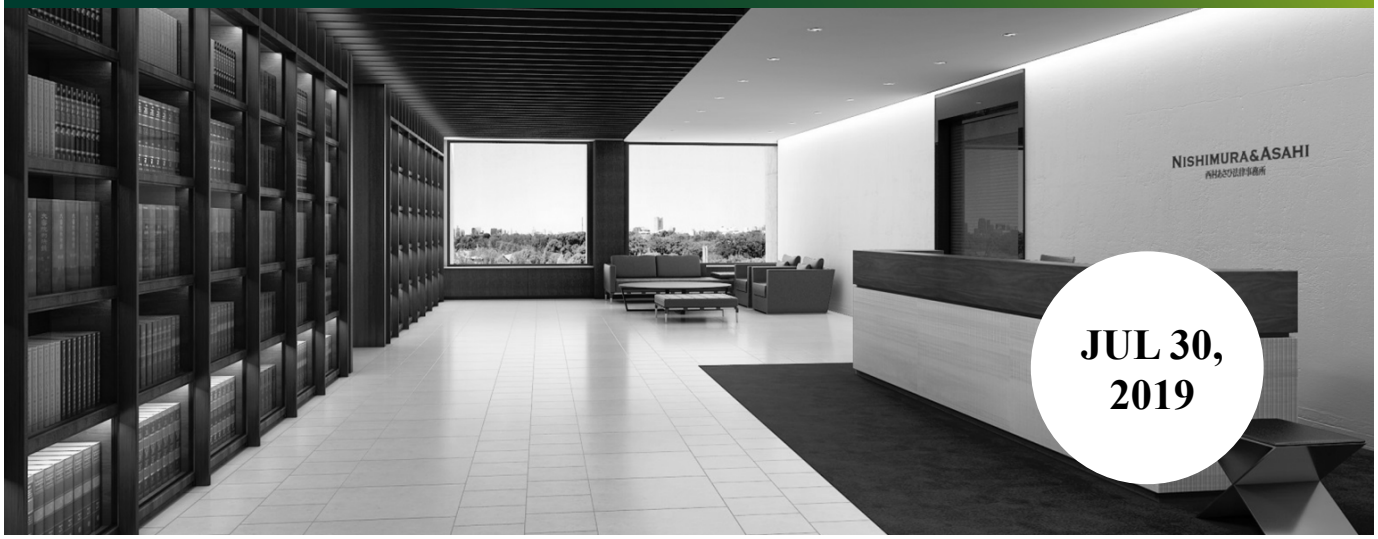
西村あさひ法律事務所
NISHIMURA & ASAHI
Robotics/Artificial Intelligence Newsletter



