GLI GLOBAL LEGAL INSIGHTS

AI, Machine Learning & Big Data

2021

Third Edition

Contributing Editors: **Matt Berkowitz & Emma Maconick**

glg global legal group

Global Legal Insights
AI, Machine Learning & Big Data

2021, Third Edition
Contributing Editors: Matt Berkowitz & Emma Maconick
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – AI, MACHINE LEARNING & BIG DATA

2021, THIRD EDITION

Contributing Editors
Matt Berkowitz & Emma Maconick, Shearman & Sterling LLP

Head of Production
Suzie Levy

Senior Editor
Sam Friend

Production Editor
Jane Simmons

Publisher
James Strode

Chief Media Officer
Fraser Allan

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Matt Berkowitz & Emma Maconick of Shearman & Sterling LLP 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 978-1-83918-116-0
ISSN 2632-7120

Printed and bound by TJ Books Limited
Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
May 2021

CONTENTS

Switzerland

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

Trends

In Switzerland, the use of artificial intelligence (AI), 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.

AI 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 incorporated a federal working group specialised in AI.[2] On behalf of the Federal Council, this working group examined the challenges of AI and need for action. Although there is still room for improvement in a number of areas, the report (published in December 2019) shows that Switzerland is well positioned for the application and challenges of AI.[3] The legal framework in Switzerland is generally sufficient to meet the new challenges posed by AI and there is currently no need for fundamental adjustments.[4] Nevertheless, applications for AI that challenge the legal system in certain areas are emerging.[5] In this light, the Federal Council has developed strategic guidelines regarding AI for the federal administration, which were published in November 2020.[6] The Federal Council has also committed to the Digital Switzerland Strategy as well as the Digital Foreign Policy Strategy 2021–2024. Within the Digital Switzerland Strategy, specific goals regarding data, digital contents and AI have been set, such as, e.g., optimising framework conditions for a transparent and responsible use of artificial intelligence.[7]

Switzerland is known for having the highest number of AI companies per capita in Europe.[8] However, 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.[9] Still, there are a good number of leading tech/telecom companies headquartered in Switzerland that are 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 AI, in order to maximise income and respond to market demand.[10] 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 questions left unanswered. When dealing with new and innovative digital technologies, Switzerland follows the following principles:

- Bottom-up approach: Switzerland wants to provide an optimal, innovation-friendly environment for the development of new technologies, while leaving the choice of specific technologies to individual actors.

- Application perspective: When assessing new technologies, the focus is on application and its effects. Regulation with regard to AI should not be based on the technology itself; it only starts where there are gaps or risks to the fundamental rights of the data subjects.
- Technology neutrality: Switzerland pursues a technology-neutral legislative and regulatory approach. Rules should be as competition-neutral as possible. The legal framework should not be geared to individual technologies, but should treat comparable activities and risk – whenever possible – equally.
- Market failure: If there is no market failure and the use of AI lies within the framework of private sector activities, regulation should generally be avoided.
- Legal admissibility: The use of AI *per se* does not justify any need for government action or regulation. The regulatory question only arises when AI affects fundamental rights or causes market failures.
- Special attention to fundamental rights: If fundamental rights are affected by AI or if the current legal system proved inadequate, there is a need for regulatory action.
- Necessary legal basis for government action: The state (administration) and judiciary may in principle use AI as a tool, even if this concerns the legal position of persons, provided that the necessary legal basis exists.[11]

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, even if it was created with the help of AI. However, works solely 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.[12]

It must be clarified how copyright law is to deal with the fact that many forms of AI require enormous amounts of data for the training process, which are at least partially protected by copyright. The data usually has to be duplicated for use by AI, which is basically a copyright infringement. This could represent a considerable hurdle for the development of AI.[13]

Copyrighted works are protected for 70 years after the death of the author (or 50 years in the case of computer programs; art. 29 para. 1 CopA).

