swiss data protection rules can become applicable even though the processed data was anonymised at some point.[12] Differential Privacy, a method to avoid re-identification of data subjects by adding "randomness" to a data set, can be implemented to avoid this. As soon as the Federal Act on Data Protection becomes applicable, however, the processing has to be in line with the general principles of data processing set out in art. 4 *et seq.* Federal Act on Data Protection, *inter alia*, the principles of lawful processing, good faith, proportionality, purpose limitation, etc. Compliance with the transparency prerequisite and obtaining consent for data processing can be a challenge when big data is concerned, as it is hard to keep track of the processing. The purpose of the data collection also needs to be clearly defined, which can be problematic. The principle of data minimisation is an inherent contradiction to how big data works, as big data only functions by processing huge amounts of data over a long period of time. The same is true for the limitation of the retention period for data.[13]

Financial trading. Market manipulation by AI/algorithms has to be avoided pursuant to art. 143 of the Financial Market Infrastructure Act. Therefore, it is prohibited to use algorithmic trading to give out false or misleading signals regarding the supply of, demand for or market price of securities. Supervised institutions that engage in algorithmic trading must employ effective systems and risk controls to ensure the avoidance of such misleading signals.[14] Art. 31 of the Swiss Financial Market Infrastructure Ordinance (FMIO) then requires market participants that pursue algorithmic trading to record all orders and cancellations, and to possess effective precautions and risk controls that ensure that their systems do not cause or contribute to any disruptions in the trading venue.

Liability. As the situation regarding liability can be unclear (see below), businesses are advised to contractually regulate responsibility and liability for any damages caused by AI/big data.

Other legal issues/examples. As businesses implement AI/big data into their daily business, they need to ensure that they are compliant with the law. For example, big data is nowadays often used in the hiring process ("hiring by algorithm"). Therefore, labour law provisions also have to be adhered to. When algorithms make hiring decisions, the person responsible has to ensure that the algorithm does not discriminate against anyone (i.e. based on age, sex, nationality, etc.). Data-related rights of employees, pursuant to art. 328b CO, also play a key role. The provision sets forth that the employer may only handle data to the extent that such data concerns the employee's suitability for the job, and are necessary for the performance of the employment contract.[15]

Civil liability

There are no specific provisions under which an employer could be held liable for damages caused by artificially intelligent machinery. General civil liability rules are applicable.

Contractual. Contractual liability plays a key role, as many AI services will be provided under agency contracts pursuant to art. 394 *et seq.* CO. In this context, as well as generally, Swiss doctrine is discussing the widening of the concept of "faithful performance", which includes human supervision of AI. It is, however, unclear how far this supervision should go. Regarding sales contract liability, it is the seller that is liable for any hardware errors of an AI robot (art. 197 CO).[16] Moreover, doctrine is debating the possibility of disclaiming liability for subcontractors such as software suppliers in general terms and conditions.[17]

Non-contractual. Art. 41 CO generally regulates civil liability for damages incurred not in relation to contracts. The person who causes the loss or damage is obliged to provide compensation. The proof of burden for any such loss or damage lies with the injured party. Art. 55 CO regulates the liability of employers for any loss or damage caused by employees or ancillary staff in the performance of their work. Furthermore, the Swiss Product Liability Act regulates liability specifically for damages incurred by faulty products. Software as a product can fall under the provisions of the Product Liability Act.

If AI causes damages in Switzerland, we need to distinguish whether such damages were caused by a faulty product, mistakes the AI made on its own, or through willful programming.

In the case that the AI makes a mistake on its own, the producer is not liable because he cannot be held responsible for the "decisions" of the product. If, however, damages are incurred due to product defects of the AI (i.e. faulty programming), the producer is liable under the Product Liability Act or art. 55 CO. Product safety liability should also be

considered. The injured party can, therefore, file claims against the producer and seek compensation.[18]

Moreover, it is important to take into account whether the manufacturer of the software and the producer of the end-product are different entities. In this case, the manufacturer cannot be held responsible for the damages caused by the end-product.

Specifically, liability for accidents caused by self-driving cars can be allocated to the driver as well as the owner, according to art. 58 of the Swiss Road Traffic Act. The owner's liability is a liability for the consequences, and is not dependent on any culpability on the part of the owner.[19]

Each case is different; for example, factors like when the product was released on the market could play a role when assigning civil liability, therefore a case by case analysis is recommended.

Criminal issues

Under the Swiss Criminal Code, there are no specific provisions regarding felonies or misdemeanours committed by artificial intelligence. General Swiss criminal law applies.

Swiss criminal law requires the personal culpability of the offender. If an AI robot or system commits a criminal act, it cannot be criminally liable under the current and traditional Swiss criminal law doctrine. The same is true if AI causes someone to commit a crime. Therefore, attribution of the criminal act to the creator/programmer or the user of the AI robot or system should be considered. If an AI robot or system was intentionally programmed to commit a criminal act, the creator or programmer is criminally liable. If it was programmed correctly but intentionally used in a way that resulted in the committing of a criminal act, the user is criminally liable. The creator/programmer as well as the user can only be punished for the negligent commission of a criminal offence if negligence is also explicitly punishable for such criminal offence.[20]

Under art. 102 of the Swiss Criminal Code, it is even possible to assign criminal liability to a corporation if the activity cannot be attributed to a natural person, and if the criminal offence was committed in the exercise of commercial activities in accordance with the object of the undertaking. The undertaking can be fined up to CHF 5 million for such liability. If AI commits a felony or misdemeanour and the requirements mentioned above are met, the corporation using the AI can be held liable.

