gli
Global Legal Insights

AI, Machine Learning & Big Data

2020

Second Edition

Contributing Editor:
Matt Berkowitz

glg global legal group

CONTENTS

Japan

Akira Matsuda, Ryohei Kudo & Haruno Fukatsu
Iwata Godo

1 Trends

1.1 Overview of the current status of AI in Japan

The Japanese government and private sector are making huge investments in artificial intelligence ("AI") technologies as key drivers of future competitiveness in Japan's aging society after the decrease in birth rate. Several policy and funding programmes are being implemented by Japanese governmental authorities. Under such governmental initiatives, the collection of big data through IoT and the development of data analysis technology through AI are making rapid progress in Japan.

Not only computers and smartphones but various types of equipment and devices, such as vehicles and home appliances, are connected to the Internet, and the digital data collected via such equipment and devices is utilised.

Technologies being utilised for business purposes include: mobility, mainly automated driving; smart cities and smart homes and buildings (big data provides infrastructure managers and urban planners with invaluable information on real-time energy consumption which makes it easier to manage urban environments and devise long-term strategies); and healthcare and wellness for healthy lives. In addition, many domains and business sectors, such as manufacturing, production control (and supply chains generally), medical/chirurgical treatment, nursing, security, disaster management and finance are also seeking to maximise synergies with the IoT and AI.

Under these circumstances, the Japanese government has announced a general policy regarding the use of AI and IoT described in section 1.2 below, and discussions are being held focusing on certain key legal issues described in section 1.3 arising from the use of AI and machine learning.

1.2 The government's view

The Japanese government established an Artificial Intelligence Technology Strategy Council in 2016, which published the Artificial Intelligence Technology Strategy in March 2017. Furthermore, in January 2016, the government issued its 5th Science and Technology Basic Plan (2016–2021) that sets out the goal for Japan to lead the transition from "industry 4.0" to "society 5.0", in which all aspects of society (not just manufacturing and other industries) are transformed by new information technologies and systems.

In May 2018, the Cabinet Office adopted the "Declaration to be the World's Most Advanced IT Nation and the Basic Plan for the Advancement of Public and Private Sector Data Utilization", which also outlines the government's policy to advance technologies using AI and IoT. Based on the updated Declaration in June 2019, the Japanese government published

"AI Strategy" in July 2019, which contains measures which the Japanese government should implement promptly under governmental initiatives in order to utilise AI and IoT for resolution of social problems.

Although companies using AI were expected to exercise self-restraint and avoid aggressive development, the "Conference toward AI Network Society of the Ministry of Internal Affairs and Communications" published the Draft AI Research & Development Guidelines in July 2017 and the Draft AI Utilization Principles in July 2018. In August 2019, the Conference published the "AI Utilisation Guidelines" which were based on and elaborate the "AI Utilisation Principles". These guidelines and principles cover matters to be kept in mind in order to reduce risks associated with systems using AI, such as the opaqueness of AI's determination processes and loss of control.

In December 2018, the government's "Conference on Principles of Human-centric AI Society" published seven core AI principles, including corporate accountability, to ensure process transparency when a company takes decisions through the use of AI technology.

1.3 Key legal issues

Key issues around AI are outlined below. Issues arising under intellectual property law, civil law, personal information/data privacy law, and competition law are covered in sections 2–6.

1.3.1 Contract regarding utilisation of AI technology and data

In order to promote and facilitate the free flow of data and utilisation of AI among businesses, the Ministry of Economy, Trade and Industry formulated the Contract Guidance on Utilization of AI and Data ("Contract Guidance") in June 2018. The Contract Guidance identifies key elements that businesses should focus on in establishing fair and appropriate rules governing data utilisation, provides a rationale for each specific use category and explains approaches that businesses should consider in negotiating and coordinating the details or terms of contract. The Contract Guidance includes an AI section and a data section. A brief outline is provided below. This Contract Guidance was updated in December 2019 in order to reflect the 2018 amendment of the Unfair Competition Prevention Act ("UCPA").

1.3.1.1 Outline of the Contract Guidance (AI Section)

The Contract Guidance classifies typical contractual formulation issues into three types:

(a) Issue 1.
Issue: Who owns the rights to AI technology development deliverables: the vendor; the user; or both?
Solution: For each item, such as raw data, machine learning datasets and AI products, the Contract Guidance defines intellectual property rights and methods to establish rights and terms of use.