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 paras 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. 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 without question. Furthermore, according to prevailing opinion, patent law in Switzerland only permits natural persons as inventors in the legal sense (or legal persons, depending on the interpretation). The recognition of AI systems is excluded due to their lack of legal capacity.[14] The Swiss legal community, therefore, currently recognises that AI-created results can be assigned to a natural person and are patentable.[15]

Data ownership/data protection. 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 (FADP) does not convey ownership to data either, as it only regulates protection

against unlawful data processing.[16] Protection and factual ownership of 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 solely 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).[17] On a more positive note, databases may be protected by copyright as collected works (art. 4 para. 1 CopA).

The revised FADP (which is expected to come into force in 2022) not only increases the right to informational self-determination in the use of information and communication technology, but also improves the transparency of data processing by information and communication technology users. In addition, the control of data subjects over their data and the powers of the Federal Data Protection and Information Commissioner are strengthened.[18] The revised FADP also introduces the definition of "profiling", which covers the automated processing of personal data to evaluate certain personal aspects relating to a natural person (art. 5 let. f revised FADP).

As decisions based on AI systems are often not comprehensible, precautions must be taken to ensure transparency. A form of explainability is therefore also provided for in the revised FADP: the data controller must inform the data subject of any decision taken exclusively on the basis of automated processing of personal data that has legal effects on or significantly affects the data subject (art. 21 para. 1 revised FADP). The data subject may request that the decisions are reviewed by a natural person (art. 21 para. 2 revised FADP). Where data subjects exercise their right to information, the data controller must state that an automated individual decision has been taken and on what logic this decision is based (art. 25 para. 2 let. f revised FADP). Arts 21 and 25 of the revised FADP are not applicable where humans interfere in the decision-making process and where AI merely served as a decision-making aid. Special traceability requirements also exist for non-automated individual decisions of authorities that are made with the help of AI and concern the legal status of a person. If an authority therefore bases its decision on AI, it is essential that the system provides information about the information and criteria it takes into account, the assumptions it makes, and the relevant reasons for the result.[19]

Another challenge arises when companies use AI in their interaction with customers, e.g. via chatbots. These can be used in a variety of ways to answer consumer questions. Since it is possible to talk to a chatbot like a human being, the consumer may not be able to tell that it is a machine. If consumers were not informed in advance about the interaction with AI systems, the Swiss Federal Act against Unfair Competition could be applied in Switzerland.[20]

De lege ferenda, in doctrine various solutions have been debated for this problem. One solution could be the qualification of data as "*lex digitalis*".[21] Data would then fall under traditional ownership and possession rules, and 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.[22]

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.[23] 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

There 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

In November 2020, the Federal Council published their guidelines regarding AI in the federal administration. These guidelines set out seven principles for the use of AI by authorities: (1) putting people at the centre of things; (2) setting framework conditions for the development and use of AI; (3) transparency, traceability and explainability; (4) responsibility; (5) security; (6) active participation in the governance of AI; and (7) inclusion of all relevant national and international actors. The guidelines refer to general Swiss law that can be applied to AI. Moreover, they set out specific guidelines for the areas or politics, education, research and innovation.[24]

There are no other specific regulations in relation to AI, 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[25] 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 specifically. 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 abuse of AI.

Legal difficulties that 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.[26] The FADP is only applicable to the processing of personal data. In particular, factual data and geo data, and under the revised FADP, data of juristic persons, 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 FADP, 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.[27] 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 FADP becomes applicable, however, the processing has to be in line with the general principles of data processing set out in art. 4 *et seq.* FADP, *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.[28] Under the revised FADP, companies will have to set up procedures regarding the right to information on automatic decisions.