An overview of Japanese law regarding data

Shinnosuke Fukuoka

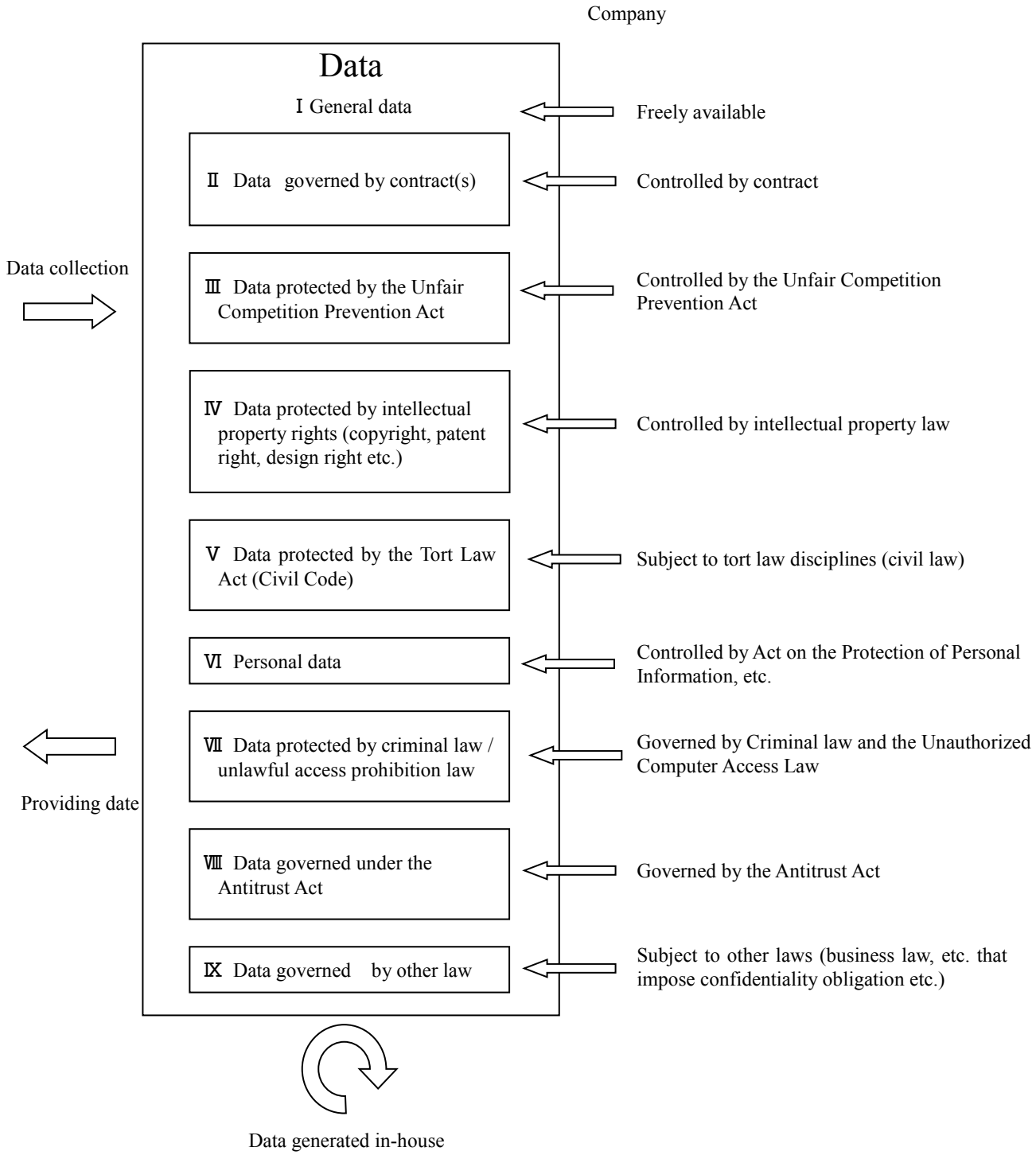
In principle in Japan, data is free to use, no matter who uses it or how they do so. However, there are exceptions to this principle, such as cases where someone is given the right to control data through the Copyright Act, Unfair Competition Prevention Act, Act on the Protection of Personal Information, or the like.[1] Misinterpretation of such exceptions can have extensive consequences. As such, it is important for companies and investors alike, to adopt a legal perspective where data is concerned. With this in mind, this article will inform readers about some of the basic elements of data regulation in Japan, following the data classifications below:[2]

(Ⅰ) General data (data other than Ⅱ to Ⅸ below)
(Ⅱ) Data governed by contract
(Ⅲ) Data protected by the Unfair Competition Prevention Act
(Ⅳ) Data protected by Intellectual Property Rights
(Ⅴ) Data protected by Tort Law Act (Civil Code)
(Ⅵ) Personal data
(Ⅶ) Data protected by criminal law / unlawful access prohibition law
(Ⅷ) Data governed under the Antitrust Act
(Ⅸ) Data governed by other law

[1] Worthy of note at the outset is that Japan does not a have a singular "data law;" instead, data regulation comprises a patchwork of interconnected laws.

[2] Note, Ⅱ to Ⅸ may overlap, as is illustrated in Chart 1 on the final page.