(b) Issue 2.
Issue: How should provisions concerning the utilisation and protection of data be stipulated?
Solution: The Contract Guidance identifies important points to consider in selecting a data trade intermediary (neutrality, income for stable operations, obligations and responsibilities with respect to security and transparency, etc.), and several alternative methods that may be used to determine the scope of use and restrictions according to the nature and type of data (confidentiality, frequency of provision, etc.).

(c) Issue 3.
Issue: Who assumes responsibility for the performance of models and how is this achieved?

Solution: The Contract Guidance proposes a method to limit the scope of responsibility of vendors based on the understanding that it is difficult to ensure the seamless performance of models.

1.3.1.2 Outline of the Contract Guidance (Data Section)

The Contract Guidance categorises data utilisation contracts into three types ((i) data provision, (ii) data creation, and (iii) data sharing), and explains the structures, legal nature, issues, proper contract preparation process, and provides model contract clauses for each contract type.

(i) Data provision type contracts: One party which owns the data grants the other party the right to the data.

(ii) Data creation type contracts: The parties create/compile the new data together and negotiate their respective rights and obligations to utilise the new data.

(iii) Data sharing type contracts: The parties share data using a platform which aggregates, stores, processes, and analyses data.

1.3.1.3 Considerations regarding cross-border transfers

The Contract Guidance also provides points of note regarding cross-border transfers, including the determination of the law applicable and the selection of a dispute resolution method, and how to comply with overseas regulations on data transfers (such as the PRC's Cyber Law or the GDPR).

1.3.2 Criminal liabilities for traffic accidents caused by automated driving cars

In Japan, criminal liabilities for traffic accidents caused by automated driving cars are discussed with reference to five different levels based on the degree of control/autonomy of vehicles which have been proposed by the Automobile Engineering Society. Levels 0 to 2: automated functions only assist driving by drivers who are natural persons, which means that drivers (natural persons) remain in control of the driving. Therefore, traditional legal theories apply to accidents in those cases. Traffic accidents caused by Level 3 or higher automated driving systems are discussed below.

1.3.2.1 Level 3

At Level 3, the system performs all driving tasks, but drivers need to respond to requests for driving instructions from the systems or to failures. Drivers are still obliged to look ahead and concentrate while the systems perform the main driving tasks.

1.3.2.2 Level 4 and Level 5

At Level 4 or higher, natural persons are not expected to be involved in the driving and are not obliged to anticipate or take action to avoid traffic accidents. Therefore, the issue of the drivers' criminal liability does not arise.

The main points of discussion are as follows: is it appropriate to hold AI liable criminally by considering that AI has capacity to act and can be held responsible/accountable? Does it make sense to recognise AI's criminal liability? And, how can AI designers and manufacturers be held criminally liable on account of product liability when the product is partially or completely controlled by AI?

1.3.3 Labour law issues

1.3.3.1 Issues relating to the use of AI for hiring and personnel evaluation purposes

As companies have wide discretion in hiring personnel and conducting performance evaluations, it is generally considered that the utilisation of AI in this HR context is not illegal in principle. However, legal or at least ethical problems could arise if the AI analysis is inappropriate, and would, for instance, lead to discriminatory treatment. This point is actively debated.

Another bone of contention is whether companies should be allowed to use employee monitoring systems using AI for the purposes of personnel evaluation, and the health management of employees from a privacy perspective.

1.3.3.2 Labour substitution by AI

Another point actively discussed is the replacement of the labour force by AI (robots in particular) and whether the redeployment and transfer of employees to another department, or their discharge because of labour substitution by AI where it leads to the suppression of a department, can be permissible. However, these discussions are part of the traditional employment law discussions on redundancies.

2 Ownership/intellectual property rights regarding AI

2.1 Overview

AI draws on developments in machine learning and rapid advances in data collection and processing. The process for developing machine learning/algorithms and statistical models using AI and outputting AI products utilising these models involves the handling of valuable information such as data, programs, and "know-how" (see section 2.2.1 below for the summarised contents of the recent amendment to the Copyright Act).

2.2 Learning stage

2.2.1 Raw data

A huge amount of "raw data" is collected and accumulated by cameras and sensors installed and operated for business activities, as well as by using methods such as data input. Such raw data will be subject to data protection regulation in Japan, where a specific individual's personal information is distinguishable from such raw data.

When the raw data corresponds to works such as photographs, audio data, video data, and novels, creators of these works acquire the copyrights, unless otherwise agreed by contract. Accordingly, using such raw data without permission of the copyright holders can be a copyright infringement.

However, the Copyright Act was amended to ensure flexibility and legal certainty for innovators which became effective on January 1, 2019, introducing the following three provisions and removing perceived copyright barriers to AI:

- New Article 30-4, which allows all users to analyse and understand copyrighted works for machine learning. This means accessing data or information in a form where the copyrighted expression of the works is not perceived by the user and would therefore not cause any harm to the rights holders. This includes raw data that is fed into a computer program to carry out deep learning activities, forming the basis of AI.
- New Article 47-4, which permits electronic incidental copies of works, recognising that this process is necessary to carry out machine learning activities but does not harm copyright owners.
- New Article 47-5, which allows the use of copyrighted works for data verification when conducting research, recognising that such use is important to researchers and is not detrimental to rights holders. This Article enables searchable databases, which are necessary to carry out data verification of the results and insights obtained through text and data mining.

In contrast, when raw data can be deemed as “trade secrets” satisfying all requirements, namely, confidentiality, non-public nature, and usefulness (Article 2, Paragraph 6 of the UCPA), such raw data is protected under the UCPA.

With the revision to the UCPA which became effective on July 1, 2019, big data, etc. that does not qualify as trade secrets but that is subject to certain access restrictions (such as ID and password setting) or restrictions limiting data supplies to third parties will also be protected under the UCPA, as “data subject to supply restrictions”.

Raw data that does not correspond to works, trade secrets, or data subject to supply restrictions cannot be protected under the Copyright Act or the UCPA. Accordingly, companies that wish to secure legal protection for raw data *vis-à-vis* third parties need to secure protection through contracts made with the third parties (i.e. terms of use).

2.2.2 Training data

The collected and accumulated raw data is then processed and converted into “training data”, which is data aggregated in a format suitable for AI machine learning.

The training data obtained by subjecting the raw data to processing and conversion, such as pre-processing for learning and adding of correct answer data, can be protected under the Copyright Act as “database works” (Article 12-2 of the Copyright Act) if the training data constitutes an intellectual creation resulting from “the selection or systematic construction of information”. That is, the creator of the training data is the copyright holder, unless otherwise agreed by contract.

“Know-how” relating to a method for processing the raw data into a dataset suitable for learning by AI shall be protected under the UCPA if the processing method falls under the definition of trade secret under the UCPA.

Know-how is often obtained through a process of collaborative operations between the vendor and the user. In such a case, if the contract between the vendor and the user does not provide for any agreement regarding the ownership of the right to the know-how, both the vendor and the user may claim the right to the know-how. Accordingly, in order to avoid disputes, the vendor and the user should expressly agree with each other on the ownership of the right and the terms of use in the contract.

In addition, the description regarding the protection of raw data in section 2.2.1 also applies to training data.

2.2.3 Program for learning

A “program for learning” is a program adapted for the input of training data and the generation of “learned parameters”.

The algorithm of the program for learning is protected under the Patent Act as an invention of a program if it satisfies the requirements for patentability, such as novelty and inventive step.

Also, a “learning approach” that is determined artificially, including the selection of training data, the order, frequency, and combining method of learning, and a method of adjusting parameters, is protected under the Patent Act as an invention of a learning approach if the learning approach satisfies the requirements for patentability.

The source code of the program is protected under the Copyright Act as a program work (Article 2(1)(x) and Article 10(1)(ix) of the Copyright Act) if the source code satisfies the requirements for works. For the copyright of a program work, the so-called “program registration”, such as the registration of a copyright (Article 77 of the Copyright Act), can be made at the Software Information Center (“SOFTIC”).

If a created program for learning or learning approach falls within the trade secret definition under the UCPA, it is protected under the UCPA.

2.2.4 Learned model

2.2.4.1 Learned parameters

In many cases, learned parameters themselves obtained by inputting training data into the program for learning are not protected under the Patent Act, the Copyright Act, or the UCPA.

Accordingly, companies that wish to secure legal protection of the learned parameters in relation to third parties need to consider protecting them, mainly by concluding contracts with the third parties to whom they intend to supply the learned parameters.

2.2.4.2 Inference program

An "inference program" is a program that incorporates the learned parameters and is necessary for obtaining constant results (AI products) as outputs derived from the input data.

In addition, as to the protection of the inference program, the above description regarding the protection of the program for learning also applies.

2.3 Use stage

2.3.1 Overview

When certain data is input to the "learned model", the learned parameters and the inference program are applied to the input data. Regarding this data, the results of predetermined judgment, authentication, assessment, and proposal are computed. Thereafter, the data is output as an "AI product" in the form of voice, image, video, letter or numeric value.

2.3.2 In the presence of creative contribution or creative intent by humans

Under the current legal system, an AI product may be protected under the Copyright Act or the Patent Act as a work or an invention made by a human, if it can be deemed that the "human" using AI is engaged in creative activity using AI as a tool in the process of producing the AI product. In this case, the creator or the inventor is the person engaged in creative activity using AI as a tool.

A situation where creative activity is performed using AI as a tool is similar to a process where, for example, a person uses a digital camera as a "tool", adjusts the focus and the shutter speed to produce a photograph as a work, and the person who has taken the photograph owns the copyright.

Thus, when creative contributions by, or creative intents of, humans are part of an AI product, the "AI user" who has made the creative contribution is basically recognised as the right holder of the AI product under the default rules of the Copyright Act and the Patent Act.

Therefore, unless otherwise agreed by contract, the right holder of training data, the right holder of an AI program or a program for learning, or the right holder of a learned model would not be the creator or the inventor.

Accordingly, where a vendor who provides a platform for product creation by AI wishes to appropriate all or part of the rights to an AI product created by a user, it is necessary to stipulate the ownership of the right to the AI product and in terms and conditions of service or the contract with the user.

2.3.3 In the absence of creative contribution by, or creative intent of, humans

Where there is no human creative activity using AI as a tool, it is currently considered that this AI product should not be regarded as a work or an invention and should not be protected under the Copyright Act or the Patent Act.

At present, as part of the discussion on future legislation, it is asserted that, from the viewpoint of suppressing free riding or securing creative incentives, even AI products obtained without human creative contribution need to be protected by intellectual property rights including copyright. However, such discussions still remain at a very preliminary stage of the legislative debate.

2.3.4 Issues regarding misleading AI-created content

Under current laws, the rights in and to an AI product vary greatly depending on whether human creative contribution is admitted in the AI product production process. However, it is difficult for third parties to distinguish and determine the presence or absence of human creative contribution from the appearance of the AI product.

Accordingly, there could be cases where content which is actually produced by AI and does not fall within the IP definition of a work could be mistakenly treated as a work protected under the Copyright Act, and if the fact that the content is produced only by AI is revealed after a business relationship has been established among many parties, this would destroy licence relationships and undermine business schemes.

3 Competition law

3.1 Overview

How to deal with AI/big data under competition law in Japan is under review, but discussions at regulator level are still at a preliminary stage and not yet reflected in any actual enforcement policy. Currently, mainly two aspects are being discussed: the first is digital cartels (whether the existence of a cartel can be admitted where prices are fixed through the use of algorithms); and the second is the impact of data on anti-competitive effect analysis – especially, data aggregation in the context of large digital platformers such as GAFA, both in the context of merger control and abuse of a superior bargaining position.

The local competition authority, the Japanese Fair Trade Commission (“JFTC”) published a report on data and competition policy in June 2017 (“JFTC Report”). In the JFTC Report, the JFTC has made a detailed analysis of the correlation between data and competition law in Japan, and it is worth noting that the JFTC has made its position clear that if data-driven activity has an anti-competitive effect in a relevant market, such activities will be the target of enforcement in the same manner as traditional anti-competitive activities.

3.2 Digital cartels (algorithms cartels)

In Japan, digital cartels are discussed in accordance with the four categorisations made by the OECD: (i) the computer as messenger; (ii) hub and spoke; (iii) predictable agent; and (iv) autonomous machine. Cartel activity in Japan requires an agreement between the parties, which could be an issue for categories (iii) and (iv). Digital cartels are also covered by the JFTC Report, and the JFTC has made its position clear that if an anti-competitive effect is caused by a digital cartel and cartel requirements are met, the JFTC will crack down on those digital cartel activities. However, so far there have not been any enforcement cases in respect of digital cartels in Japan.

3.3 Data aggregation and anti-competitive effect

According to the JFTC Report, when analysing the anti-competitive effect resulting from the aggregation of data, certain factors must be taken into consideration, such as: (i) whether there is an alternative method to obtain such data; (ii) economic analysis on the usage of data (including its size); and (iii) correlation with AI.

If a company acquires blue chip start-up companies with a small market share from an economic standpoint but having developed cutting-edge technology, software or know-how, such acquisitions could be anti-competitive but fail to show negative implications in a merger control analysis (or could even not be caught by merger control regulations). Furthermore, as a result of the network effect, market entry by new entrants could be hampered. Accordingly, the traditional market definition theory based on market shares from an economic perspective might not work well for the digital market where data plays a far more important role (i.e. free market and multifaceted market). Similarly, in the context of merger control, when a corporation with aggregated data (i.e. digital platformer) is going to merge, when deciding whether it has a dominant position in a given market, it is possible to take into consideration the rarity of the data and whether there are alternative methods to collect such data, in addition to the traditional economic analysis based on past revenue.

These aspects are also discussed in the JFTC Report; however, the regulator is still in the study phase regarding these new theories, and the JFTC's thinking is not yet finalised and reflected in its decisions.

3.4 Latest trends: the JFTC's position on enforcement against digital-related vertical restraints

The JFTC publicly announced in December 2018 that they would carefully watch digital platformers in Japan (i.e. GAFA and the likes), looking for horizontal restrictions (i.e. cartels) and vertical restrictions (i.e. abuse of a superior bargaining position (which is a similar concept to "abuse of dominance", but dominance is not required, and the abuse of a superior bargaining position will suffice)). A typical example of abuse of a superior position is a situation in which a party makes use of its superior bargaining position relative to another party with whom it maintains a continuous business relationship to take any act to unjustly, in light of normal business practices, cause the other party to provide money, services or other economic benefits. In connection with this exercise, the JFTC conducted a survey of the contracting practices of large digital platformers in January 2019. In this connection, the Japan Cabinet proposed a Bill for the Digital Platform Transparency Act, which is expected to be adopted in the ordinary Diet session in 2020. This Act would regulate large-scale online malls and app stores, by requiring certain disclosure and to take measures to ensure fairness in operations in Japan.

4 Data Protection

4.1 Overview

The main data protection legislation in Japan is the Act on Protection of Personal Information ("APPI"), which was significantly overhauled in May 2017 to strengthen data protection. Bi-lateral adequacy referrals on cross-border data transfer restrictions between the EU and Japan came into effect on January 23, 2019. We will explain the AI and big data-related issues from a data protection perspective in Japan, by distinguishing three phases: collection; use; and transfer of personal data. Specific rules apply to anonymised data, which are not described here but can be relevant to big data and data mining. The APPI is scheduled to be amended in 2020 and the details for the amendment are expected to be clear in the middle of 2020. It is expected that the concept of pseudonymised personal data would be newly introduced, which will promote the usage of such data in the context of feeding the AI.

4.2 Phase 1: Collection of personal data

Under the APPI, consent from the data subject is not required upon collection of personal data from such data subject (except for sensitive personal data). However, under the APPI, the purpose of use must be either disclosed or notified to the data subject prior to collection, and proper collection of personal data is required. Accordingly, if a business operator is collecting personal data from data subjects in order to use such data for analysis or development of AI-related systems, it should limit the categories of personal data to be collected to the extent reasonably expected by the data subject, and ensure transparency.

4.3 Phase 2: Use of personal data

The use of personal data by the business operator is limited to the purpose of use disclosed or notified to the data subject prior to such use. In case the business operator uses collected personal data for development of AI-related systems or analysis related to AI, such usage must be covered by the disclosed or notified purpose of use of the personal data. If such usage is not covered, the business operator must modify the purpose of use and disclose or notify to the data subject of such modification. We note that in contrast with the GDPR, profiling itself is not regulated under the APPI.

4.4 Phase 3: Transfer of personal data

Under the APPI, if a business operator is transferring personal data to a third party, such business operator must obtain the prior consent of the data subject, unless such transfer is made in conjunction with entrustment, joint use or business succession (i.e. M&A), or such transfer falls under exemptions specified under the APPI (i.e. public interests). In terms of AI-related software or systems, such system or software normally does not contain personal data, and in such case, the transfer of software or systems will not trigger any consent requirement under the APPI.

5 Regulation/government intervention

5.1 Overview

This section covers regulations, including proposed regulations, and government intervention with respect to AI, big data and deep learning.

5.2 Special laws on automated driving

The Japanese government aims for practical use of Level 3 automated driving (see section 1.3.2.1) at express highways and Level 4 automated driving (see section 1.3.2.2) at depopulated areas by around 2020. In order to achieve such goal, the Road Transport Vehicle Act ("RTVA") and the Road Traffic Act ("RTA") were amended in 2019. The following outlines and explains these amendments.

5.2.1 RTVA

(a) After the amendment comes into force, if the automated driving system conforms to safety standards, driving a car using such system on a public road is allowed.

(b) The Minister of Land, Infrastructure, Transport and Tourism sets conditions for using an automated driving system (such as speed, route, weather and time of the day) according to the amended RTVA.

(c) The certification of Director of the District Transport Bureau is newly required for the replacement or repairment of equipment using automated driving technology such as dashboard cameras and sensors.

(d) The permission of the Minister of Land, Infrastructure, Transport and Tourism is newly required for modification of programs used for automated driving systems.

5.2.2 RTA

(a) The definition of "driving" has been expanded to include driving using an automated driving system.

(b) Although using mobile phones with hands and focusing on the screen whilst using a car navigation system was universally prohibited by the RTA before its amendment, the amended RTA allows these actions in automated driving under certain conditions. However, drink driving, sleeping and concentrating on reading and using a smartphone when driving are still prohibited.

(c) Recording and keeping information for confirmation of operating conditions of the automated driving system are newly required.

5.3 Special laws on AI development and utilisation of data

In line with the fast development of AI technology and the increasing significance of data, laws have been enacted or amended to further promote AI development and utilisation of data. For example, the Act on Anonymously Processed Medical Information to Contribute to Research and Development in the Medical Field was enacted in 2017 and came into force in May 2018. Under this law, universities and research institutions can utilise patients' medical information held by medical institutions as big data in a more flexible manner. In addition, the UCPA was amended in 2018, as explained in section 2.2.1 above.

Furthermore, the Telecommunication Business Act and its sub-legislation was amended (effective April 2020) and the duty to place cyber security measures on IoT devices will be imposed. Another amendment is expected in 2020 to introduce its extra-territorial application. Also, as explained in section 3.4 above, the Platform Transparency Act is expected to be adopted in the ordinary Diet session in 2020.

5.4 Guidelines, etc. for AI

In addition to laws and regulations, the government is publishing various guidelines to facilitate the utilisation of AI technology and big data. For details, see section 1.2 (various guidelines by the Japanese government), section 1.3.1.1 (Contract Guidance (AI section)) and section 1.3.1.2 (Contract Guidance (Data section)) above.

6 Civil liability

6.1 Overview

This section covers civil liability issues linked to the utilisation of AI.

6.2 AI and civil liability

When AI causes any damage to an AI user or a third party, the entities that can be held liable may be (1) the AI user, and (2) the AI manufacturer broadly interpreted. With regard to "the AI user", the following issues may arise: (a) whether or not AI should be held liable in tort if it causes any damage to a third party; and (b) what could be the AI user's liability where AI performs a contract on its own. For the "AI manufacturer", liability under the Product Liability Act could arise.

6.3 Liability of AI users

6.3.1 Liability in tort

If an AI user is found negligent with respect to the utilisation of AI, the AI user will be liable for damages in tort (Article 709 of the Civil Code). In determining whether or not the negligence of the AI user can be established, the concept of negligence is not considered to have a different definition or scope especially for the utilisation of AI from the traditional interpretation of negligence.

In order to find AI users negligent, the AI users need to be able to foresee the occurrence of specific results and to avoid such results arising from the act of AI. However, the act of AI is almost unforeseeable for the AI users given that its judgment process is not known to them at all. From this standpoint, it is unlikely that the AI users will be negligent (although being aware of uncontrollable risks inherent in the black box and still using the AI could be negligence).

Nevertheless, there may be a case where AI users are required to perform a certain degree of duty of care for the act of AI. At least at the early stage of AI introduction, it is not appropriate to rely fully on the act of AI and AI users are likely to be required to comply with a certain degree of duty of care by monitoring the act of AI.

6.3.2 Liability under contracts executed by AI

There could be cases in which AI executes a contract; for example, by placing an order automatically after checking the remaining stock of commodities in a household or of products in a factory. When the execution of the contract by AI is appropriate, the contract is regarded as valid. However, if AI makes a mistake in executing the contract (for example, when it purchases unnecessary goods or when the price is significantly higher than as usual), it is questionable whether the AI user should be liable under such contract.

When the AI user entrusts AI with the execution of a contract, it is considered that the user expresses its intention to "sign the contract using AI" to the counterparty. Similarly, the counterparty expresses its intention to "accept the contract offer made by AI". Since the intentions of the AI user and the counterparty match one another, the contract is deemed duly executed between the AI user and the counterparty.

The contract is valid and effective in principle even when a mistake is found in the contract offer made by AI, because the intention of the AI user to "sign the contract using AI" and the intention of the counterparty to "accept the contract offer made by AI" match each other. AI's execution of a contract is considered "invalid due to mistakes" only in exceptional circumstances where the motive of the AI user can be deemed to have been expressed to the counterparty.

6.4 Liability of AI manufacturers

The manufacturer of a product will be liable for the damage arising from the personal injury/ bodily harm or death or loss of damage to property caused by a defect in such product (Article 3 of the Product Liability Act). Accordingly, if AI has a "defect" (i.e. "lack of safety that it should ordinarily provide"), the AI's manufacturer will be liable under the Product Liability Act.

No established view exists at present as to when AI should be regarded as "lacking safety that it should ordinarily provide", and further discussions are expected.

Akira Matsuda
Tel: +81 3 3214 6282 / Email: amatsuda@iwatagodo.com

Akira Matsuda is a partner at Iwata Godo and head of the AI/TMT practice group. He is an attorney-at-law admitted in Japan and based both in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions and capital markets, as well as international disputes (litigation/arbitration). Mr. Matsuda is also advising many Japanese and foreign clients for data security issues, in terms of Japanese laws, Singapore PDPA, and GDPR including structuring of global compliance systems.
A graduate of the University of Tokyo (LL.B.) and Columbia Law School (LL.M.).

Ryohei Kudo
Tel: +81 3 3214 6237 / Email: rkudo@iwatagodo.com

Ryohei Kudo is a partner at Iwata Godo. He is an attorney-at-law (admitted in Japan and New York) and patent attorney. His practice focuses on IP and a wide variety of domestic and international dispute resolution. His practice also includes cross-border transactions, M&A, corporate commercial work, corporate governance, shareholders' meetings, and general corporate law. Before joining Iwata Godo, he worked for the Government of Japan (Ministry of Defense). A graduate of the University of Tokyo (J.D. & LL.B.) and Columbia Law School (LL.M.).

Haruno Fukatsu
Tel: +81 3 3214 6031 / Email: haruno.fukatsu@iwatagodo.com

Haruno Fukatsu is an associate at Iwata Godo. She is an attorney-at-law (admitted in Japan). Her practice focuses on general corporate matters and a wide variety of domestic dispute resolution. Her practice also includes corporate governance, shareholders' meetings and M&A. Additionally, Ms. Fukatsu has advised many clients for data protection and data security issues in terms of Japanese laws and GDPR. She graduated from the University of Osaka (LL.B.) and the University of Kyoto (J.D.).

Iwata Godo

Marunouchi Building 15F, 2-4-1 Marunouchi, Chiyoda-ku, Tokyo 100-6315, Japan
Tel: +81 3 3214 6205 / Fax: +81 3 3214 6209 / URL: www.iwatagodo.com

www.globallegalinsights.com

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

- **Banking Regulation**
- **Blockchain & Cryptocurrency Regulation**
- **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**

ECLA

Strategic partner