Financial trading. Market manipulation by AI/algorithms must 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.[29] 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.). According to the general prohibition of discrimination under labour law in art. 328 CO, algorithms are not allowed to be programmed in such a way that they discriminate directly. They must also not discriminate indirectly, i.e. in spite of neutral regulation they may have disadvantageous effects for different groups of employees (based on race, age, sex, nationality, etc.), unless this is objectively justified and proportionate. However, there are hardly any deterrent sanctions against discriminatory behaviour. It was not until May 2016 that the Federal Council established that there are gaps in the protection against discrimination in private law. The general prohibition of discrimination under labour law is supplemented by special statutory prohibitions of discrimination, which, however, offer only very selective protection: for example, the Gender Equality Act prohibits any direct or indirect discrimination based on sex (art. 3). The Disability Discrimination Act only applies to federal employment relationships, but excludes the area of private-law employment relationships. The general prohibition of discrimination under labour law (art. 328 CO) does not provide a satisfactory solution to address the problem of possible discrimination by algorithms.[30] 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.[31] It is questionable whether the professional element required by art. 328b CO is given if the algorithm takes into account data whose information content lies in the correlation between non-work-related data and work performance.[32]

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).[33] Moreover, doctrine is debating the possibility of disclaiming liability for subcontractors such as software suppliers in general terms and conditions.[34]

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 wilful or negligent 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. Liability for the operation

of autonomous information systems must always be linked to the act or omission of an offender. In addition, machines do not act intentionally (i.e. with knowledge and will), negligently (i.e. without taking into account the consequences of their lack of caution) or culpably (i.e. personally accusable), nor do they develop judgment (i.e. subjective insight, ability to form wills and ability to implement wills).[35] 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.[36]

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.[37] This corresponds largely to the regulation in the Swiss Federal Act on Civil Aviation, which covers, among other things, the flying of drones.[38]

Each case is different; for example, factors like when the product was released on the market could play a role when assigning civil liability, and therefore a case-by-case analysis is recommended. The Federal Council currently considers the existing regulations to be sufficient. So far, the application to robots has not resulted in any gaps in responsibility. However, this assessment does not exclude the possibility that sooner or later the question of specific regulatory requirements will arise. In other cases, the legislator has reacted by introducing a strict liability. Damage caused by the new technology is therefore attributed to a person who will then be responsible for the damage regardless of fault. Anyone who benefits from the new technology should also assume the risks associated with it.[39]

Criminal issues

Under the Swiss Criminal Code, there are no specific provisions regarding felonies or misdemeanours committed by AI. General Swiss criminal law applies. The Federal Council currently also considers the existing provisions in criminal law to be sufficient. In fact, offences committed using robots can be prosecuted like any other crime committed by a person using an object. Thus, as things stand at present, there is no legal loophole that the legislator would have to fill.[40]

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.[41]

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

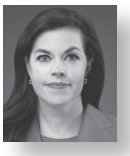
* * *

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. https://www.sbfi.admin.ch/sbfi/de/home/das-sbfi/digitalisierung/kuenstliche-intelligenz.html.
4. https://www.sbfi.admin.ch/sbfi/de/home/aktuell/medienmitteilungen/news-anzeige-nsb.msg-id-77514.html.
5. https://www.sbfi.admin.ch/sbfi/de/home/das-sbfi/digitalisierung/kuenstliche-intelligenz.html.
6. https://www.sbfi.admin.ch/sbfi/de/home/aktuell/medienmitteilungen/news-anzeige-nsb.msg-id-81319.html.
7. https://www.digitaldialog.swiss/en/objectives/switzerland-has-a-modern-coherent-legal-foundation-in-terms-of-the-rights-to-data-and-its-use.
8. https://asgard.vc/the-european-artificial-intelligence-landscape-more-than-400-ai-companies-made-in-europe/.
9. Philipp A. Ziegler "*MSM Research AG – Research at a glance – Artificial Intelligence*", November 2018.
10. Joachim Hackmann "*Trends for 2019: How companies can use data better*", Teknowlogy Group, January 2019, commissioned by Swisscom and Teknowlogy/PAC.
11. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 34–36.
12. Markus Christen *et al*., *Wenn Algorithmen für uns entscheiden: Chancen und Risiken der künstlichen Intelligenz*, in TA-SWISS Publikationsreihe (Hrsg.): TA 72/2020, Zürich: vdf, 129f.
13. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 40.
14. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 40.