【**Chart 1**】Data type and constraints



Ⅰ General data

Generally, data are free to use for any purpose (unless the data falls under categories Ⅱ to Ⅸ). For example, data about temperature and humidity and data on traffic volume are freely available to the public. In other words, the person generating the data can not assert rights over such data no matter how they collected the data or intended to use it. However, even if it can be used freely, as a matter of fact, only those who have actual access to the data can use it.

Ⅱ Data governed by contract

In cases where parties have agreed by contract, the parties are required to handle associated data according to the contents of such agreement (especially when such agreement includes a confidentiality clause). Moreover, the penalties for failing to handle data in the manner outlined by a relative agreement can be (and typically are) also determined within the agreement. As such, data governed by contract differs from both the data concerned in Ⅰ and the data concerned in Ⅲ to Ⅸ, in that, in principle, the contents, terms, and penalties can be freely set by the parties involved. Keep in mind, contracts can only bind the signatories; contracts cannot prevent third parties (i.e. those not bound by the contract) from utilizing the associated data, other than through the control of access as discussed with relevance to general data (Ⅰ).

In addition, it is necessary to pay attention to both the data associated provisions of a contract and the contract as a whole. Despite the agreement of the parties, some data provisions may not necessarily be valid or effective; among other things, parties cannot contract to circumvent the law, the Civil Code (after the revision and Consumer Protection Act) may take precedence, or the contract as a whole may be invalidated for reasons unrelated to the associated data. In short, it is necessary to pay attention, first, to whether the contract is really a contract and, second, whether the data related provisions are drafted effectively.[3]

Ⅲ Data protected by the Unfair Competition Prevention Act

With respect to data protected by the Unfair Competition Prevention Act ("UCPA"), it is possible to request an injunction or demand damages from a person who acquired, used, or disclosed data in a manner that could be considered in furtherance of unfair competition (Articles 3 and 4). This is because the UCPA seeks to protect data related to "trade secrets;" information that is: (i) managed for secrecy, (ii) useful for business purposes, and (iii) non-public.[4,5] Therefore, when desiring to protect trade secret data, it is necessary to manage confidential information through such means as limiting users and/or having approved users sign a non-disclosure agreement. Moreover, data that is provided to a large number of people (i.e. "big data") does not qualify as "confidential" and cannot be protected as a trade secret by the UCPA. However, according to a recent amendment of the UCPA (effective July 1, 2019), data that does not qualify for trade secret protections but that satisfies the requirements necessary to qualify as big data,[6] will be subject to the protection of the new UCPA concept: "limited offer data."

Ⅳ Data protected by Intellectual Property Rights

There are various laws regarding intellectual property rights, but in relation to data, the Copyright Act, Patent Act, and Design Act are often considered the most applicable. Examples of copyrighted data include sentences written by third parties and photographs of pictures in general. Even if data itself is not copyrighted, a copyright can be established for a collection of data (i.e. a "database"). If data itself and database are copyrighted, the copyright holder has the right to control copying, modification, and assignment of the copyrighted data and database. A person other than the copyright holder cannot do these acts without the permission of the copyright holder.

---

3 Matters for which we recommend seeking professional guidance.

4 UNCA Art. 2(6) - *The term 'Trade Secret' as used in this Act means technical or business information useful for business activities, such as manufacturing or marketing methods, that are kept secret and that are not publicly known*.

5 The UCPA is also more broadly associated with Intellectual Property Law but, as it does not grant property rights to the information itself, it differs from the intellectual property law such as the Copyright Act, etc. (discussed below)

6 e.g. purchase records and movement records of customers.

However, there are cases where the Copyright Act restricts the rights of copyright holders, allowing third parties to use copyrighted works without obtaining permission from the copyright holder. This is because, from a historical perspective, "copyright" was legislated for the protection of novels, music, paintings and other such expressions of "creativity." As it is generally considered that there is no "creativity" involved with the collection of "factual data," copyright is often not established on such data.[7]

Ⅴ Data protected by the Tort Law Act (Civil Code)

Unauthorized users of data may be subject to damages in accordance with the severity of the associated wrongful acts.[8] For example, some court cases have recognized liability for damages due to torts involving the copying of significant volume of data, concerning proposed labor and cost reductions. However, there is also a Supreme Court ruling that suggests that damages cannot be claimed against the use of data that is not protected by copyright law. Therefore, whether copying of significant volume of data without copyrights creates liability for tort damages is still a matter of discussion.[9]

Ⅵ Personal data

Information on individuals is also called "personal data." The handling of personal data is governed by the Personal Information Protection Law, etc. It is generally required by the law to obtain the consent of the person himself/herself when using data that concerns them or providing such data to a third party, though there are some exceptions. Moreover, there are cases where such data cannot be used at all and/or punishment has been rendered in association with such use.

Ⅶ Data protected by criminal law / unlawful access prohibition law

Access to certain data may be prohibited by law. Criminal punishment may be imposed concerning unauthorized access to such data. Such punishment may include penalties under both criminal law and the UCPA.

Ⅷ Data governed under the Antitrust Act

Handling of certain data may be subject to the Antitrust Act; issues concerning control of such data are multifaceted. First, the exchange of pricing data among peer companies (i.e. those competing in the same market or markets), is considered cartel behavior and prohibited by the Antitrust Act. Second, when a business operator in a superior position (i.e. having an influential presence in a market defined by the relevant authority) uses the position to unfairly acquire data from or concerning a counterparty, use of such data could be considered abuse of their superior position (unfair trade practice) and thus penalizable under the Antitrust Act. Third, the collection and possession of large amounts of data by platform operators and others has recently increased in popularity and extent. It is under discussion whether the act of monopolizing such data violates the Antitrust Act. Recently, Japanese Government has started to discuss how to apply the Antitrust Act to companies who hold big data.

---

7 For database works, creativity is considered unrelated to the data itself, but creativity is necessary for selection and systematic organization of information.

8 Civil Code, Art. 709 - *A person who has intentionally or negligently infringed any right of others, or legally protected interest of others, shall be liable to compensate any damages resulting in consequence*.

9 In the case of data, it is difficult to make an injunction due to the fact that the principle of monetary damages is central to Japanese law (Civil Code, Art. 722 (1)). Civil Code, Art. 417 - *Unless other intention is manifested, the amount of the damages shall be determined with reference to monetary value*.

Ⅸ Data governed by other law

Although the above mentioned laws are the primary means by which data is governed in Japan, there are other laws that regulate the handling of data. For example, financial institutions, telecommunications carriers, doctors, and lawyers are obligated to maintain confidentiality according to the laws of their respective fields. Therefore, with regard to the data held by those persons, free usage of data is restricted by these laws.

Conclusion

In principle, data can be used freely, but there are some types of data to which this principle does not apply. For companies in a position to use data, it is important to understand these limitations and to take a position on the data they own. There are few legal protections hampering the use freely available data, but there are restrictions on the use of legally protected data; this makes knowing how to categorize data important for companies and individuals alike.

Therefore, when using data, it is essential to analyze the intended use from a legal perspective and to create a "scheme" of data usage based on such analysis. Building an appropriate scheme for using data is important not only from the perspective of compliance and avoidance of conflicts but also for the purpose of improving brand value, reducing costs, and securing future development potential. In order to conduct such legal analysis and scheme creation, it is essential to consider the above various laws related to data.

Shinnosuke Fukuoka Partner
E-mail: s_fukuoka@jurists.co.jp

Shin Fukuoka is a partner of N&A. In the area of Robotics/Artificial Intelligence, he mainly handles A.I., Big Data, and IoT. He contributes to numerous publications, including the "Law and Contract of Data," "Artificial Intelligence: Law and Issues," and "Law and Strategy of the Internet of Things and Artificial Intelligence."

Public Relations Section, Nishimura & Asahi
Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo 100-8124, Japan
Tel: +81-3-6250-6202 Fax: +81-3-6250-7200 E-mail: newsletter@jurists.co.jp URL: https://www.jurists.co.jp/en