Discrimination and bias

Under Swiss law, there are no applicable regulations in relation to discrimination and bias of machines. The logic discussed above may apply accordingly.

National security and military

In Switzerland, artificial intelligence is being used by the military, but so far there are no specific laws relating to AI, machine learning or big data.

* * *

Endnotes

1. SECO press release "*The pros and cons of artificial intelligence*", https://www.seco.admin.ch/seco/en/home/seco/nsb-news.msg-id-71639.html.

2. The Swiss Confederation on "*The Swiss Digital Action Plan*", 5 September 2018; also see The Swiss Confederation on "*Digital Switzerland Strategy*", September 2018.
3. Philipp A. Ziegler "*MSM Research AG - Research at a glance – Artificial Intelligence*", November 2018.
4. Joachim Hackmann "*Trends for 2019: How companies can use data better*", Teknowlogy Group, January 2019, commissioned by Swisscom and Teknowlogy/PAC.
5. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 634.
6. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 630.
7. Dr. Martin Eckert, LL.M. on "*Daten als Wirtschaftsgut – wem gehören digitale Daten*", 2016.
8. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 631.
9. Peter Georg Picht and Benedikt Freund on "*Wettbewerbsrecht auf algorithmischen Märkten*", sic!, November 2018, 669.
10. Prof. Thomas Jarchow and Beat Estermann on "*Big Data: Opportunities, risks and need for action by the Confederation*" – results of a study commissioned by the Federal Office of Communications.
11. Martina Arioli on "*Daten als Treibstoff selbstlernender Systeme, Ist der Datenschutz den neuen Herausforderungen gewachsen*", presentation dated 28 September 2018.
12. Astrid Epiney on "*Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?*", Jusletter IT, 21 May 2015.
13. Martina Arioli on "*Daten als Treibstoff selbstlernender Systeme, Ist der Datenschutz den neuen Herausforderungen gewachsen*", presentation dated 28 September 2018.
14. FINMA Circular 2013/8 on "*Market conduct rules*".
15. Isabelle Wildhaber on "*Robotik am Arbeitsplatz: Robo-Kollegen und Robo Bosse*", AJP 2017, 215 *et seq*.
16. Melinda F. Lohmann on "*Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse*", AJP 2/2017, 157.
17. Marco J. Minder on "*Artificial Intelligence: Eine Bestandesaufnahme im Jahr 2018*", sic!, 2019, 51.
18. Silvio Hänsenberger on "*Die Haftung für Produkte mit lernfähigen Algoritmen*", Jusletter, November 2018.
19. Dr. Martin Eckert and Luca Hitz on "*Selbstfahrende Autos: Zulässigkeit, Haftung und Datenschutz*", https://www.mme.ch/de/magazin/selbstfahrende_autos_zulaessigkeit_haftung_und_datenschutz/.
20. Nora Markwalder and Monika Simmler on "*Roboterstrafrecht*", AJP 2/2017, 173 *et seq*.

Clara-Ann Gordon
Tel: +41 58 800 80 00 / Email: clara-ann.gordon@nkf.ch

Clara-Ann Gordon is specialised in the areas of TMT/outsourcing, data privacy, internal investigations/e-discovery and compliance. She regularly advises clients in the above areas on contractual, governance/compliance and other legal matters, represents clients in transactions and before the competent regulatory and investigating authorities as well as before state courts, arbitral tribunals and in mediation proceedings, and renders opinions on critical regulatory and contract law topics in the said industry-specific areas.

She has advised on and negotiated a broad range of national and international IT, software and outsourcing transactions (also in regulated markets), has represented clients in technology-related court proceedings and international arbitration, and is experienced in data protection and secrecy laws, white-collar investigations and e-discovery, telecom regulations (including lawful interception), e-commerce, and IT law.

Ms. Gordon regularly publishes in the field of technology (ICT) and frequently speaks at national and international conferences on emerging legal issues in technology law.

Dr. András Gurovits
Tel: +41 58 800 80 00 / Email: andras.gurovits@nkf.ch

András Gurovits specialises in technology (IT, telecoms, manufacturing, regulatory) transactions (including acquisitions, outsourcing, development, procurement, distribution), data protection, corporate, dispute resolution (including administrative proceedings) and sports.

He regularly advises clients on contractual, compliance, governance, disputes and other legal matters in the above areas.

Thus, he not only advises in these areas, but also represents clients before the competent regulatory and investigating authorities, state courts and arbitral tribunals.

Dr. Gurovits is distinguished as a leading lawyer by various directories, such as *Chambers* and *The Legal 500*. Dr. Gurovits has been a lecturer at the University of Zurich for more than a decade. Presently, he is a listed arbitrator with the Court of Arbitration for Sport CAS/TAS in Lausanne and member of the Legal Committee of the International Ice Hockey Federation.

Niederer Kraft Frey Ltd.

Bahnhofstrasse 53, 8001 Zurich, Switzerland
Tel: +41 58 800 80 00 / URL: www.nkf.ch

Other titles in the **Global Legal Insights** series include:

- **Banking Regulation**
- **Blockchain & Cryptocurrency Regulation**
- **Bribery & Corruption**
- **Cartels**
- **Commercial Real Estate**
- **Corporate Tax**
- **Employment & Labour Law**
- **Energy**
- **Fintech**
- **Fund Finance**
- **Initial Public Offerings**
- **International Arbitration**
- **Litigation & Dispute Resolution**
- **Merger Control**
- **Mergers & Acquisitions**
- **Pricing & Reimbursement**

Strategic partner: