Legal 500
Country Comparative Guides 2025

Japan
TMT

Contributor

Nagashima Ohno &
Tsunematsu

Keiji Tonomura

Partner | keiji_tonomura@noandt.com

Minh Thi Cao Koike

Counsel | minhthi_caokoike@noandt.com

Hiroya Nadamoto

Associate | hiroya_nadamoto@noandt.com

Anju Yamamoto

Associate | anju_yamamoto@noandt.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Japan.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Japan: TMT

1. Software – How are proprietary rights in software and associated materials protected?

Under Japanese law, computer software may be legally protected by patents or copyrights.

Under the Patent Act, a computer program, including any information that is to be processed by a computer and is equivalent to a computer program, can be protected where the software program fulfils the requirements of an invention, which is defined as a highly advanced creation of technical ideas utilizing the laws of nature. Registration is required to secure patents or exercise patents with respect to third parties.

While patents protect the ideas underlying computer software, copyrights protect the expression of those ideas. Copyrights provide the copyright owners of certain works (including computer programming works) with certain exclusive rights, including the right to reproduce, distribute, transfer and create derivative works of the software. Registration is not required to secure copyrights or exercise copyrights with respect to third parties, but registration is required to assert the transfer of copyrights against third parties, although conducting such registration is uncommon in practice.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Unless otherwise stipulated in a contract with a software developer or consultant, the patents and the copyrights will vest in the inventor or the creator, respectively.

Notwithstanding the foregoing, under Article 15 of the Copyright Act, if a work of computer programming is created by a person engaging in the business of a corporation at the initiative of the corporation in the course of the performance of his/her duties, the copyright of such work will vest in the corporation unless otherwise stipulated in a contract or elsewhere at the time the work is made. Although the "person engaging in the business of a corporation" is not limited to a person who has entered into an employment agreement with the corporation, external independent contractors and third parties usually do not qualify as such person engaging in the business of a corporation, unless his/her engagement can be deemed substantially the same as employment relationship.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

There are no specific laws applicable to the liability caused by software or computer systems. While the general law for product liability, the Product Liability Act, does not govern intangibles such as software, it may apply to software or computer systems if they are incorporated in hardware products.

4. Software – To the extent not covered by (3) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The Act on Prohibition of Unauthorized Computer Access prohibits unauthorized access including inputting someone else's identification information and evading access control features, and the Penal Code stipulates "Crimes Related to Electronic or Magnetic Records Containing Unauthorized Commands", which includes the act of creation and distribution of computer viruses.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

In Japan, there are no specific laws that directly prohibit, restrict or otherwise govern software transactions or cloud technology. If the data being placed in the cloud is personal data, use of cloud-based services may be considered as constituting the provision of personal data to third-parties under the Act on the Protection of Personal Information ("APPI"), which requires the prior consent of the relevant individual (subject to certain exceptions depending on whether such third-parties are located in or outside of Japan). However, the guidelines

published by the Personal Information Protection Commission ("PPC") provide that the use of cloud services to store personal data does not constitute the provision of personal data to cloud service providers under the APPI as long as it is ensured by contract or otherwise that the cloud service providers will not handle the personal data stored in the cloud and the cloud service providers are properly restricted from accessing such personal data.

Aside from the personal data protection regulations, provision or use of cloud-based services may be subject to other restrictions depending on the nature of the services or the stored data, including consumer protection regulations and sector-specific guidelines in medical and financial sectors, such as Version 2.0 of the Safety Management Guidelines for Providers of Information Systems/Services for Medical Information, published by the Ministry of Economy, Trade and Industry ("METI") in March, 2025. The Information Security Management Guidelines for the Use of Cloud Services (2013), published by METI in March 2014, provides advice for the selection and implementation of appropriate controls from the ISO Q 27002 (code of practice) and guidance for optimal implementation in order to address risks associated with the use of cloud services. Also, the Information Security Measures Guidelines for the Provision of Cloud Services (3rd edition, 2021) published by the Ministry of Internal Affairs and Communications ("MIC") in September 2021, provides advice for cloud service businesses to address risks associated with the provision of IoT or cloud services, the Guidelines for Appropriate Settings for the Use and Provision of Cloud Services published by MIC in October 2022, provides advice for security measures for both users and providers, and the Guidebook for Preventing Mistakes When Setting Up Cloud Services published by MIC in April 2024, provides advice to users of cloud services on measures to prevent mistakes in connection with the set-up of cloud services.

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

It is common for SaaS agreements to have a clause to limit maximum financial liability of a vendor to a customer, while such clause is not typical in a software license agreement. The cap amount is usually set forth as the amount equivalent to the service fee for 6 months or 12 months.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

Among the areas of liability above, wilful or deliberate breaches are typically excluded. Also, according to Article 8(1) of the Consumer Contract Act, clauses that exempt the vendor from all liability or exempt the vendor from part of its liability that arises due to its wilful act or gross negligence are invalid. Other areas of liability may be excluded from the liability cap in cross border contracts, but are typically not excluded in domestic transactions.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

The Software Information Center (SOFTIC) is a major escrow agent for software source codes. As of March 31, 2022, SOFTIC's services had been used only for 395 contracts; given the small number of users, it cannot be said that use of these escrow services is normal practice. SOFTIC also offers services for cloud-based software by receiving deposit of source codes and other materials.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

The Foreign Exchange and Foreign Trade Act provides for a permit system by METI for transactions in which certain technologies, including programs, specified in the Foreign Exchange Order ("Specified Technology" are provided to or in a foreign country. For example, the provision of certain cryptographic technologies in a foreign country is subject to those regulations.

Uploading data containing specified technology to a

cloud server located in a foreign country does not constitute a transaction requiring a permit as long as the purpose is for the cloud service user to use the data for its own purposes. On the other hand, if, in substance, the purpose is to provide Specified Technology to a cloud service provider or a third party, the act of uploading the data is subject to the regulations.

SaaS that provides Specified Technology constitutes a transaction that requires a permit. However, for services that provide a program that is commercially available, a permit is not required if the requirements of the Ministerial Ordinance on Trade Related Invisible Trade, etc. are met (e.g., in the case where it is designed so that technical assistance of the distributor is not required).

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

There are no specific laws that govern IT outsourcing transactions, but general laws could be applicable to outsourcing transactions. For example, under the Act against Delay in Payment of Subcontract Proceeds, etc. to Subcontractors, which aims to protect the interests of subcontractors in a weak bargaining position, large procuring enterprises are obligated to deliver documents to subcontractors that contain matters required by the Act. In addition, if the outsourced individual is treated as the company's own employee, it may violate the Act on Securing the Proper Operation of Worker Dispatching Businesses and Protecting Dispatched Workers. Furthermore, the Act on Optimization, etc. of Transactions concerning Specified Consignees, commonly referred to as the "Freelance Protection Act", which was enforced on November 1, 2024, requires certain business operators that outsource their business to freelancers, among other obligations, to clearly state the conditions of the transaction, to pay the compensation within 60 days, and to establish a system to prevent harassment.

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

Under the Act on the Succession to Labor Contracts upon Company Split, in the case where the parties agree to transfer a certain business (including employees, assets, third-party contracts and/or liabilities) by way of a company split (kaisha-bunkatsu), employees who are primarily engaged in the transferred business but who will not be transferred, and employees who are not primarily engaged in the transferred business but who will be transferred, are entitled to certain opt-out rights concerning their non-transfer or transfer, respectively. The purpose of this law is to protect employees who will be significantly affected by the succession of their labor contract.

Also, in the case where the parties agree to transfer a certain business by way of a business transfer or merger, the parties are recommended to comply with the Guidelines Concerning the Matters That Should Be Noted by Companies upon Business Transfer or Merger, which was established by the Ministry of Health, Labour and Welfare. These Guidelines will be revised as needed to take into account the creation of the Enterprise Value Charge, a collateral system that covers the entirety of the businesses' assets, including intangible assets, under the Act on the Promotion of Cash Flow-Based Lending, which was promulgated on June 14, 2024.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The principal law governing telecommunications networks and services in Japan is the Telecommunications Business Act (the "Act"). The primary purpose of this Act is to ensure the efficient provision of telecommunications services, promote fair competition among service providers, and protect the interests of users. It is notable that the Act also may apply to a foreign entity that provides telecommunications services for customers in Japan from abroad, in which case the foreign entity is required to appoint a representative or agent in Japan.

A summary of the Act is as follows:

- General rules: Telecommunications carriers are prohibited from censorship of information and are required to protect the secrecy of communications.
- Rules related to entry: Please see next question.
- Rules related to consumer protection: The Act provides rules for consumer protection that telecommunications carriers and agents must comply with, such as explaining the terms of service to users,

providing written documents to users, and informing users when intending to suspend or discontinue telecommunications services.
- Rules related to user information: Telecommunications carriers are subject to rules regarding the external transmission of user information. Also, telecommunications carriers providing telecommunications services to a large number of users would be subject to certain rules for the proper handling of specific user information, such as the establishment of information handling policies, and the self-evaluation of handling of specific user information.
- Rules related to telecommunications facilities: Telecommunications carriers who install telecommunications line facilities, and those who provide large-scale paid telecommunications services, are subject to rules concerning telecommunications facilities used for the telecommunications business, such as maintaining compliance with technical standards.
- Rules related to reporting: Telecommunications carriers are required to promptly report when there are certain leaks of specific user information as defined in the Act.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

Those who wish to engage in the telecommunications business must register with or notify MIC in advance according to the content of their telecommunications business. The definition of the telecommunications business that requires registration or notification is complex, but in general, those who (i) install telecommunications line facilities or (ii) mediate others' communications are required to register or notification. For item (i), if the span of the telecommunications line facilities to be installed exceeds the certain threshold, registration is required. In the registration procedure, MIC examines whether the applicant falls under any statutory disqualification grounds, and the standard processing period from application to registration is generally about 15 days. A notification, by contrast, entails no substantive review; operators may commence business simply by submitting the prescribed particulars to MIC before starting operations.Telecommunications businesses that do not fall under either (i) or (ii) (the scope of these telecommunications businesses is broad, including many social networking services, online shopping malls, online search engines, and various online information provision services) do not require registration or notification. However, they must comply with certain regulations under the Act, such as rules related to user information described question 12 above.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

In Japan, the “secrecy of communications" is strongly protected by the Constitution and the Telecommunications Business Act and there is no statute that allows the government to comprehensively collect communications data. Government bodies and law enforcement agencies must follow strict legal procedures to access an individual's communications data, such as call content, email content, call logs, and location data.

The principal laws and legal frameworks governing this access are as follows:

- For criminal investigations, law enforcement agencies require a warrant issued by a judge to obtain communications data.
- The Act on Enhancing Cyber Response Capabilities and related legislation, passed by the Diet in May 2025 and scheduled to come into effect by November 2026, aims to establish a framework for active cyber defense.
    - Scope and Application: This law stipulates that the government can acquire certain communications information to understand the nature of foreign attack infrastructure and cyberattacks against Japan. The scope of data acquisition is limited to communications involving foreign countries (i.e., foreign-to-foreign, foreign-to-domestic, and domestic-to-foreign communications). Communications that are purely domestic are excluded.
    - Types of Data: The data that can be requested is limited to “mechanical information" that does not

reveal the essential content of communications, such as IP addresses, communication logs, and commands.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

In the global field of information and communications, there are de jure standards created by international standardization organizations such as the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC), as well as de facto standards created by private organizations such as the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers, Inc. (IEEE), and the World Wide Web Consortium (W3C). In Japan, in addition to the above organizations, there are private standardization organizations that create voluntary standards, including the Telecommunication Technology Committee (TTC), the Association of Radio Industries and Businesses (ARIB), and the Japan Cable Television Engineering Association (JCTEA).

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Standardization of information and communication services, including connected devices, refers to a series of efforts aimed at achieving common specifications for both hardware and software across networks, including terminal equipment, switches, and multiplexing devices. The effects of standardization include not only ensuring interoperability and interconnectivity but also enabling mass production of equipment and systems, leading to lower prices and increased user benefits. Additionally, it facilitates the efficient provision of information and communication services and promotes competition through the entry of new business operators and manufacturers into the market.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that govern data protection, including a brief explanation of the general purpose of those laws.

The Act on the Protection of Personal Information ("APPI") contains a comprehensive, cross-sectional framework for the protection of personal information, which regulates the use of personal information by both the public and private sectors. The APPI is implemented by cross-sectional administrative guidelines prepared by the PPC. With respect to certain sectors, such as medical, financial and telecommunications businesses, sector-specific guidance and guidelines are published by the relevant governmental ministries jointly with the PPC given the highly sensitive nature of personal information handled in those sectors.

The APPI is scheduled to be reviewed every three years starting in 2022. In 2024, the PPC held discussions on, among others, regulations regarding subjects' consent, reporting and notification of data breaches, handling of children's personal information, regulations concerning biometric data, and supervisory and monitoring measures, including the introduction of fines. However, in 2025, a proposed amendment of the law was postponed, and discussions on the revisions remain ongoing.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Under the APPI, there is no administrative fine for breach of the APPI, although there have been discussions on the introduction of fines in the PPC. However, criminal penalties may be imposed on business operators handling personal information under certain circumstances. The maximum criminal fine that can be imposed on corporations is JPY 100,000,000, in situations where business operators violate either (i) the prohibition against theft or illegal provision of a personal information database or (ii) a PPC order.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

Technology contracts without international elements does not usually refer to external data protection regimes, while they may be referred in cross-border transactions.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

There are two main types of laws that govern cybersecurity; (i) laws on prevention of cyber attacks and mitigation of damage and (ii) laws punishing cyber attacks.

- Law on Prevention of Cyber Attacks and Mitigation of Damage

The principal laws that prevent and mitigate damage from cyber attacks in Japan are the Basic Act on Cyber security (the "Basic Act"), and the Act on the Prevention of Damage Caused by Unauthorized Acts Against Important Electronic Computers (the "Enhancement Act") together with its Enforcement Act (the "Enforcement Act").

The Basic Act establishes the basic principles for cybersecurity measures in Japan and defines the responsibilities of the national government, local governments, and businesses. Under the Basic Act, businesses that operate critical social infrastructure or cybersecurity-related services are obligated to take proactive measures to ensure cybersecurity and to cooperate in cybersecurity measures implemented by the national government or by local governments.

The Enhancement Act and the Enforcement Act were enacted in May 2025 (to be implemented by November 2026).

The purpose of the Enhancement Act and the Enforcement Act is to prevent damage caused by cybersecurity breaches, and their purport is to: (i) strengthen public-private cooperation through incident reporting by core infrastructure operators; (ii) allow administrative agencies to use communication information to understand the actual state of cyberattacks; (iii) establish new procedures for the police and Self-Defence Forces to access and neutralize attackers' servers; and (iv) establish a system to promote government-wide efforts by strengthening existing organizations related to cybersecurity measures and establishing a new coordinating body.

In addition, METI, the Financial Services Agency ("FSA"), the Ministry of Land, Infrastructure, Transport and Tourism ("MLIT"), and other agencies have established guidelines on cybersecurity for certain business entities and business fields. For example, the following guidelines have been established: "Cybersecurity Management Guidelines" (METI, March 2023), "Guidelines on Cybersecurity in the Financial Sector" (FSA, October 2024), and "Guidelines on Ensuring Information Security in Each Important Infrastructure Field" (MLIT).

- Laws Punishing Cyber Attacks

The principal laws which punish cyber attacks are the Penal Code and the Act Concerning Prohibition of Unauthorized Access to Computer Systems.

Specifically, the following acts may constitute the following crimes: (i) creating electronic records related to rights, obligations, or factual proof with the intent to cause errors in another person's business operations constitutes the crime of unauthorized creation of electronic records (Article 161-2 of the Penal Code); (ii) creating or providing computer viruses with the intent to execute them on another person's computer without authorization constitutes the crime of unauthorized creation of electronic records containing malicious instructions (Article 168-2 of the Penal Code); (iii) if data on another person's server is deleted or altered through a cyberattack, this may constitute the crime of destruction of electronic records (Article 258 and 259 of the Penal Code); (iv) if computer data is altered or deleted without authorization, this may constitute the crime of obstruction of business by damaging electronic computers (Article 234-2 of the Penal Code); (v) a person's use of a website or email claiming to be a financial institution in order to defraud visitors of money may subject that person to a charge of computer fraud (Section 246-2 of the Criminal Law); and (vi) If a person obtains IDs or passwords unlawfully and accesses another person's management page or account, they may be charged with violation of the Unlawful Access Prevention Act (Article 3 of the Act Concerning Prohibition of Unauthorized Access to Computer Systems).

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

Under the Basic Act, the obligations of business operators are merely best efforts obligations and there is no administrative fine for breach of the Basic Act.

However, under the Enhancement Act and the Enforcement Act, criminal penalties may be imposed on business operators under certain circumstances. The

maximum criminal fine that can be imposed on corporations is JPY 200,000,000 (two hundred million) in situations where core infrastructure operators fail to report incidents or take corrective measures even after receiving an order to do so; and JPY 300,000 (three hundred thousand) in situations where core infrastructure operators fail to respond to requests for the submission of materials related to incident reports.

Additionally, under the Penal Code and the Act on Punishment of Crimes Related to Information and Communications, those who jeopardize cybersecurity may be punished, for example: (i) computer damage and obstruction of business (ie, unauthorized alteration or destruction of computer data) is punishable by up to five years' imprisonment or a maximum fine of JPY 1,000,000 (one million); (ii) computer fraud (ie, using a website or email claiming to be a financial institution to defraud visitors of money) carries a maximum sentence of 10 years' imprisonment; and (ii) unauthorized access carries a maximum sentence of three years' imprisonment or a maximum fine of JPY 1,000,000 (one million).

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Under the newly enacted AI Act (see question 23), the AI Strategic Headquarters will be established in the Cabinet Office by September 2025. The AI Strategic Headquarters is responsible for, among others, drafting and implementing the Basic Plan for AI, which outlines the fundamental policies and comprehensive and strategic measures that the government should take to promote the research and development of AI-related technologies.

While the AI Strategic Headquarters does not regulate AI, several ministries and agencies are primarily responsible for the enforcement of AI-related laws under their jurisdiction based on the relevant sector. As part of a soft law approach, the MIC and the METI published the "AI Guidelines for Business Operators Version 1.1" on March 28, 2025 (see question 23).

In the public sector, the Japan AI Safety Institute ("AISI") has been established in the Information-technology Promotion Agency (IPA). AISI is responsible for (i) investigating and discussing standards for safety assessment, (ii) discussing methods of conducting safety assessment, and (iii) engaging in international cooperation with relevant institutes in other countries such as the AI Safety Institute in the US and the UK.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

The Act on Promotion of Research and Development, and Utilization of AI-related Technology ("AI Act") was enacted on May 28 and enforced on June 4, 2025. The purpose of the AI Act is to promote the innovation and address the risks regarding AI. The Act includes limited provisions concerning the responsibilities of private entities as most of its provisions target the government. Entities utilizing AI, such as "developers," "providers," and "users," including foreign entities, are obligated (i) to actively make an effort to enhance and advance their business activities and create new industries through the proactive use of AI-related technologies and (ii) to cooperate with the measures implemented by national and local governments.

In some sectors, relevant laws regulate the deployment and use of artificial intelligence. For example, in the medical device sector, there is a move to accommodate AI-enabled medical devices under the Pharmaceutical and Medical Devices Act. In relation to automated driving, the Road Traffic Act establishes relevant rules, including a permit system for Level 4 automated driving.

In addition, the "AI Guidelines for Business Operators Version 1.1" were published on March 28, 2025. While these guidelines are not legally binding, they represent soft-law with a goal-based approach, based on other existing three guidelines on AI ("Governance Guidelines for Implementation of AI Principles", "AI R&D guidelines for international discussions", and "AI Utilization Guidelines"). Business operators engaged with AI are expected to voluntarily promote specific initiatives, such as establishing appropriate AI governance. An overview of the guidelines is as follows:

- The entities covered by the guidelines are broadly classified into three categories: (i) "AI Developers" (including entities that study AI), (ii) "AI Suppliers" (entities that provide services incorporating AI), and (iii) "AI Users" (entities that use AI systems or AI services).
- The guidelines present ten principles that are common to the entities subject to the guidelines, and points of emphasis in AI activities are specified based on the category of such entities. The ten principles are: (i) human-centric, (ii) safety, (iii) fairness, (iv) protection of privacy, (v) security, (vi) transparency, (vii) accountability, (viii) education and literacy, (ix) fair

competition, and (x) innovation.
- The appendix to the guidelines includes the following:
  - Relationships among entities and examples of AI services;
  - AI benefits and possibilities, specific examples of risks;
  - practical points for developing AI governance and practical examples;
  - commentaries based on the three categories (AI developers, AI suppliers, and AI users), examples of specific methods for implementing the guidelines, and easy-to-understand references; and
  - checklist for business operators for compliance with the guidelines.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

There is no general legal regime governing the deployment and use of Large Language Models and/or generative AI; however, there are certain provisions of relevant laws and regulations. For instance, with respect to the use of copyrighted works in the development of AI, in certain cases where the use is not intended to enjoy the thoughts or sentiments expressed in the copyrighted work, copyright protection will not apply and such use is not considered copyright infringement, with certain exceptions, under Article 30- 4 (ii) of the Copyright Act. Under this rule, use of third-party copyrighted works for the purpose of "AI learning" for generating AI-created work does not usually constitute copyright infringement. As for the issues under the Copyright Act including the above provisions in the context of generative AI, the Agency for Cultural Affairs published a paper entitled, "General Understanding on AI and Copyright in Japan" on March 15, 2024. This paper is not legally binding.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

Although the AI Act has been enacted, we have not identified any typical mandatory provisions dealing with AI.

As for recommended provisions, there are no provisions typically contained in technology contracts; however, there are several provisions used to mitigate risks related to AI.

In the training and development phase of AI, if the data used for the process infringe on the rights of third parties, the training or development, or outputs of such AI may infringe on such rights of third parties. Therefore, in some cases, a provider of data provides representations and warranties stating that use of the data does not infringe on the rights of third parties including intellectual property rights. In contracts that are favourable to providers of data, on the other hand, such warranties can be disclaimed in addition to the disclaimer of accuracy and completeness of data.

In the generation and use phase, there is a risk that the outputs of AI may not be copyrighted works. Thus, in some outsourcing contracts, the consignee is prohibited from using AI in order to allow the consignor to obtain copyright for the deliverables

The AI section of the "Contract Guidelines on Utilization of AI and Data Version 1.1" (2019) published by the METI explains factors to consider and methods to prevent issues including some of the above, for contracts that concern the development and utilization of AI-based software. The Contract Guidelines are supplemented by the appendix to the "AI Guidelines for Business Operators" in consideration of changes to the development and utilisation of AI since the publication of the Contract Guidelines. The "Checklist for Contracts Regarding the Use and Development of AI" (2025) has also been published by the METI.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs can be found in contracts and terms and conditions for AI that is broadly provided to general users. In many cases, the rights and ownership are vested in users subject to certain conditions of usage.

27. Blockchain – What are the principal laws

(present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

There are no laws that govern blockchain specifically.

Regarding digital assets, if the assets constitute security tokens, then the regulations related to securities will apply under the Financial Instruments and Exchange Act ("FIEA").

Shares and bonds represented in tokens and electronically recorded transferable rights are classified as securities which are required to be handled by Type I Financial Instruments Business Operators and are subject to disclosure rules. Security tokens that are subject to technological restrictions on transfer may fall into another type of securities.

As for the digital assets which fall under crypto-assets, the crypto-asset exchange service providers and the intermediaries of crypto-assets are regulated under the Payment Services Act ("PSA"). There are ongoing discussions about subjecting crypto-assets to the regulations of the Financial Instruments and Exchange Act, including the imposition of disclosure obligations and insider trading regulations to protect investors.

Stablecoins are also subject to the regulations under the PSA. Certain stablecoins are classified as electronic payment instruments and the PSA regulates the intermediaries of stablecoins.

Further, from the perspective of anti-money laundering, certain services handling digital assets are subject to the Act on Punishment of Organized Crime and Control of Proceeds of Crime.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

The Telecommunications Business Act governs both search engines and marketplaces. Separately, multiple laws related to online sales, advertising, and platforms apply with respect to marketplaces.

- Regulations under the Telecommunications Business Act

Under the Telecommunications Business Act, large-scale internet search engines and large-scale social media service providers with at least 10 million monthly users that are designated by the Minister of MIC must make a telecommunications business filing and comply with certain regulations under the Act. Marketplaces are not subject to these requirements.

Further, the Minister of MIC may designate telecommunications carriers (including search engines and marketplaces) as providing telecommunications services that have a significant large number of users (at least 10 million users for free services and at least 5 million users for paid services). If so designated, such telecommunication carriers must properly handle specific user information (i.e., (i) information protected under secrecy of communications and (ii) certain searchable information that can identify users).

Further, when certain telecommunications carriers stipulated in Regulations for Enforcement of the Telecommunications Business Act (including search engines, marketplaces, and social media services) send certain programs to users' devices to transfer such users' information stored in their devices (such as third-party cookies, tags, and advertising IDs) externally, they must give prior notification to the users of the content of the user information that is to be sent externally, the destination of such information, and the purpose of use of such information, or place the user in a position where they can obtain such information.

- Regulations Related to Marketplaces

Under the Act on Specified Commercial Transactions, regarding online sales, it is obligatory for businesses to display important information when advertising, and false or exaggerated advertisements are prohibited. Furthermore, the Act against Unjustifiable Premiums and Misleading Representations prohibiting businesses from making inappropriate advertisements or representations that could mislead consumers and offering excessive benefits that could distort consumer judgement

Under the Act on the Protection of Consumers Who Use Digital Platforms for Shopping, obligations are imposed on "digital trade platforms (DTPs)" such as online malls, to make efforts to implement certain measures to address issues related to online sales transactions conducted using the DTP and resolve disputes. Furthermore, DTPs are obliged to publicly disclose an outline and implementation status of such measures.

Under the Act on Improving Transparency and Fairness of Specified Digital Platforms, the Minister of Economy, Trade and Industry designates businesses that provide

platforms exceeding a certain size as “specified digital platform providers”. The designated “specified digital platform providers” are obliged to (i) disclose information such as commercial terms, (ii) ensure fairness in business operations, and (iii) report on the status of their business operations. As for the platform providing online mall or app stores, three online mall operators (Amazon, Rakuten, LY Corporation(Line Yahoo)) and two app stores (Apple, Google) have been designated as specified digital platform providers to date.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

While there are no laws that specifically govern social media, the Telecommunications Business Act and the Provider Liability Limitation Act are closely related to social media.

Providers of social media services generally fall under the category of telecommunications carriers and have a duty to protect the secrecy of users' communications. Services that mediate the communications of others using telecommunications equipment are generally required to file a notification under the Telecommunications Business Act. The provision of a direct chat function would correspond to the mediation of others' communication. Therefore, social media services with a direct chat feature must file a notification under the Telecommunications Business Act (even without a direct chat feature, as stated in #26, large-scale social media services need to make a notification). As described in #26, obligations related to specified user information in the case of telecommunications services with a significant large number of users and obligations related to the external transmission of information regarding users also apply to social media services.

The Information Distribution Platform Act sets out the requirements for exemption from civil liability for telecommunications providers (including social media) in the event that information infringing on the rights of third parties (“rights-infringing information”) is posted on social media. The Act sets out certain conditions for the provider to be exempted from civil liability in the case where (i) the provider deletes the rights-infringing information without the consent of those who post it or (ii) the provider does not delete the rights-infringing information. Furthermore, the Act allows the relevant third-party to request the provider to disclose information regarding the party that posted the rights-infringing information.

Additionally, the Act includes new provisions for transparent and prompt responses to information infringing on rights, effective May 17, 2025. Under these new provisions, certain large-scale web media, such as social networking services (SNS) designated by the Minister of Internal Affairs and Communications (Currently, a total of 9 companies, including Google, LY Corporation, Meta, TikTok, and X, have been designated), are required to fulfill the following obligations:

1. Publicize the method for receiving requests from infringed persons (those whose rights have been violated by information distributed on the web media).
2. Investigate the infringing information: When an infringed person requests the large scale web media to take measures to prevent the transmission of infringing information, the large scale web media shall promptly conduct an investigation.
3. Appoint and register specialists to investigate infringing information.
4. Notify the requester: Within 14 days from the date of receipt of the request from an infringed person, notify the requester of the results of the investigation and whether measures will be taken to prevent the transmission of infringing information.
5. Publicize the standards for implementing measures to prevent transmission.
6. Notify those who post the information when action is taken to prevent the transmission of infringing information.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

If a business operator violates the new provisions of the Information Distribution Platform Act mentioned above, the Minister for Internal Affairs and Communications will first issue a recommendation to take the necessary measures to rectify the violation. If the operator fails to comply with this recommendation, the Minister can then issue a rectification order. Only if the operator fails to comply with this rectification order will criminal penalties be imposed: imprisonment with work for not more than one year or a fine of not more than JPY 1 million for the individual offender, and a fine of not more than JPY 100 million for the legal entity (however, the obligation to investigate mentioned above is excluded from these dispositions). This system is designed to compel a transparent and prompt response to rights infringements

through a phased escalation from recommendation to order, and finally to criminal penalty.

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

In Japan, there is no single law regulating spatial computing. However, under the Unfair Competition Prevention Act, it is possible to seek injunctive relief or damages if a counterfeit product is provided in a digital space (Article 2, Item 3; Article 3; Article 4).

Additionally, when creating or using content in spatial computing, it is necessary to ensure that the process does not infringe upon other parties' intellectual property rights, such as copyrights, patents, or design rights, and to avoid infringing upon portrait rights when using other parties' portraits. Further, compliance with existing intellectual property laws and portrait rights provisions is required. However, under Japanese law, rights related to digital content are distinguished from those related to physical content. Whether intellectual property rights and portrait rights for digital content are granted/arise in the same manner as in physical space, and to what extent the rights to digital content extend into physical space (and vice versa), are currently subjects of debate and must be considered on a case-by-case basis.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

In Japan, there is no single law regulating quantum computing and related issues. However, the Economic Security Promotion Act and the Foreign Exchange and Foreign Trade Act make references to quantum computing technology and the import/export thereof.

The Economic Security Promotion Act establishes basic policies for promoting the economic security, and designates “quantum information science" as a specific critical technology. On the other hand, the Foreign Exchange Act manages and coordinates foreign exchange and foreign trade transactions with the aim of promoting the proper development of foreign trade and maintaining peace and security in Japan and the international community. It stipulates that prior approval from the relevant authorities is required for the export or provision of technology related to quantum computers or related items (Article 48 of the Act, Article 1 of the Export Trade Control Order, and Appendix 1, etc).

In addition, the quantum industry is viewed with importance, and policies for creation and development are under consideration.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

Under Japanese law, there is no single statute that governs the data center business, which is in essence a collection of various services, and instead a variety of laws may apply depending on the overall deal structure, the nature of the services offered, the facility's structural design, its physical configuration, and so forth.

- Regulations on Telecommunications

If a data center operator provides telecommunications lines, which it procures itself, to service users, this activity is classified as a telecommunications business and requires registration or notification under the Telecommunications Business Act.

- Regulations on Building Construction and Operation

A business that contracts for the completion of certain civil engineering and construction works must obtain a permit under the Construction Business Act. Therefore, a permit under the Construction Business Act may be required when contracting for the completion of data center construction or various other works, such as electrical work requested by users after construction or during user turnover. Also, depending on the deal structure (e.g., a GK-TK structure and a TMK structure), careful compliance with the relevant regulations is required. For example, in the case of a GK-TK structure, it is necessary to take care not to become subject to the regulations under the Act on Specified Joint Real Estate Ventures and to also ensure that anonymous partnerships are not denied.

- Regulations on Security Services

A business that performs security services for certain facilities is classified as providing security services and must obtain certification under the Security Services Act. Therefore, anyone providing resident security services at a data center must be certified under the Security

Services Act.

- Regulations on Waste Management

Waste generated at data centers must be handled in accordance with the Act on Waste Management and Public Cleaning.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

In the near future, we expect developments in the fields of (i) AI, (ii) web 3, and (iii) Metaverse.

- AI

As for AI, guidelines related to AI technologies are planned to be established and published by the Cabinet Office under the AI Act. These guidelines will not be legally binding and are expected to be voluntarily followed by entities, but depending on the content, entities utilizing AI may have a responsibility to cooperate therewith.

The Japan Patent Office is working on clarifying the concepts under the Patent Act in light of the advancement of AI technology. Specifically, there are ongoing discussions about whether inventions made by natural persons utilizing AI qualify as "inventions" under the Patent Act, and what criteria should be used to identify the "inventor," including considerations involving AI developers.

The practical application of agentic AI is advancing, and it is expected to become even more widespread in the near future. Regarding agentic AI, various legal issues may arise, such as the legal subjectivity of agentic AI, the treatment of contracts signed by agentic AI, liability for tort, product liability, criminal liability, regulations on services provided by agentic AI, regulations on advertising and labeling, handling of intellectual property, data, and personal information, issues related to competition law, and employment and labor laws.

- web3

As for web 3, the web 3 working group in the Liberal Democratic Party published the "Web3 Proposal 2025 – Transforming Crypto-Assets into Assets that Contribute to People's Asset Building" in May 2025. The Proposal aims to make crypto-assets reliable and sound by subjecting them to the regulations of the Financial Instruments and Exchange Act, including the imposition of disclosure obligations and insider trading regulations for investor protection. This proposal also calls for subjecting crypto assets to separate taxation, similar to other financial instruments, under the tax laws.

Furthermore, with the amendment of the Payment Services Act in June 2025, regulations related to crypto[-] asset related businesses and stablecoins have been revised to ensure user protection and promote innovation. It is important to continue monitoring regulatory developments related to web 3.

- Metaverse

As for Metaverse, at the Ministry of Internal Affairs and Communications, the "Study Committee for Realizing a Safe and Secure Metaverse" has been convened in anticipation of a significant increase in the market size and number of users of the metaverse in the near future, and experts thereat are engaged in discussions aimed at creating a safer and more secure metaverse for users. This committee has published a report on the market, technology, and domestic and international policies and regulations regarding the metaverse, and has formulated the "Principles of the Metaverse." These principles outline the principles for the further self-motivated and autonomous development of the metaverse and principles for improving trustworthiness for metaverse-related service providers (including "world" providers and platformers).

In light of damages arising from unauthorized imitation and sale of designs in both the physical and virtual worlds, the Japan Patent Office is discussing the direction of the design patent regime concerning designs in virtual spaces. Specifically, they are considering the revision of the design patent regime and the implementation of institutional measures to include images representing the shapes and forms of virtual goods as protected subjects.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

No, technology contracts do not commonly include such provisions, while ESG is a hot issue in the technology field.

Contributors

Keiji Tonomura
Partner
keiji_tonomura@noandt.com

Minh Thi Cao Koike
Counsel
minhthi_caokoike@noandt.com

Hiroya Nadamoto
Associate
hiroya_nadamoto@noandt.com

Anju Yamamoto
Associate
anju_yamamoto@noandt.com