15. Markus Christen *et al*., *Wenn Algorithmen für uns entscheiden: Chancen und Risiken der künstlichen Intelligenz*, in TA-SWISS Publikationsreihe (Hrsg.): TA 72/2020, Zürich: vdf, 128f.
16. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 634.
17. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 630.
18. Bundesamt für Kommunikation BAKOM, Geschäftsstelle Digitale Schweiz GDS, Aktionsplan, Digitale Schweiz, November 2019, 38.
19. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 37–38; Federal Council on "*Guidelines "Artificial Intelligence" for the federal administration*", November 2020, 4–5.
20. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 38.
21. Dr. Martin Eckert, LL.M. on "*Daten als Wirtschaftsgut – wem gehören digitale Daten*", 2016.
22. Alan Schmid, Kirsten Johanna Schmidt, Herbert Zeck on "*Rechte an Daten – zum Stand der Diskussion*", sic!, November 2018, 631.
23. Peter Georg Picht and Benedikt Freund on "*Wettbewerbsrecht auf algorithmischen Märkten*", sic!, November 2018, 669.
24. Federal Council on "*Guidelines "Artificial Intelligence" for the federal administration*", November 2020, 3–6.
25. 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.
26. Martina Arioli on "*Daten als Treibstoff selbstlernender Systeme, Ist der Datenschutz den neuen Herausforderungen gewachsen*", presentation dated 28 September 2018.
27. Astrid Epiney on "*Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?*", Jusletter IT, 21 May 2015.
28. Martina Arioli on "*Daten als Treibstoff selbstlernender Systeme, Ist der Datenschutz den neuen Herausforderungen gewachsen*", presentation dated 28 September 2018.
29. FINMA Circular 2013/8 on "*Market conduct rules*".
30. Isabelle Wildhaber/Melinda F. Lohmann/Gabriel Kaspar on "*Diskriminierung durch Algorithmen – Überlegungen zum schweizerischen Recht am Beispiel prädikativer Analytik am Arbeitsplatz*", ZSR vol. 138 (2019) I issue 5, 459, 470–471.
31. Isabelle Wildhaber on "*Robotik am Arbeitsplatz: Robo-Kollegen und Robo Bosse*", AJP 2017, 215 *et seq*.
32. Isabelle Wildhaber/Melinda F. Lohmann/Gabriel Kaspar on "*Diskriminierung durch Algorithmen – Überlegungen zum schweizerischen Recht am Beispiel prädikativer Analytik am Arbeitsplatz*", ZSR vol. 138 (2019) I issue 5, 459, 479.16.
33. Melinda F. Lohmann on "*Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse*", AJP 2/2017, 157.
34. Mario J. Minder on "*Artificial Intelligence: Eine Bestandesaufnahme im Jahr 2018*", sic!, 2019, 51.

35. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 36.
36. Silvio Hänsenberger on "*Die Haftung für Produkte mit lernfähigen Algoritmen*", Jusletter, November 2018.
37. 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/.
38. Markus Christen *et al*., *Wenn Algorithmen für uns entscheiden: Chancen und Risiken der künstlichen Intelligenz*, in TA-SWISS Publikationsreihe (Hrsg.): TA 72/2020, Zürich: vdf, 121.
39. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 36–37.
40. Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF on "*Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe 'Künstliche Intelligenz' an den Bundesrat*", December 2019, 36–37.
41. 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 (incl. administrative proceedings) and sports.

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

He, thus, 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. He is also a member of the board of directors of Grasshopper Fussball AG.

Niederer Kraft Frey Ltd.

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

www.globallegalinsights.com

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

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

GLI GLOBAL LEGAL INSIGHTS